Interdisciplinary Description of Complex Systems 23(2), 95-104, 2025

CYBERSECURITY AND THE FLIGHT SAFETY OF UNMANNED AERIAL SYSTEMS AND UNMANNED AERIAL VEHICLES

Ahmed Douzi[1], Róbert Szabolcsi[2] and Judit Lukács[2, *]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering
Budapest, Hungary

DOI: 10.7906/indecs.23.2.2
Regular article

Received: 31 January 2024.
Accepted: 24 April 2025.

ABSTRACT

Unmanned Aerial Systems (UAS) and Unmanned Aerial Vehicles (UAV) are increasingly susceptible to cybersecurity threats, posing significant risks to flight safety and operational integrity. This article presents a comprehensive study of the cybersecurity challenges faced by UAS and UAV, emphasizing their vulnerability to cyber-attacks due to reliance on wireless communications and remote operations. The potential impacts of cyber threats on UAS and UAV, including financial losses and operational disruptions, are examined. Furthermore, the article discusses ongoing investigations and regulatory measures aimed at integrating cybersecurity and physical security protocols to mitigate credible threats to national security and public safety. By addressing these critical issues, this article aims to contribute to the understanding of cybersecurity in the context of unmanned aerial platforms, providing insights into the evolving landscape of cyber threats and the measures required to ensure the safe and secure operation of unmanned aerial systems. This article provides a short overview of the key focus areas including the cybersecurity challenges, potential impacts, ongoing studies, and regulatory measures related to UAS and UAV.

KEY WORDS

unmanned aerial systems, unmanned aerial vehicles, cyber-attacks, cybersecurity threats, best practices

CLASSIFICATION

JEL: L63, L92, R41

*Corresponding author, η: lukacs.judit@bgk.uni-obuda.hu; -;
Óbuda University, Népszínház 8., H-1081 Budapest, Hungary

INTRODUCTION

UAS and UAV have revolutionized various industries, including commercial, military, and recreational sectors, by offering unprecedented capabilities for aerial operations [1, 2]. As these systems continue to proliferate, the critical importance of cybersecurity in ensuring the flight safety and operational integrity of UAS and UAV becomes increasingly evident. Cybersecurity threats pose significant risks to the reliable and secure operation of these aerial platforms, potentially leading to financial losses, operational disruptions, and compromised safety. Therefore, understanding and addressing the cybersecurity challenges associated with these systems are paramount to ensuring their safe and effective utilization in diverse applications.

In this context, the introduction aims to provide a comprehensive overview of the significance of cybersecurity in the realm of UAS and UAV, setting the stage for the subsequent discussion on cybersecurity threats, current research, regulatory measures, and best practices.

SPECIFIC CYBERSECURITY VULNERABILITIES

The vulnerability of Unmanned Aerial Vehicles (UAVs) to cyber-attacks is mainly due to their reliance on wireless communications and their tendency to be operated from a distance. They are susceptible to interception, spoofing, and hijacking by malicious actors. In addition, the data transmitted between UAVs and their operators can be intercepted and used to gain access to sensitive information or networks. The report by SkyGrid emphasizes the vulnerability of UAV systems to cyber threats and the need to mitigate the risk of drone-based cybersecurity attacks [3].

There were 26 distinct types of threats identified, collectively constituting the entire attack surface for UAS. These threats encompass the full spectrum of confidentiality, integrity, availability, and privacy. The specific threats are detailed in Table 1.

Table 1. Recognized risks associated with UAVs [4].

Threat Source	Threat	Confidentiality	Integrity	Availability	Privacy
Supply-Chain	Firmware Hijacking	✓	✓	✓	✓
	Hardware Forgery	✓	✓	✓	✓
Physical	Damage		✓	✓	
	Capture	✓	✓	✓	
Sensor	Spoofing		✓	✓	
	Jamming			✓	
Communication	Eavesdropping	✓			✓
	Jamming			✓	
	De-authentication			✓	
	Poisoning	✓		✓	✓
	Replay		✓		
	Authentication Hijacking	✓		✓	✓
	Hijacking Session	✓	✓		✓
Malware	Eavesdropping based Malware	✓			✓
	Dos control			✓	
Miscellanea	Forging Commands		✓	✓	
	Hijacking Video	✓	✓		
	Battery Exhaustion Dos			✓	
	AI-hijacking		✓	✓	
	Hardwar-Dos			✓	
Hardening Defects	Open Service Exploitation	✓		✓	✓
	SWDEV Flaws Exploitation	✓	✓	✓	✓
	Authentication Bypass	✓		✓	✓
UAV Network	Rogue-Drone	✓	✓		✓
	Routing-Control	✓	✓	✓	✓

By addressing these vulnerabilities and understanding the breadth of potential threats, it becomes possible to develop effective strategies to enhance the cybersecurity posture of UAS and mitigate the associated risks.

POTENTIAL IMPACTS OF CYBER THREATS ON FLIGHT SAFETY

The potential consequences of cyber threats on flight safety within the aviation industry are extensive, encompassing the capacity to disrupt operations, impose financial burdens, and compromise passenger and crew safety. Cybersecurity threats have the potential to cause severe operational disruptions, leading to flight delays or cancellations, damage to the reputation of an airport, loss of customer trust, and financial losses, Figure 1.

These threats are particularly concerning given the increasing digitization of the aviation industry, which has resulted in a significant rise in cybersecurity risks. Unauthorized access to critical systems, such as air traffic control and aircraft systems, could have catastrophic consequences, including endangering safety and disrupting the air traffic control system. Furthermore, cyber-attacks on airlines and airports pose the risk of data breaches, flight disruptions, and potential threats to national security.

The extensive interconnectivity and complexity of the aviation industry, coupled with its critical role in the socio-economic development of states, make it a prime target for cyber-attacks. As a result, the industry is actively addressing these challenges through ongoing research, regulatory measures, and the development of global frameworks to enhance cybersecurity and ensure the safety and security of aviation systems and networks.

The interconnected nature of the aviation industry, spanning various sectors and stakeholders, presents multiple-entry points for cyber-attackers, including reservation systems, air traffic controls, in-flight entertainment devices, cockpit instruments, and cargo handling systems [6].

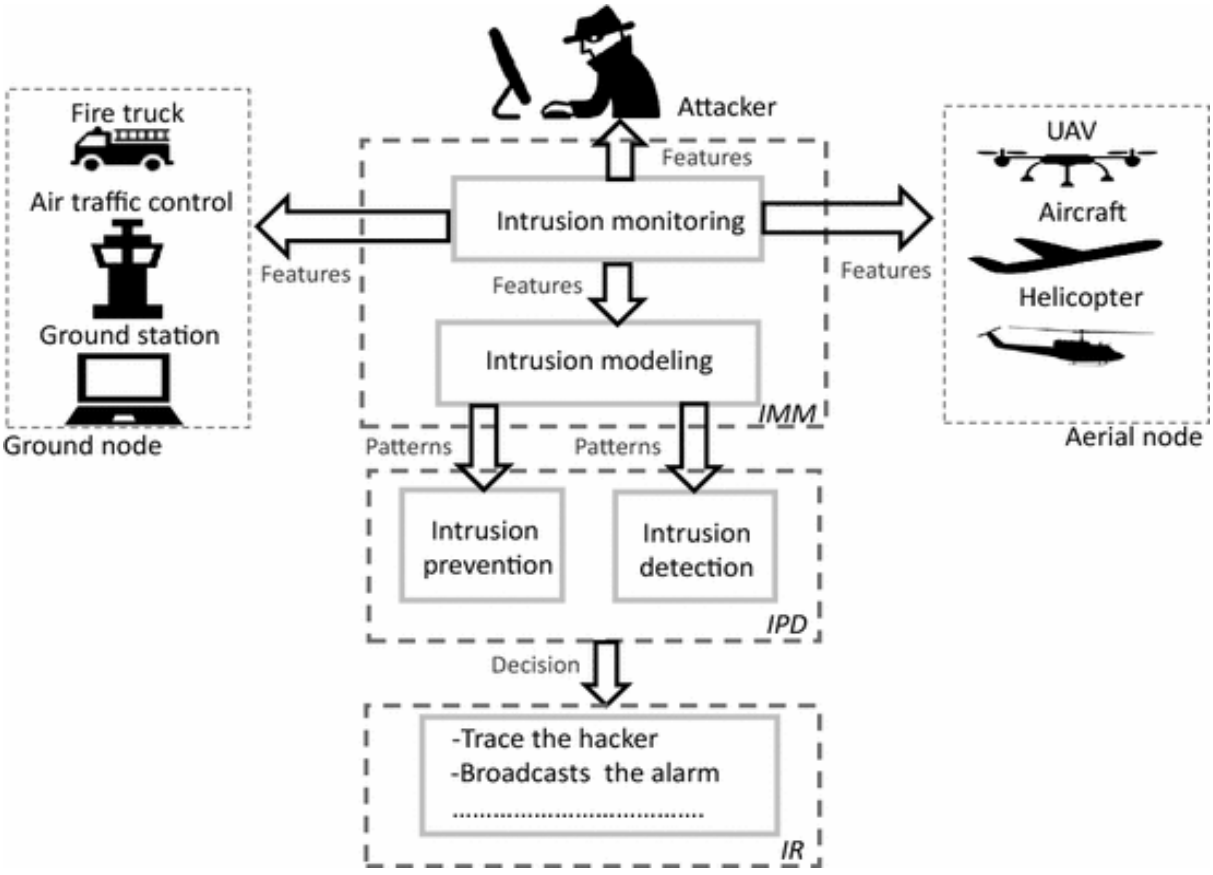

Figure 1. Illustration of the Aircraft Security Framework [5].

Furthermore, the reliance on automation and digital solutions, coupled with reduced airport staff due to the pandemic, has increased the vulnerability of airport and airline systems to cyber-attacks. The consequences of cyber threats extend beyond immediate operational disruptions, affecting passengers, airlines, and even national security [7].

Understanding the full scope of these impacts is crucial for comprehending the severity of the cyber threats facing the aviation industry and underscores the necessity for robust cybersecurity measures. Implementing proactive and multi-layered cybersecurity strategies, including regular risk assessments and the prioritization of cybersecurity, is essential to mitigate the industrial vulnerability to cyber-attacks.

Ongoing research on cybersecurity vulnerabilities for UAS and UAV is crucial in the aviation industry. This research focuses on understanding the vulnerabilities of these systems, the types of cyber-attacks faced, and the development of robust countermeasures.

Integration of cybersecurity and physical security protocols is another key area of focus. The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes the importance of incorporating cybersecurity and physical security into policies and procedures that support secure drone operations [8]. This includes understanding and managing cyber and physical risks, providing risk mitigation guidance, and coordinating federal capabilities to counter credible drone threats [9].

Regulatory measures are also essential to ensure safe and secure UAS/UAV operations. The Federal Aviation Administration constantly assesses regulations to ensure that small UAS operations do not pose a threat [10]. It is suggested that a risk-based approach to regulating UAS could set out regulatory requirements based on the size of the aircraft, the location, and the complexity of the operation [11]. In addition, tools and courses are also available to facilitate the implementation of harmonized UAS regulations and the oversight framework that will enable safe UAS operations.

Unmanned Aerial Systems are inherently unmanned, meaning their navigation and control rely on a mix of remote control and autonomous pre-programmed decisions. In cases of lost remote connectivity, UAS are usually equipped with pre-programmed safe landing sites that align with their mission profile [12].

In this article, a military example is introduced and analyzed to reveal several lacks that lead to the need for the continuous improvement of good practices in UAV applications. The best practices for implementing cybersecurity measures in the aviation industry involve ongoing research on cybersecurity vulnerabilities, integration of cybersecurity and physical security protocols, and the implementation of regulatory measures to ensure safe and secure UAS/UAV operations. Also, the issues concerning the personnel are presented even in non-militarian fields.

RISK ASSESSMENT OF THE UAV COTS AUTOPILOTS AND THEIR COTS GCSS

RISKS THREATENING FLIGHT SAFETY OF THE UAV

In the context of risk assessment for UAV COTS autopilots and their COTS GCSs, it is essential to consider the safety and privacy regulations for unmanned aerial vehicles and the existing regulatory frameworks. The safety risk management of UAS is a critical aspect that requires thorough identification and evaluation of active and hidden risks [13]. Additionally, the currently existing UAV-specific regulations place high emphasis on the safety of UAVs and UAV operations, highlighting the importance of adhering to safety standards and regulations in the assessment of COTS autopilots and GCSs [14].

Moreover, the Unmanned Aircraft Systems Regulatory Framework by ICAO provides relevant documentation, tools, and courses to facilitate the implementation of harmonized UAS regulations and oversight frameworks that enable safe UAS operations [11]. This framework offers valuable guidance for evaluating the regulatory compliance and safety aspects of COTS autopilots and GCSs.

Furthermore, Janik et. al. presented a risk assessment methodology for UAS, emphasizing the importance of assessing technical issues, deterioration of external systems supporting UAS operation, human error, and adverse operating conditions [15]. This methodology can provide valuable insights into the risk assessment process for COTS autopilots and GCSs, enabling a comprehensive evaluation of their safety and security aspects. By leveraging the insights from these resources, a comprehensive risk assessment of UAV COTS autopilots and their COTS GCSs can be conducted, considering safety regulations, risk management methodologies, and existing regulatory frameworks to ensure the safe and secure operation of UAS and UAV.

EVALUATION OF SELECTED AUTOPILOTS FOR CYBERSECURITY

The evaluation of selected autopilots for cybersecurity should consider the following aspects:

- **Vulnerability assessment** – conduct a comprehensive vulnerability assessment of the autopilots, considering potential weaknesses in communication protocols, data encryption, and firmware integrity [4].
- **Threat detection and mitigation** – implement robust threat detection and mitigation measures to safeguard against cyber threats, ensuring the integrity and security of the autopilots and their associated system [16].
- **Compliance with best practices** – ensure that the selected autopilots adhere to industry best practices for secure communication, data integrity, and resistance to tampering, providing a secure and reliable operation in various environments and under different threat scenarios [17].
- **Adherence to regulatory standards** – verify that the autopilots comply with existing safety and privacy regulations for UAVs and the regulatory frameworks governing their operation.

OPTIONS FOR USE AND LIMITS FOR FLIGHT MISSIONS

The options for the use of selected autopilots should be determined based on their ability to provide secure and reliable operation in various environments and under different threat scenarios. Additionally, the limits for their flight missions should be established considering their cybersecurity features, regulatory compliance, and the specific operational requirements of the UAVs and UAV systems. By leveraging the insights from the provided resources, a comprehensive evaluation of the selected autopilots for cybersecurity, along with options for their use and limits for their flight missions, can be conducted, ensuring the safe and secure operation of UAS and UAV.

CASE STUDIES AND EXAMPLE IN MILITARY APPLICATIONS: THE RQ-170 DRONE LOST INCIDENT

The RQ-170 incident occurred on December 5, 2011, when RQ-170 Sentinel UAV was captured near the city of Kashmar. It was announced that the UAV was brought down by the cyber-warfare unit, which commandeered the aircraft and safely landed it. These claims were at first denied, but later acknowledged [18].

This event raises questions about the failure of the drone and the lack of self-destruct capability. One possibility is that the RQ-170 failed in flight and crash-landed in an area where it was recovered before friendly forces could reach it. The cause of the failure remains uncertain,

whether it was due to system failure, compromised navigation systems, or physical damage to the aircraft [18].

Officially it was claimed that technology was utilised to trick the drone into landing where the drone erroneously considered its actual base is. Reverse engineering techniques were used to develop after exploring less sophisticated drones that were captured or shot down previously. That made possible cutting off the communications link by jamming on the communications, forcing the drone into autopilot. The GPS coordinates of the UAV were reconfigured and precise latitudinal and longitudinal data was utilised to force the drone to land on its own [19, 20].

Following the incident, drones based on the captured RQ-170 were produced, including the Shahed 171 Simorgh and Shahed Saegheh [18]. In 2018, it was noticed that oned intercepted drone was a “copy” of the RQ-170 Sentinel [21].

The incident led to a significant shift in the defense industry’s approach to unmanned vehicle security. As a result of the RQ-170 incident, cybersecurity for has risen to the top priority. Enabling technologies like multi-level encryption and cross-domain solutions represent hot markets in the unmanned industry [22].

The absence of a self-destruct capability is a significant concern, as flying near or over hostile territory inherently carries a risk of capture. An auto-destruct system could have been triggered remotely when it was determined that the system was not in friendly control. Alternatively, a destruct mechanism could be logically triggered by lack of signaling, using an extended period without authorized contact as a triggering event for auto-destruct.

This incident and many others underscore the importance of robust cybersecurity measures for UAS and UAVs. They highlight the need for ongoing research into cybersecurity vulnerabilities, the integration of cybersecurity and physical security protocols, and the implementation of regulatory measures to ensure safe and secure UAS/UAV operations. They also emphasize the importance of learning from past incidents to prevent similar occurrences in the future.

DISCUSSION ON CYBERSECURITY BEST PRACTICES FOR UASS AND UAVS

To enhance the cybersecurity of UAS and UAVs, operators should adhere to cybersecurity best practices. Derbah et al. provided a procedural guide emphasizing the importance of secure software and firmware installation, as well as the use of standalone devices with no external connections during operations [23]. Additionally, the CISA offers best practices for operating commercial UASs, including using complicated Service Set Identifiers to obfuscate UAS operations on the network and running mobile device applications in a secure virtual sandbox configuration [24]. These practices aim to protect networks, information, and personnel involved in UAS operations.

Furthermore, it is crucial for UAS operators to evaluate cybersecurity best practices when dealing with software and firmware associated with UAS, ensuring secure communications during all aspects of usage [24]. By implementing these recommendations, UAS and UAV operators can significantly enhance the cybersecurity of their systems and reduce associated risks.

In total, it can be said that there are some main fields that can enhance the security (and cybersecurity) level of UAVs. Since these vehicles are utilized in various sectors, some general and specific areas are to be controlled, Figure 2.

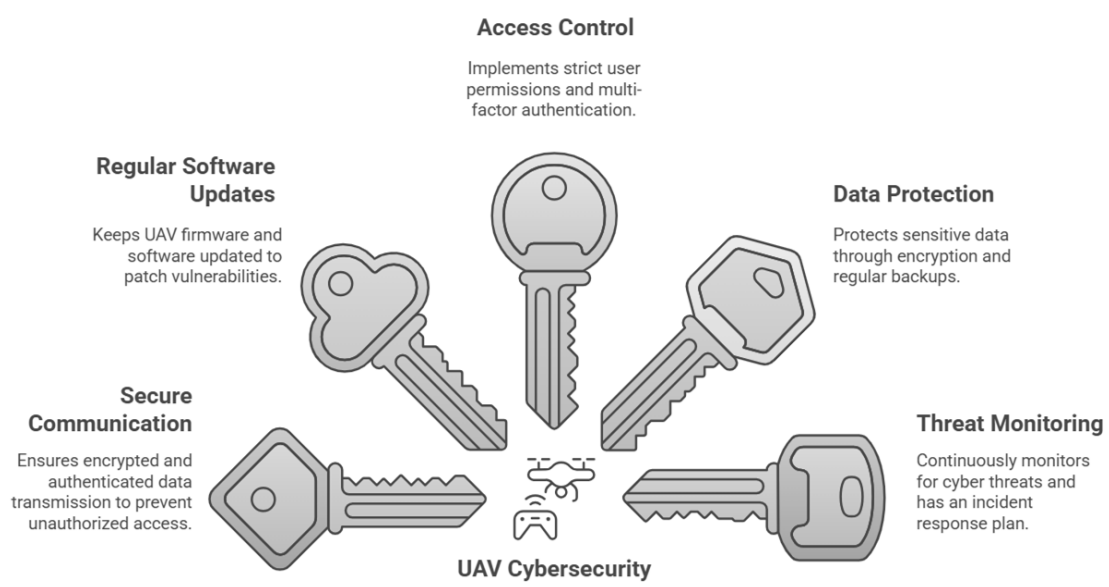

Figure 2. UAV good practices [25]-[35].

The first key issue is the secure communication channel. Since UAVs have ground control stations, a strong encryption protocol is needed for data transmission. That is a possible solution to avoid unauthorized access and cyber-attacks [25], [26]. In addition, to reduce vulnerabilities and improve security levels, it is also important to use softwares and updates that are obtained from trusted sources [27]. The following indicator for efficient, good practices is authentication. To start with, strict access control measures need to be implemented [27]. Furthermore, role-based access control can also improve the niveau of cybersecurity [28]. Finally, Multi-Factor Authentication (MFA) can also add an extra layer of security [29], [30]. Encryption is also useful to handle and protect sensitive data and to avoid cyber incidents [31]. Continuous monitoring systems can reveal unusual activities by monitoring UAVs, and there are also incident response plans to effectively react to any kind of cybersecurity incidents [32].

The next level is the training of the human operators and the personnel on the awareness of potential threats and best practices. Simulated attacks can be a potential tool to conduct real-world scenarios and improve strategies [33]. Tamper detection mechanisms are also applied to alert unauthorized access attempts [34]. Moreover, the knowledge of local and international regulations and standards is also a crucial factor [35].

Finally, there are several additional good practices also in civilian applications that are specifically area-focused: for data collection in different environments [36][37] and further operation strategies [38].

CONCLUSION

The research on cybersecurity threats and solutions for Unmanned Aerial Vehicles and Unmanned Aircraft Systems highlights the vulnerabilities found in system components, emphasizing the need to protect the entire UAS system against potential attacks. The RQ-170 incident has significantly influenced the approach of the defense industry to unmanned vehicle security, leading to a heightened focus on cybersecurity for unmanned vehicles. This incident has prompted the prioritization of cybersecurity in the defense industry, with a particular emphasis on enabling technologies such as multi-level encryption and cross-domain solutions.

The rapid growth in drone usage has raised concerns about cybersecurity implications, both in terms of UAS as cyber-weapons and UAS as cyber-targets. Conceptual approaches have been proposed to enable the enumeration and categorization of UAS-related cyber threats,

emphasizing the need to understand, inventory, and model cybersecurity implications to address current vulnerabilities and future trends. Additionally, industry trends and the implications of these trends for cybersecurity have been presented, highlighting the importance of safeguarding UAS against potential attacks.

The implications of these findings underscore the critical importance of enhancing cybersecurity measures to ensure the safety and security of UAS and UAV systems in the face of evolving cyber threats. By implementing robust cybersecurity best practices and recommendations, UAS and UAV operators can mitigate potential risks and contribute to the overall safety and security of unmanned aerial systems.

In total, it can also be concluded that the good practices include detailed recommendations covering many areas of drone handling and operation to achieve the desired level of cybersecurity.

ACKNOWLEDGMENT

Supported by the 2024-2.1.1 University research scholarship program of the Ministry for culture and innovation from the source of the national research, development and innovation fund.

REFERENCES

[1] Hell, P.M. and Varga, P.J.: *Drone Component for Radio Frequency Detection.* Interdisciplinary Description of Complex Systems **20**(3), 230-238, 2022, http://dx.doi.org/10.7906/indecs.20.3.2,

[2] Vida, G.; Melegh, G.; Süveges, Á.; Wenszky, N. and Török, Á.:*Analysis of UAV Flight Patterns for Road Accident Site Investigation.* Vehicles **5**(4), 1707-1726, 2023, http://dx.doi.org/10.3390/vehicles5040093,

[3] Skygrid: *Cybersecurity Threats Within UAV Systems*. https://www.skygrid.com/addressing-cybersecurity-challenges-to-build-trust-in-advanced-air-mobility,

[4] Sanghavi, P., and Kaur, H.: *A Comprehensive Study on Cyber Security in Unmanned Aerial Vehicles.* In: *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*. New Delhi, IEEE, pp.804-811, 2023,

[5] Sedjelmaci, H. and Senouci, S.M.: *Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution*. The Journal of Supercomputing **74**(10), 4928-4944, 2018, http://dx.doi.org/10.1007/s11227-018-2287-8,

[6] Gopalakrishnan, K.; Govindarasu, M.; Jacobson, D.W. and Phares, B.M.: *Cyber security for airports*. International Journal for Traffic and Transport Engineering **3**(4), 365-376, 2013, http://dx.doi.org/10.7708/ijtte.2013.3(4).02,

[7] Stastny, P. and Stoica, A.M.: *Protecting aviation safety against cybersecurity threats*. IOP Conference Series: Materials Science and Engineering **1226**(1) No. 012025, 2022, http://dx.doi.org/10.1088/1757-899X/1226/1/012025,

[8] U.S. Department of Homeland Security: *Unmanned Aircraft Systems: Be Air Aware - Safe and secure integration of UAS requires effective cyber and physical risk mitigation.* https://www.cisa.gov/topics/physical-security/unmanned-aircraft-systems,

[9] Wang, H., et al.: *Survey on unmanned aerial vehicle networks: A cyber physical system perspective*. IEEE Communications Surveys & Tutorials **22**(2), 1027-1070, 2019, http://dx.doi.org/10.1109/COMST.2019.2962207,

[10] Federal Aviation Administration: *Safe and Secure Operations of Small Unmanned Aircraft Systems*.
https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems,
[11] Masutti, A. and Tomasello, F.: *International Regulation of Non-Military Drones*.
Edward Elgar Publishing, pp.65-90, 2018,
http://dx.doi.org/10.4337/9781785367571.00015,
[12] Alam, M.S. and Oluoch, J.: *A survey of safe landing zone detection techniques for autonomous unmanned aerial vehicles (UAVs)*.
Expert Systems with Applications **179**, No. 115091, 2021,
http://dx.doi.org/10.1016/j.eswa.2021.115091,
[13] Clothier, R.A.; Walker, R.A.: *The safety risk management of unmanned aircraft systems.*
In: Valavanis, K. and Vachtsevanos, G., eds.: *Handbook of unmanned aerial vehicles*. Dordrecht, Springer, pp.2229-2275, 2013,
http://dx.doi.org/10.1007/978-90-481-9707-1_39,
[14] Lee, D.; Hess, D.J. and Heldeweg, M.A.: *Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis.*
Technology in Society **71**, No. 102079, 2022,
http://dx.doi.org/10.1016/j.techsoc.2022.102079,
[15] Janik, P.; Zawistowski, M.; Fellner, R. and Zawistowski, G.: *Unmanned aircraft systems risk assessment based on sora for first responders and disaster management.*
Applied Sciences **11**(12), No. 5364, 2021,
http://dx.doi.org/10.3390/app11125364,
[16] Manesh, M.R. and Kaabouch, N.: *Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions.*
Computers & Security **85**, 386-401, 2019,
http://dx.doi.org/10.1016/j.cose.2019.05.003,
[17] Tang, A.C.: *A Review on Cybersecurity Vulnerabilities for Urban Air Mobility.*
In: AIAA Scitech 2021 Forum, No. 0773, 2021,
http://dx.doi.org/10.2514/6.2021-0773,
[18] Sauliuc, A.: *Growing USA–Iran tensions increase the volatility in the Persian gulf region.*
Romanian Military Thinking **1**(1), 100-115, 2020,
[19] Veilleux-Lepage, Y. and Archambault, E.: *A Comparative Study of Non-State Violent Drone use in the Middle East.*
[20] Frantzman, S.J.: *The Drone Wars: Pioneers, Killing Machines, Artificial Intelligence, and the Battle for the Future.*
Bombardier Books, 2021,
[21] Opall-Rome, B.: *Israel Air Force Says Seized Iranian Drone Is a Knockoff of US Sentinel*.
Defense News, 12, 2018,
[22] Shifa, A., et. al.: *MuLViS: Multi-level encryption based security system for surveillance videos.*
IEEE Access **8**, 177131-177155, 2020,
http://dx.doi.org/10.1109/ACCESS.2020.3024926,
[23] Derhab, A., et. al.: *Internet of drones security: Taxonomies, open issues, and future directions.*
Vehicular Communications **39**, No. 100552, 2023,
http://dx.doi.org/10.1016/j.vehcom.2022.100552,
[24] Nichols, R.K., et al.: *Unmanned Aircraft Systems in the Cyber Domain*.
New Prairie Press, 2019,
[25] Haque, M.S. and Chowdhury, M.U.: *A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV).*
In: *International conference on security and privacy in communication systems*. Springer International Publishing, Cham, pp.113-122, 2017,
http://dx.doi.org/10.1007/978-3-319-78816-6_9,

[26] Bithas, P.S., et al.: *UAV-to-ground communications: Channel modeling and UAV selection.*
IEEE Transactions on Communications **68**(8), 5135-5144, 2020,
http://dx.doi.org/10.1109/TCOMM.2020.2992040,

[27] Nawaz, H.; Ali, H.M. and Laghari, A.A.:*UAV communication networks issues: A review*.
Archives of Computational Methods in Engineering **28**(3), 1349-1369, 2021,
http://dx.doi.org/10.1007/s11831-020-09418-0,

[28] Zhong, L., et al.: *Distributed Optimization of multi-role UAV Functionality Switching and Trajectory for Security Task offloading in UAV-assisted MEC.*
IEEE Transactions on Vehicular Technology **73**(12), 19432-19447, 2024,
http://dx.doi.org/10.1109/TVT.2024.3434354,

[29] Deebak, B.D. and Hwang, S.O.: *Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era*.
Computer Networks **225**, No. 109664, 2023,
http://dx.doi.org/10.1016/j.comnet.2023.109664,

[30] Saqib, R.M., et al.: *Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security.*
Intelligent Automation & Soft Computing **32**(3), 1633-1647, 2022,
http://dx.doi.org/10.32604/iasc.2022.021786,

[31] Kim, K. and Kang, Y.: *Drone security module for UAV data encryption.*
In: 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, Jeju, pp.1672-1674, 2020,
http://dx.doi.org/10.1109/ICTC49870.2020.9289387,

[32] Ramesh Babu, J., et al.: *Drone Network Incident Detection And Response.*
Material Science and Technology **22**(06), 224-228, 2023,
http://dx.doi.org/10.10543/f0299.2023.41652,

[33] Javaid, A.Y.; Sun, W. and Alam, M.: *Single and multiple UAV cyber-attack simulation and performance evaluation.*
EAI Endorsed Transactions on Scalable Information Systems **2**(4), No. e4, 2015,
http://dx.doi.org/10.4108/sis.2.4.e4,

[34] Gu, Y., et al.: *Detection, estimation, and compensation of false data injection attack for UAVs.*
Information Sciences **546**, 723-741, 2021,
http://dx.doi.org/10.1016/j.ins.2020.08.055,

[35] Sanz, D., et al.: *Safe operation of mini UAVs: a review of regulation and best practices.*
Advanced Robotics **29**(19), 1221-1233, 2015,
http://dx.doi.org/10.1080/01691864.2015.1051111,

[36] Cromwell, C., et al.: *A systematic review of best practices for UAS data collection in forestry-related applications.*
Forests **12**(7), No. 957, 2021,
http://dx.doi.org/10.3390/f12070957,

[37] Guan, S., et al.: *sUAS monitoring of coastal environments: A review of best practices from field to lab.*
Drones **6**(6), No. 142, 2022,
http://dx.doi.org/10.3390/drones6060142,

[38] Teppati Losè, L.; Chiabrando, F. and Giulio Tonolo, F.: *Boosting the timeliness of UAV large scale mapping. Direct georeferencing approaches: Operational strategies and best practices.*
ISPRS International Journal of Geo-Information **9**(10), No. 578, 2020,
http://dx.doi.org/10.3390/ijgi9100578.