Essay

The Cybersecurity Risks Threatening Drones: Innovative Solutions in the Digital Age

Driss Abbadi * and Abdelkader Lachkar

Posted Date: 9 January 2025

doi: 10.20944/preprints202501.0694.v1

Keywords: cybersecurity risks; drones; innovative solutions; legislation; regulatory frameworks

Essay

The Cybersecurity Risks Threatening Drones: Innovative Solutions in the Digital Age

Driss Abbadi * and Abdelkader Lachkar

Research Laboratory in Legal, Political, and Economic Studies, Faculty of polydisciplinary Studies, Taza, Sidi Mohamed Ben Abdellah University of Fès, Morocco

* Correspondence: driss.abbadi@usmba.ac.ma

Abstract: Unmanned Aerial Vehicles (UAVs), or drones, were initially developed for military purposes, primarily for surveillance and military operations. Over time, their use expanded into various civilian sectors, including delivery and monitoring. This rapid proliferation has sparked growing concerns about cybersecurity. This article explores the cybersecurity risks faced by drones in an increasingly interconnected digital landscape and proposes innovative solutions to mitigate these threats. The analysis is structured into two main parts: the first examines the latest technological trends and the cybersecurity challenges confronting UAVs, while the second focuses on technical solutions to address these risks, as well as the role of local and international regulations in ensuring the safe deployment of this technology.

Keywords: cybersecurity risks; drones; innovative solutions; legislation; regulatory frameworks

1. Introduction

Unmanned aerial vehicles (UAVs), initially used for military purposes, began to transition into civilian applications during the first decade of the new millennium (Koç, 2023, p. 1). Over time, their numbers have increased significantly, driven by a growing global demand for their diverse applications. The widespread adoption of drones is attributed to their ability to fulfill a variety of needs. They provide users with aerial views that can be accessed virtually anywhere and at any time, in addition to their ability to fly and transport goods. UAVs are also utilized by law enforcement and border surveillance teams. In disaster scenarios, such as nuclear accidents, hazardous material spills, floods, earthquakes, and wildfires, drones are employed to gather information or deliver essential supplies (Yaacoub et al., 2020; Restas, A., 2015). These drones continue to evolve rapidly, playing a prominent role in social media and corporate competition (Koç, 2023, p. 1). Moreover, UAVs have become a vital part of modern military arsenals, representing unmanned aerial systems capable of performing a wide range of missions, from surveillance and reconnaissance to precision strikes and supporting military operations (Grigore & Cristescu, 2024; Majeed, R., et al., 2021).

However, the rapid proliferation of drones has raised significant concerns regarding privacy and security. This growth demands the implementation of essential regulations and controls to prevent accidents and other issues related to overuse and loss of control (Koç, 2023, p. 1). Against this backdrop, this article addresses the cyber risks threatening drones and explores advanced solutions designed to mitigate these risks.

1.1. Importance of the Topic

The subject of "Cybersecurity Challenges of Drones: Innovative Solutions in the Digital Age" is a highly relevant and pressing issue in today's world. As drones are increasingly used in sensitive civilian and military sectors, including transportation, security, logistics, and defense, the risks they face from cybersecurity threats are growing. This study aims to shed light on these threats, particularly as drones become more integrated into critical infrastructure. It also focuses on exploring innovative solutions to strengthen drone security, including methods to protect data, detect cyberattacks, and ensure the safety of embedded systems. By doing so, the study seeks to promote the safe and secure use of drones and offer regulatory frameworks that align with ongoing digital advancements.

1.2. Research Problem

As drones continue to be deployed across various sectors, they encounter significant security challenges in the digital age. Drones are increasingly vulnerable to sophisticated cyber threats, including hacking, unauthorized communication, and cyberattacks that could lead to their hijacking or malicious exploitation. At the same time, emerging technologies such as artificial intelligence and encryption offer potential solutions to bolster drone security and mitigate these risks. However, the dual nature of these technologies presents a complex challenge: developing security solutions that protect drones from escalating threats, while ensuring these solutions are applied safely and effectively without compromising privacy or public security. This leads to several key research questions.

1.3. Research Questions

-What are the latest technological trends in drone development?

-What cybersecurity risks do drones face in the digital age?

-How can modern technologies, such as artificial intelligence and encryption, enhance drone security?

-How can innovative security solutions be developed to protect drones from cyber threats?

-How can legislative and regulatory measures ensure the safe and responsible use of drones at local and international levels?

1.4. Objectives of the Study

The study of "Cybersecurity Challenges of Drones: Innovative Solutions in the Digital Age" aims to explore the increasing security threats faced by drones due to rapid technological advancements. It seeks to analyze the security vulnerabilities that cyberattacks could exploit, such as breaches in control systems and communication networks. The study also focuses on investigating innovative solutions, including artificial intelligence and advanced encryption techniques, to enhance security and protect drones from potential threats. Furthermore, the study aims to assess the legislative and regulatory frameworks that govern drone security, considering the influence of both international and local policies in shaping or disrupting the security standards for this technology.

1.5. Importance of the Study

The significance of this study lies in its focus on the security challenges drones encounter in the digital era and its exploration of innovative solutions to bolster the security of this technology. The study aims to identify security gaps and cyber threats that could target drones, contributing to the improvement of security policies and technologies used to protect them. Additionally, the study seeks to provide novel solutions that promote the safe use of drones across various sectors and foster the development of effective legislative and regulatory frameworks that evolve alongside technological advancements in this field.

1.6. Methodology of the Study

This study will adopt a descriptive-analytical approach to detail the cybersecurity challenges drones face. It will emphasize the importance of developing innovative security solutions that leverage modern technologies such as artificial intelligence and encryption to enhance drone security, enabling them to effectively and efficiently combat emerging cyber threats.

1.7. Research Framework

The study of "Cybersecurity Challenges of Drones: Innovative Solutions in the Digital Age" is divided into two main sections:

The first section focuses on drones within the context of modern technological trends and the cybersecurity risks they face. It covers the latest technological trends in drones and the security threats they encounter in the digital age, including breaches in systems and communications, software attacks, and unauthorized control of drones. This section also examines the security vulnerabilities that attackers could exploit for malicious purposes and the impact of these threats on public safety.

The second section explores the management of cybersecurity risks that threaten drone security by investigating innovative technical solutions aimed at enhancing drone security. These solutions include the application of artificial intelligence, advanced encryption techniques, and early attack detection systems. This section also addresses the role of international and local legislative and regulatory frameworks in ensuring the safe use of this technology.

2. Drones in Light of Modern Technological Trends and the Cybersecurity Risks They Face

Unmanned Aerial Systems (UAS), or drones, are among the most significant technological innovations of recent years, revolutionizing various fields, from security and surveillance to transportation and logistics. With rapid technological advancements, the use of drones has become more diverse and widespread, reflecting global trends toward improving efficiency and reducing costs. As drones have become easier and more affordable to purchase, it is generally expected that both private and public usage of drones by individuals, businesses, and governmental authorities will significantly increase in the coming years (Custers, B., 2016). However, despite the many benefits this technology offers, it faces significant challenges, particularly the cybersecurity risks that threaten its security and functionality (National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis (OCIA), 2018). Drones face multiple threats, including cyberattacks such as jamming and hijacking, which could lead to their disruption or misuse for harmful purposes (Yassine Mekdad, et al., 2024). Therefore, it is crucial to examine these modern technological trends within the context of cybersecurity and analyze the associated risks to ensure the safe use of this innovative technology in the future.

2.1. Modern Technological Trends for Drones

Drone software engineering has garnered significant attention, leading to notable advancements. The rapid evolution of drone technology can be attributed to its ability to dramatically improve efficiency and open new opportunities compared to traditional operational methods in several fields. Many advanced technologies, such as artificial intelligence, computer science, and obstacle avoidance technology, have been developed in tandem to enhance drone operations. Drones are equipped with sensors such as accelerometers, gyroscopes, and GPS devices to gather environmental data and adjust flight status. This data is then sent to the simulation unit for decision-making, while the main system controls essential flight functions, including altitude, direction, and speed. The control system incorporates algorithms and methods that ensure flight stability, as well as a communication unit that transmits data between the drone and remote control systems via technologies like radio waves, Wi-Fi, LTE, or military-grade communication systems (Ngoc-Bao-Van et al., 2024, pp. 19-20).

Modern technological trends for drones are evolving rapidly, enhancing their capabilities and expanding their applications across various sectors. Some of the most significant trends include:

-Modern drones are equipped with state-of-the-art technology, with their capabilities continuously improving. Drones are now utilized in a broad range of fields, such as construction, defense, photography, marketing, delivery, agriculture, rescue operations, and entertainment. It is anticipated that drones will soon enter new sectors based on emerging needs (Koç, M. T., 2023, pp. 21-22);

-Drones equipped with thermal sensors represent a major advancement in search and rescue operations, especially in locating individuals trapped under rubble following natural disasters such as earthquakes (Herrera Velasco & Delgado Guevara, 2024). Additionally, drones outfitted with infrared sensors, night vision cameras, and transmitters serve as highly effective tools for providing real-time information on the locations of individuals in challenging and elevated terrains. Furthermore, these drones play a crucial role in monitoring illegal hunting activities by tracking wildlife in forests and protected areas without disturbing the animals (Koç, 2023, pp. 21-22);

-Unmanned Aerial Vehicles (UAVs), also known as drones, have found a wide range of applications due to their affordability, ease of use, vertical takeoff and landing capabilities, and ability to operate in high-risk or difficult-to-reach areas (Quamar, M. M., & al., et. 2023). Among their many uses, drones play a crucial role in ensuring crowd safety during protests, marches, and public events. Drones equipped with high-definition cameras are also successfully used in aerial photography of sporting events. Thermal sensors and gyroscopes, along with their high maneuverability, compact size, and power, improve the accuracy of regional and national weather forecasts by enabling scientists to monitor weather events in detail. Their use is expected to grow in early warning systems and precautionary measures, offering valuable insights into the trajectory of large-scale weather events such as hurricanes (Koç, M. T, 2023, pp. 21-22).

-To enhance agricultural production and optimize food management, the agricultural sector requires an advanced monitoring system based on unmanned aerial vehicles (UAVs) (Gupta, Y., et al., 2022). UAVs offer a unique solution to the problem of damage caused by heavy machinery used in large-scale, efficient, and economical production. This technology is particularly significant within the context of Agriculture 4.0, where Internet of Things (IoT) applications enable the rapid collection of data from expansive agricultural areas through UAVs and unmanned ground vehicles (UGVs). UAVs communicate with one another, improving the ability to map land and execute agricultural operations based on the data collected (Koç, M. T, 2023, pp. 21-22).

-Drones significantly benefit from advanced technologies, which enhance their ability to perform a wide range of tasks with precision and efficiency. Below are examples of how drones leverage cutting-edge technology:

2.1.1. Artificial Intelligence (AI) and Machine Learning

The integration of artificial intelligence (AI) with drones represents a dynamic and promising field of innovation. Originally designed for unmanned aerial operations, drones have undergone significant transformation with the incorporation of AI algorithms. The increasing availability of onboard computational power, combined with continuous improvements in AI algorithms, allows drones to perform tasks that adapt to changing environments and make complex, real-time decisions (Caballero-Martin, D., et al., 2024, pp. 23-24).

Given the limitations of drone resources—such as battery life, payload capacity, energy consumption, weather conditions, data storage, connectivity, and response time—AI algorithms have the potential to process and analyze data in real-time. This enables drones to make informed decisions about optimizing their limited resources. For instance, machine learning algorithms can predict energy consumption patterns and optimize flight paths, thereby extending the drone's range. Additionally, AI's ability to adapt to environmental changes or specific tasks ensures more efficient resource utilization, enhancing the practical applications of drones (Caballero-Martin, D., et al., 2024, pp. 23-24).

In terms of sustainability and energy efficiency, there is an urgent need to develop more efficient, lightweight batteries and explore alternative energy sources to reduce environmental impact. To address these challenges, leveraging AI capabilities is essential. Moreover, from a regulatory standpoint, the collection of big data for AI models presents ethical and legal challenges. Issues surrounding privacy, autonomy in decision-making, and accountability require clear standards and

doi:10.20944/preprints202501.0694.v1

robust regulation to foster trust and interoperability among drone systems. In this regard, AI can help address these challenges by improving fleet coordination, optimizing energy use, and ensuring operational safety (Caballero-Martin, D., et al., 2024, pp. 23-24).

2.1.2. Advanced Communications

Unmanned Aerial Vehicle (UAV) networks and drone communications are emerging research areas that focus on achieving high productivity, long range, and extensive coverage compared to current networks. With autonomous operation potential, drones can be tailored for critical missions. There is growing interest from both industry and academia to integrate UAV systems with traditional networks, focusing on enhancing service quality, deployment strategies, and ensuring reliable communication. Moreover, drones play a crucial role in distributing vital information and extending LTE networks to remote locations. UAVs are expected to be a key component of 5G and beyond deployments, significantly boosting coverage and capacity (Sharma, V., 2019).

Drones offer significant benefits in providing timely services, particularly during or after disasters, by improving communication capabilities for public safety. Wireless communication through UAVs can save lives and protect ecosystems by managing crises effectively (Sharma, V., 2019).

Another example of drone-supported communication is integrated network formations. The coordination between UAVs and wireless sensor networks (WSNs) can support a wide range of civilian and military applications, including search and rescue, navigation, control, and reconnaissance (Sharma, V., 2019).

2.1.3. Energy and Efficient Design

Drone batteries are more than just power sources; they are essential to the drone’s capabilities, whether for aerial photography or critical search-and-rescue operations. Over the years, battery technology has undergone significant advancements, unlocking the full potential of drones. As drones continue to integrate into various sectors, they increasingly rely on Lithium Polymer (LiPo) batteries, known for their light weight and high energy output. These batteries consist of cells with a polymer electrolyte, allowing for higher energy density in a smaller package. Additionally, LiPo batteries are flexible in shape, allowing for customization to fit the varied and compact designs of drones (Shah, K., 2024).

2.1.4. Drones in Smart Agriculture

Advanced drone technologies present significant opportunities to address numerous challenges in agriculture. Key applications include irrigation management and crop monitoring. The first use of aerial vehicles in agriculture dates back to 1921, when the U.S. Department of Agriculture (USDA), in collaboration with the U.S. Army, used aircraft to distribute pesticides. A major event occurred in 2017 in South Africa, where the fall armyworm destroyed over 100,000 hectares of maize in Zambia. The Zambian Air Force assisted the Ministry of Agriculture and Disaster Management by using aircraft to apply pesticides to pest hotspots across the country. Recently, Israel has made significant strides in drone use for agriculture. Initially adopted by the military, drones were quickly embraced by other sectors as their broad applications became evident (Vaheed, M., et al., 2023, pp. 105-106).

Today, agricultural drones enhance crop production and provide valuable insights into disease management through imaging and sensor technologies. They also assist in monitoring irrigation systems and water supplies, helping predict water availability from glaciers. If UAVs and Wireless Sensor Networks (WSN) are widely implemented in the near future, millions of farmers could gain access to real-time data about their farms. This would reduce the need for farmers to spend extensive time collecting data and provide them with early warnings of disasters and weather changes (Vaheed, M., et al., 2023, pp. 105-106).

2.1.5. Drones in Military and Security Fields

Unmanned Aerial Vehicles (UAVs) have been a staple in military operations for years, gaining popularity due to their ability to conduct surveillance, reconnaissance, and strike missions without risking soldiers' lives. These drones are remotely controlled, allowing for prolonged flight times, which makes them ideal for exploratory and monitoring tasks. UAVs are especially valuable for accessing areas that may be too dangerous or unreachable for human soldiers.

Military drones are equipped with specialized features that set them apart from civilian models. For example, they can be outfitted with high-resolution cameras and advanced surveillance systems to gather intelligence on terrain and enemy positions. Some UAVs are also fitted with precision-guided weapons, enabling them to strike specific targets with remarkable accuracy. Despite the numerous benefits they offer in military operations, their use has sparked debates, especially concerning privacy and ethical implications, particularly when military strikes are conducted without direct human intervention. There are also concerns about the security of these drones, as they could potentially be shot down or hacked by adversaries (Márquez Díaz, J. E., 2023, p. 138).

Autonomous drones, viewed as low-cost, high-impact weapons, are expected to revolutionize future battlefields. This evolution calls for a reevaluation of their role in global security, especially as modern warfare continues to evolve, intensifying the arms race in response to emerging military requirements. Additionally, the integration of technologies such as artificial intelligence (AI), the Internet of Things (IoT), and quantum computing is enhancing the autonomy, combat capabilities, and data processing power of these drones (Márquez Díaz, J. E., 2023, p. 138).

2.1.6. Swarming Technology

Drone swarms are advanced, information-dependent weapons designed to operate in diverse environments, including land, sea, air, and space. A fundamental characteristic of these swarms is their reliance on stable communication links and efficient data processing to achieve coordinated objectives. The effectiveness of a drone swarm stems from its ability to exchange information, with key advantages derived from three core factors: size, customization, and diversity. Each of these factors necessitates precise information management. Larger swarms, equipped with more sensors and munitions, possess greater capabilities for executing large-scale collective attacks. In contrast, more agile swarms can adapt and form smaller, focused units for precise strikes. Additionally, diverse swarms can integrate various sensors and munitions, improving coordination across multiple domains, but this integration also introduces coordination challenges. These capabilities enable new tactical approaches, such as concentrating fire on specific targets or quickly reconfiguring to counter a threat, all of which require robust and efficient communication for success (Kallenborn, Z., 2022, pp. 87-88).

Drone swarms have already proven their presence on modern battlefields. For instance, in the 2021 conflict between Israel and Gaza, the Israeli military became the first to deploy a swarm of drones in active combat. Similarly, during the ongoing conflict between Russia and Ukraine, Russia introduced the "Kalashnikov KUB-BLA" lethal drone munitions, which have the potential to form swarms. Russia also possesses "Lancet-3" munitions capable of creating airborne minefields to target drones and other aircraft. Both the United States and its allies, as well as their adversaries, are heavily investing in the development of swarm technologies. This pursuit is unsurprising, given that drone swarms have numerous applications across all branches of the military, from infantry and logistics support to nuclear deterrence (Kallenborn, Z., 2022, pp. 87-88).

What distinguishes drone swarms from previous technologies is their ability to communicate autonomously, allowing them to adjust their collective behavior based on real-time data collected from sensors on each individual drone. As new information is gathered, the swarm can dynamically adjust its movements or tactics. This responsiveness can either be pre-programmed into the swarm's control system or managed by a single operator, who oversees the swarm as a unified entity. To enhance resilience and reduce vulnerabilities, each drone in the swarm can be programmed to take on “leadership roles,” or the swarm’s behavior may emerge from the decentralized coordination of its members, eliminating the need for centralized command (Lynn, S. K., & al., 2020, p. 3).

Furthermore, drone swarms represent a truly transformative technology. They have the potential to replace humans in hazardous or hostile environments. When deployed in sufficient numbers, they can gather and integrate data from multiple perspectives and locations, generating insights that would be otherwise unattainable. This information can then be used to guide decision-makers who cannot physically access the environment or who require intelligence from a variety of angles and viewpoints (Lynn, S. K., & al., 2020, p. 4).

2.1.7. Drones in Transport and Logistics

The rapid advancements in Unmanned Aerial Vehicle (UAV) technology, commonly known as drones, over the past decade have led to their widespread adoption across various industries. In particular, the logistics sector has increasingly relied on drones, transforming these advanced devices from experimental tools into vital components of modern logistics systems, especially in delivery services. For instance, some countries have integrated drones into last-mile delivery operations to improve efficiency and speed in both urban and rural areas. Amazon, a key player in this technology, has begun delivering parcels across various regions of the United States, including both urban and rural locations. Furthermore, postal services in South Korea are enhancing public delivery systems by testing drones to deliver packages to remote islands facing logistical challenges. Consequently, numerous academic studies have emerged that explore the integration of drones into last-mile delivery. The role of drones in logistics is being increasingly affirmed, not only through their integration with vehicles in last-mile operations but also through innovative models that connect drones with delivery personnel. These transformations have been accompanied by significant advancements in related technologies, such as improved battery life, autonomous mobility, and sophisticated sensing and control systems (Kim, K., et al., 2024, pp. 1-2).

As these trends progress, unmanned aerial vehicles (UAVs) are expected to take on an increasingly diverse and important role in the future, expanding into advanced areas such as artificial intelligence, renewable energy, and sustainable transportation. However, this rapid technological advancement is accompanied by several risks. The primary threat comes from cyberattacks, including jamming, spoofing, and malware. Jamming and spoofing disrupt communication and navigation in UAVs, respectively, while malware infiltrates the UAV’s software, granting unauthorized access and causing system malfunctions. These attacks could also result in the theft of sensitive UAV data or the reverse engineering of its technology. Furthermore, unauthorized surveillance of UAVs and data breaches represent significant privacy threats, as sensitive information is exposed through intercepted data (Malik, S., 2024).

2.2. Cybersecurity Risks of Drones

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have become widely used technologies in both civilian and military sectors. In the civilian realm, their applications include agriculture, logistics, aerial surveillance, forest monitoring, and more. In the military sector, drones are employed for tasks such as surveillance of military zones, combat, intelligence gathering, and bomb detection. Despite their cost-effectiveness and performance advantages, the security of drones remains a significant challenge. Drones are vulnerable to various types of cyberattacks, including eavesdropping, Distributed Denial of Service (DDoS) attacks, and GPS spoofing, all of which threaten the confidentiality, integrity, and availability of data. These attacks can result in data loss, operational disruptions, or even hijacking of the drone (Niyonsaba, S., et al., 2023, p. 688).

With the rapid advancement of UAV technology, ensuring the security and safety of these systems has become crucial. UAVs are exposed to several cybersecurity risks, such as unauthorized access, system takeovers, or manipulation, which threaten both their safety and the integrity of the data they handle. Additionally, these vehicles face challenges due to limited computational resources, wireless communication vulnerabilities, system weaknesses, evolving technical threats, regulatory compliance issues, and human factor influences (Wasswa, S., et al., 2023, pp. 1-2). Below is a summary of some of the key cybersecurity risks:

2.2.1. Attacks on Drone Control and Communication Systems

Communication is a vital component of drone systems, as it facilitates flight control and data transmission. Most drones rely on Wi-Fi to communicate with ground control stations, but the complexity and dynamic nature of these wireless networks can create vulnerabilities, exposing the system to significant risks (Krichen, M., 2022, pp. 5-7).

Moreover, small UAVs, such as quadcopters, heavily rely on GPS for navigation, making them susceptible to GPS signal spoofing attacks. These attacks involve broadcasting counterfeit GPS signals that deceive the drone's GPS receiver into accepting false location data, allowing attackers to redirect the drone to an unintended location, which could result in crashes or hijacking. GPS spoofing can also disrupt the drone's operations entirely, rendering it unable to navigate and exposing it to greater risks (Amrami, D., 2023).

2.2.2. Attacks on Data

Cyberattacks targeting UAV systems primarily focus on three categories of data: confidentiality, integrity, and availability (Benkraouda, H., et al., 2018, pp. 87-89).

-Availability Attacks: These attempts attempt to seize control of the drone or cut off its communication with the Ground Control Station (GCS). In one scenario, an attacker may take control of the drone or the ground station to disable sensors, such as surveillance cameras, or alter the drone's location, thereby corrupting the data and creating a false impression of the environment. In another scenario, the communication link between the drone and the ground station can be severed using techniques like jamming or GPS spoofing, disrupting operations and preventing the transmission of legitimate data. Furthermore, DoS/DDoS attacks can flood the network with fake requests, rendering the system unavailable and preventing the transmission of legitimate data packets. DoS attacks can be carried out through flooding, spoofing, or buffer overflow (Benkraouda, H., et al., 2018, pp. 87-89).

-Integrity Attacks: These attacks involve the modification or replacement of transmitted data with false information. In one example, an attacker might replay previously recorded video to avoid detection. In another scenario, fake sensor data can be generated through a "man-in-the-middle" attack, leading to incorrect decisions by the security team (Benkraouda, H., et al., 2018, pp. 87-89).

-Confidentiality Attacks: These attacks focus on intercepting sensitive data. A passive attack may involve the attacker eavesdropping on communications between the drone and the ground station, such as video streams from surveillance cameras. Alternatively, an active attack might involve intercepting and redirecting data for financial or intelligence purposes, such as selling the intercepted information on the black market (Benkraouda, H., et al., 2018, pp. 87-89).

2.2.3. Software Attacks

Software plays a crucial role in the operation of Unmanned Aerial Vehicles (UAVs) by managing flight operations and controlling the systems connected to the drone. Before each mission, the computer responsible for the UAV exports the necessary data for its operation. The primary security threats in these systems include attacks on drone operators, the Ground Control Station (GCS), drone components, communications, and cloud services. Operators are responsible for controlling the flight, navigation, imaging, or exploration tasks and ensuring the mission's safety. However, they are exposed to threats such as unauthorized access, social engineering, privilege escalation, and insider attacks. The GCS, responsible for mission planning and communication with the drone, is vulnerable to the accidental upload of viruses, which could compromise the drone's security (Veprytska, O., & Kharchenko, V., 2023, pp. 3-5).

Attacks targeting drone components include backdoor attacks, aimed at inserting malicious software into the control system; flooding attacks, which deplete the drone's resources; and selfish node attacks, which harm other drones in the network. Other threats include GPS manipulation (GPS spoofing) and telemetry spoofing, which corrupt data collected from sensors (Veprytska, O., & Kharchenko, V., 2023, pp. 3-5).

Regarding communication, threats include eavesdropping on data transmitted over unencrypted channels, jamming wireless communication channels, and man-in-the-middle (MITM) attacks, where the attacker intercepts and modifies messages. Replay attacks also occur when encrypted messages are intercepted and retransmitted (Veprytska, O., & Kharchenko, V., 2023, pp. 3-5).

When drones communicate with each other, they are susceptible to Sybil attacks, where multiple fake drones are created to control the network, and impersonation attacks, where a malicious drone pretends to be part of the legitimate network. For cloud-to-drone communication, threats include black hole attacks that disrupt communication with the cloud, deauthentication attacks that sever the connection between the drone and the cloud system, and data manipulation during transmission (Veprytska, O., & Kharchenko, V., 2023, pp. 3-5).

Despite advancements in cybersecurity, UAV systems remain vulnerable to various attacks, making it essential to strengthen regulations and security standards to ensure their protection (Veprytska, O., & Kharchenko, V., 2023, pp. 3-9).

2.2.4. Attacks Related to Artificial Intelligence: Vulnerabilities and Attacks on Artificial Intelligence Systems in UAVs

Attacks on AI technology encompass a wide range of threats designed to affect the security and reliability of information systems. These attacks exploit vulnerabilities in AI systems, threatening the confidentiality, integrity, and availability of data. These attacks can be classified into three main types: adversarial attacks, poisoning attacks, and model extraction attacks (Veprytska, O., & Kharchenko, V., 2023, pp. 3-9).

Adversarial Attacks

These attacks aim to cause classification errors by making minimal changes to input data, leading the model to misclassify it.

Poisoning Attacks: These involve introducing malicious samples during the training process, increasing classification errors and reducing model accuracy (Veprytska, O., & Kharchenko, V., 2023, pp. 3-9).

Model Extraction Attacks

These attacks attempt to create a replica of the original model, either for intellectual property theft or to extract the same vulnerabilities present in the original model(Veprytska, O., & Kharchenko, V., 2023, pp. 3-9).

Each of these attacks poses a significant threat to the security and efficiency of unmanned aerial vehicles (UAVs). The UAV system consists of hardware, software, sensors, networks, and communication systems. It has been emphasized that each of these components may be individually vulnerable to cyberattacks. Since these components contain elements of information technology, the cyber threats and attacks we face today also pose a risk to them (Cosar, M. 2022).

To mitigate these risks, various defensive techniques can be employed, such as encryption, authentication, intrusion detection systems, firewalls, machine learning algorithms, and other solutions. Conducting a comprehensive cybersecurity assessment within the UAV sector—studying cyberattacks, defense techniques, and future research trends—is essential. This assessment helps organizations enhance their ability to protect themselves and gain a deeper understanding of emerging threats. It also supports the development and design of effective defense technologies to combat attacks on UAV systems and adapt to evolving threats (Niyonsaba, S., et al., 2023, p. 688).

The field of UAV software engineering faces significant challenges that require interdisciplinary collaboration to overcome. Key issues that need attention include ensuring real-time control, reliable sensor data processing, autonomous decision-making, network security, and improved energy consumption. Furthermore, designing scalable software architectures, conducting thorough testing, ensuring legal compliance, and achieving platform interoperability are critical factors that contribute to the safe and effective adoption and deployment of UAV technology (Ngoc-Bao-Van et al., 2024, pp. 19-20). These are the issues we aim to address in the second section.

3. Managing Cybersecurity Risks Threatening UAV Security

Cybersecurity has become a crucial aspect of our increasingly digital world, impacting various fields and technologies. Among these technologies, Unmanned Aerial Vehicles (UAVs), also known as drones, have emerged as a sophisticated tool with a wide range of applications in surveillance, delivery services, disaster management, and military missions. As UAVs continue to develop and gain greater autonomy, ensuring their cybersecurity has become essential. Cyberattacks pose significant risks to their integrity and functionality. This is why the field of UAV cybersecurity has gained increasing attention in recent years (Wasswa, S., et al., 2023, pp. 1-2). To be effective, UAV cybersecurity requires a comprehensive approach that integrates both legal and technical measures. Addressing these challenges necessitates strategies aimed at protecting systems from potential cyberattacks, whether through the implementation of strict regulations governing UAV use or by adopting advanced technologies to enhance the cybersecurity of these systems.

3.1. Legal Measures for Managing Cybersecurity Risks Threatening UAV Security

In this section, we present examples of legal regulations related to UAVs (drones), with particular emphasis on the legal framework in the United States and the Budapest Convention adopted by the Council of Europe. We will also explore how these models can be used to develop and improve national legislation in other countries (Kutynska, A., & Dei, M., 2023, p. 39).

Among the leading countries in regulating UAV use is the United States, which has implemented comprehensive rules through the Federal Aviation Administration (FAA) to regulate drone operations (Kutynska, A., & Dei, M., 2023, p. 42). In the U.S., the government has issued several laws and directives to address cybersecurity threats to UAVs. For example, the “Drone Cybersecurity Analysis Act” (DETECT Act) requires the National Institute of Standards and Technology (NIST) to develop cybersecurity guidelines for UAVs used by federal agencies. This legislation aims to protect UAVs from cyberattacks and strengthen security standards in this field. UAVs have the capability to collect sensitive information, and with their increasing use, ensuring the security of this technology has become of paramount importance. The DETECT Act seeks to address cybersecurity concerns by directing NIST to develop a set of guidelines. Senator Warner stated, “Drones and unmanned systems have the potential to transform how we operate, manage infrastructure, and deliver life-saving medicines. As the role of drones grows in our society, it’s crucial that we ensure their safety and security. This legislation will provide clear cybersecurity guidelines for drones used by the federal government to protect sensitive information while we continue to invest in this emerging technology.” Senator Thune added, “As drone capabilities evolve and their use grows within both the federal government and the private sector, it’s essential that these systems operate safely. This legislation will require the federal government to follow strict cybersecurity protocols and guidelines for drones and unmanned systems” (McNabb, M. 2024).

The General Data Protection Regulation (GDPR), adopted by EU countries in 2016 and enforced in 2018, also represents a significant advancement in protecting drones by safeguarding the personal data they collect. GDPR is the most significant shift in data privacy regulation over the past two decades, fundamentally transforming how personal data is processed across various sectors, from healthcare to banking, both within the EU and globally (Spalevic, Z., & Vićentijević, K., 2022, pp. 55-56). For the drone industry, GDPR is particularly relevant when drones are used to collect or process personal data, such as through aerial photography, surveillance, and mapping, which may capture identifiable individuals. Compliance with GDPR is essential to avoid hefty fines and to ensure the protection of privacy rights (Stoner, J. 2024)). Additionally, compliance is crucial for safeguarding the data collected by drones against potential cyberattacks.

At the international level, one of the most significant forms of cooperation is the Council of Europe's Convention on Cybercrime (Convention sur la cybercriminalité—Conseil de l'Europe), adopted by the Committee of Ministers of the Council of Europe during its 109th session on November 23, 2001. It was the first international treaty on cybercrime, entering into force on July 1, 2004, and is known as the Budapest Convention. This convention is not limited to Council of Europe member states; it also allows countries outside the Council to sign it, making it an international mechanism to combat crimes committed through or against information technology (Al-Razi, S. M. A., 2019, p. 31). The convention aims to harmonize national laws on cybercrime, enhance national capacities to investigate these crimes, and promote international cooperation. It focuses on gathering digital evidence for various types of crimes, not just cybercrimes (Al-Bidri, A. W., 2021, pp. 105-106). As of 2024, 75 countries have ratified the convention.

The convention was designed to intensify international cooperation and, as a priority, to achieve the common goal of protecting society from cybercrimes by adopting and enhancing appropriate legislation to facilitate effective international cooperation. Although the signing of this convention began in late 2001, it remains the most important treaty in discussions about any international agenda regarding cooperation and the fight against digital crime (Martins dos Santos, B. 2022, p. 4).

The European Convention on Cybercrime marked a pioneering step in international cooperation among nations to address this growing threat. It is still the only agreement of its kind in terms of the number of participating countries and its broad scope (Al-Ashqar Jbour, M., 2016, pp. 106-115). The central principle of this convention is "protecting you and your rights in cyberspace" (Seger, A. 2012). The convention consists of four chapters: (a) terminology, (b) measures to be adopted at the national level, (c) international cooperation, and (d) final provisions. While it was initially discussed and formulated within the context of the Council of Europe, the Budapest Convention has established itself as a primary legal text for international cooperation in prosecuting and preventing cybercrimes (Martins dos Santos, B. 2022, pp. 6-7). The convention classifies internet crimes into four main categories: the first involves crimes against the privacy, integrity, and availability of systems and data; the second includes fraud and forgery; the third covers crimes related to content, such as producing, distributing, and possessing child pornography; and the fourth concerns crimes related to intellectual property rights and associated rights (Al-Ashqar Jbour, M., 2016, pp. 106-115). Based on the outcomes of this convention, it can be considered a successful example of balancing law enforcement with human rights, democracy, and the rule of law. Initially, the Budapest Convention aimed to harmonize cybercrime laws and address the limited number of cross-border investigations into internet crimes and the prosecution of offenders. In recent years, the focus has shifted to addressing challenges in collecting digital evidence (Klynge, C. 2021).

The success of this convention and its protocol is also evident in the participation of many non-European countries, such as the United States, Japan, Australia, South Africa, and Canada. As the convention is implemented in all signatory countries, it becomes a tool for managing cybersecurity risks and threats. The convention's effectiveness lies in its practical measures, which require signatory countries to incorporate them into their national laws (Al-Ashqar Jbour, M., 2016, pp. 106).

International cooperation is also facilitated through other mechanisms, such as cooperation between judicial authorities or via the International Criminal Police Organization (INTERPOL). Various forms of cooperation between police departments have emerged, including the establishment of the International Web Police in 1986 to receive complaints from network users, track down cybercriminals, search for evidence, and bring offenders to trial. Additionally, the Internet Fraud Complaint Center was established in the U.S. in 2000 to collaborate with the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (Al-Ashqar Jbour, M., 2016, pp. 106).

However, these efforts face several challenges. For example, the Budapest Convention has two major limitations: first, its geographic reach, as only 75 countries have ratified it; second, its applicability in the deep and dark web, where forums are specifically designed to facilitate the use of malicious computing tools and services, making it particularly difficult to control misuse (Gery, A. 2018). Moreover, international cooperation in cyberspace is currently limited to addressing cybercrimes and does not extend to tackling state-sponsored cyber threats. Major powers that adopt offensive strategies to meet their goals often do not benefit from framing such attacks, further complicating the regulation of cyberspace (Antar, Y. 2019, pp. 22-23).

The lack of trust between major countries, exemplified by the United States and China, has significantly delayed the conclusion of many international agreements (Abis Nima Al-Fatlawi, A., 2018, p. 105). To overcome these delays in finalizing international agreements, it is important to identify the obstacles to cooperation. These challenges can be summarized as follows: (Suleiman, Q. 2022, p. 21):

-The absence of a unified model for criminal activity, due to differences in legal systems and lack of consensus on the definition of criminal activities, stemming from inadequate legislation that has not kept pace with rapid technological advancements and cybercrime;

-The lack of bilateral or multilateral treaties that allow effective cooperation in the cybersecurity domain. Even when such agreements exist, they often fail to provide the necessary protection.

Countries may manipulate laws to serve their own interests, and international law is often criticized for its lack of clarity and decisiveness. Efforts should be made to improve the outdated legal system to align with developments in cybersecurity, artificial intelligence, and drone warfare (Khan, A. 2023, p. 54). To prevent worsening existing gaps in legal procedures concerning UAVs, adopting innovative and effective technical solutions is essential, which will be discussed in the final section of this article.

3.2. Technical Mechanisms for Managing Cybersecurity Risks Threatening UAV Security

With the rapid pace of technological advancement, Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become integral to various sectors, including security, transportation, agriculture, and photography. As their use expands, significant cybersecurity challenges emerge, with potential risks threatening the stability of these systems and exposing them to increasing cyberattacks. To protect these systems and ensure their security, it has become crucial to implement sophisticated and effective technical solutions. These solutions include leveraging artificial intelligence, blockchain technology, machine learning, fog computing, and encryption to secure data and defend against cyber threats.

3.2.1. Artificial Intelligence (AI) for Threat Detection

In UAV technology development, researchers and engineers have found that integrating AI systems can greatly enhance the autonomy and functionality of these devices. AI empowers UAVs to make decisions based on data analysis from sensors and cameras, optimize flight paths, adapt to environmental changes, and perform tasks autonomously without operator intervention. However, the inclusion of AI in UAVs also introduces new vulnerabilities and risks. According to analysis from “Web of Science” over the past five years, there has been considerable focus on cybersecurity research for artificial intelligence to protect UAV assets. However, studies specifically addressing the safety of UAVs through AI techniques are considerably less frequent (Veprytska, O., & Kharchenko, V., 2024, p. 2).

AI Functions in UAV Systems

UAVs (drones) operate autonomously using various advanced learning algorithms, including supervised and unsupervised learning, reinforcement learning, and federated learning. AI models play a vital role in enhancing UAV performance across a range of operational tasks, as these systems execute diverse functions at multiple levels (Veprytska, O., & Kharchenko, V., 2024, pp. 8-9);

-Optimal Deployment Mission: This involves strategically placing ground stations to minimize energy consumption by UAVs while reducing the load on the Ground Control System (GCS). It also aims to create an organized radio map, especially in areas with complex terrain, to ensure effective network coverage.

-Communication Efficiency Enhancement Mission: This focuses on improving communication between UAVs and base stations, particularly in conditions where wind may affect signal stability. Recurrent Neural Network (RNN) techniques are used to predict the future position and tilt angles of the UAV based on past data.

-Path Loss Prediction Mission: This mission addresses signal loss in wireless communication systems. Algorithms such as "K-Nearest Neighbors" and "Random Forests" are used to predict signal loss based on factors such as distance and elevation angle.

-Anomaly Detection and Monitoring Mission: This mission aims to detect malfunctions or anomalies that may occur during operation by using techniques such as deep learning, image analysis, and GPS data. It also involves using sensors to measure vibrations and temperatures in the UAV's motors, helping to assess its condition and anticipate failures.

-Computer Vision Mission: This enhances the UAV's ability to detect safe landing sites in emergencies and to detect and classify objects in the surrounding environment using visual analysis and imaging technologies.

-Path Planning Mission: Reinforcement Learning (RL) is utilized for path planning in unknown environments, where the UAV learns how to interact with its surroundings through sensor data to achieve its objectives.

-Collision Avoidance Mission: This mission focuses on developing techniques to avoid collisions using technologies such as GPS and sensors like LiDAR, sonar, and radar, enabling the UAV to navigate safely in complex environments.

-Temporary Content Storage Mission: This involves storing data locally on the UAV to facilitate model training, reducing the need for continuous communication with the central network.

-Energy Distribution Optimization Mission: This requires optimizing the use of network resources through comprehensive data analysis, supporting effective decision-making for resource management and task execution within the required timeframe. Federated learning algorithms are used to distribute resources optimally based on the data from each device.

These missions are part of a broad range of applications where artificial intelligence enhances the efficiency of UAVs, making them more adaptable to changing operational environments and technical challenges.

3.2.2. Blockchain Technology for Enhancing UAV Communication Security

Blockchain is a cutting-edge technology designed to store data in a manner that makes modification, corruption, or tampering virtually impossible. It functions as a decentralized digital ledger where transaction records are replicated and shared across a network of computers and devices within a chain of blocks. Each block contains a series of transactions, and when new transactions occur, matching records are added to the local copies of all participants in the network. Distributed Ledger Technology (DLT) refers to a decentralized database managed by a wide range of participants (Krichen, M., 2022, pp. 5-7).

Blockchain has the potential to set new security standards in the UAV industry by addressing critical security challenges. Even if a drone is compromised, the data it holds remains secure due to encryption. Blockchain bolsters UAV communication security across multiple dimensions:

Real-time Location Updates

Blockchain enables continuous updates of a drone's location, providing other drones with real-time positioning information to avoid accidents. It can also update restricted area data in real-time, preventing drones from entering these zones (Krichen, M., 2022, pp. 5-7);

Blockchain-based Identification System

This system tracks the flights of registered drones and generates reports that can be investigated by authorities without compromising the drone owner's privacy. Information marked as confidential is fully protected (Krichen, M., 2022, pp. 5-7);

Encrypted Data Transmission

DLT ensures that data transmitted from drones is encrypted, safeguarding the information and making it suitable for use in sensitive missions and activities (Krichen, M., 2022, pp. 5-7).

Moreover, blockchain offers effective solutions to secure the Internet of Drones (IoD) environment in several ways. It enables the creation of unique digital identities for drones, helping to prevent identity spoofing, while ensuring the confidentiality and integrity of data through advanced encryption and access control mechanisms. The data transmitted is encrypted with sophisticated algorithms, and only entities possessing the correct decryption keys can access the original data. Blockchain also secures communication between drones and control stations, preventing attacks, enforcing strict access control, and improving the system's resilience against security threats (Tychola, K. A., et al., 2024).

However, despite its potential, blockchain technology still faces several challenges, including: (Krichen, M., 2022, pp. 5-7)

-Limited Transaction Capacity: The number of transactions that can be processed per time unit is constrained.

-Limited Scalability: Blockchain systems do not provide the same scalability as centralized systems.

-High Energy Consumption: Blockchain technology requires significant amounts of energy, making it impractical for certain UAV applications.

3.2.3. Machine Learning Techniques to Enhance the Security of Drone Communications: (Krichen, M., 2022, pp. 6-10)

Machine learning is a branch of artificial intelligence that enables computers to learn and improve autonomously, without the need for explicit programming. This field is dedicated to developing software that can independently read and analyze data, then adapt its behavior based on the insights it gains.

Machine learning techniques are applied in various key areas within drone technology, including:

-Reducing Latency and Enhancing Data Reliability: Machine learning techniques are used to optimize data transmission to the cloud, reduce latency, and improve the overall reliability of the process.

-Detecting Denial-of-Service Attacks: Support Vector Machines (SVM) and neural networks are employed to detect denial-of-service attacks through machine learning-based models.

-Identifying Adversaries and Avoiding Malicious Attacks: Machine learning models, particularly Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN), are used to detect adversaries and mitigate the risk of malicious attacks.

-Improving Radar Detection: Machine learning techniques can address issues related to recognition and tracking, enhancing traditional radar detection methods.

-Preventing Privacy Leakage: Recent studies have explored machine learning methods to reduce privacy leakage in drone communications.

3.2.4. Fog Computing Technology to Enhance Drone Communication Security

Fog computing is a distributed computing framework designed to allocate resources such as data and programs across logical locations between the data source and the cloud. Its primary objective is to provide critical analytical services at the network edge, improving performance by positioning computational resources closer to where they are needed, thus enhancing overall network efficiency. Fog computing can also serve security purposes by segmenting bandwidth flow and incorporating multiple firewalls into the network, thereby bolstering security levels(Krichen, M., 2022, pp. 6-10).

Here are some examples of how fog computing can improve drone communication security: (Krichen, M., 2022, pp. 6-10)

-Ensuring Data Privacy: Security operations, including key generation and encryption tasks, are offloaded to more powerful nodes at the network edge.

-Intrusion Detection and Prevention: A system for detecting and preventing intrusions has been introduced, enabling management of "man-in-the-middle" attacks at the fog computing layer.

-Counteracting Threats and Attacks: A fog computing system, leveraging military-grade anti-drone technology, has been implemented to detect jamming and GPS spoofing attacks.

-Latency Reduction: A fog computing solution has been proposed to reduce latency in drone communications, enhancing real-time network speed and responsiveness.

3.2.5. Encryption for Information Security

The core principles of information security revolve around three key concepts: (Aissaoui, R., et al. 2023, pp. 10-11) ;

-Confidentiality: Ensures that unauthorized users cannot access the information.

-Integrity: Ensures the information remains unaltered and uncorrupted during use.

-Availability: Ensures authorized users can access and use the information when needed.

Various methods are available to enhance security in communication links. Since wireless links and the network structure in Unmanned Aerial Systems (UAS) are dynamic, physically securing the links becomes impractical. Therefore, encryption remains the most effective method for securing communication links in these environments.

Encryption technologies have been studied for centuries to ensure information security, leading to the development of proven solutions for data protection. In the field of encryption, four primary properties ensure data security: (Aissaoui, R., et al. 2023, pp. 10-11);

-Confidentiality: Guarantees that only authorized users can access the information.

-Integrity: Verifies that the information has not been altered or corrupted during its use.

-Authentication: Establishes trust in the identities of the parties exchanging the information.

-Non-repudiation: Prevents parties from denying the origin of the information.

When encryption techniques are implemented correctly, using best practices and standards, they ensure that information remains confidential, reliable, and non-repudiable while maintaining its integrity. According to Kerckhoffs's principle, system security should depend solely on the secrecy of the random transactions (the key) rather than the secrecy of the algorithm itself. In fact, all system algorithms should be publicly known, and they should only be used by legitimate users who possess the secret key. The One-Time Pad (OTP) system is the only one that has been proven to be perfectly secure, relying on the use of a random secret key of the same length as the plaintext (which will be encrypted) and used only once. However, this system is impractical due to the challenges in transmitting and storing the key. For systems where perfect security cannot be established, the security level is defined by the complexity of the best-known attack against it. For instance, if the best-known attack on an encryption algorithm requires 280 computational cycles, the system's security level is considered 80 bits (equivalent to a system where an attack using brute force would involve an 80-bit key). However, as of 2022, encryption tools providing 80-bit security or less are considered vulnerable to efficient attacks using modern computers(Aissaoui, R., et al. 2023, pp. 10-11).

There are three main types of essential tools in modern encryption: (Aissaoui, R., et al. 2023, pp. 10-11);

-Encryption (Symmetric or Asymmetric): Ensures confidentiality and authentication.

-Hash Functions: Ensure data integrity.

-Digital Signatures: Ensure authentication and non-repudiation.

When these tools are combined, they ensure that all necessary properties for securing any type of information are achieved. For example, a hash-based message authentication code (HMAC) ensures both authentication and integrity, while adding a hash function to an encrypted message guarantees integrity.

Hybrid encryption is a structure that widely incorporates these tools, where an asymmetric encryption algorithm is used to establish a shared key between two entities, providing authentication, and then using this temporary key for communication via symmetric encryption. The initial step in this system, known as the Authenticated Key Exchange (AKE) or Authenticated Key Agreement (AKA), is critical. If this step is compromised, the entire system's security is at risk(Aissaoui, R., et al. 2023, pp. 10-11).

The transition to symmetric encryption offers key advantages: First, leaking the session key does not affect other sessions, meaning that the compromise of a secret key only impacts past and future communications. Second, symmetric encryption is more efficient, faster, and has less impact on bandwidth. The Transport Layer Security (TLS) protocol, which uses this structure, is fundamental to securing internet communications (Aissaoui, R., et al. 2023, pp. 10-11).

4. Conclusion

In conclusion, cybersecurity challenges for unmanned aerial vehicles (UAVs) remain a critical issue in the rapidly evolving digital age, as these aircraft face a range of cyber threats that could impact their security and core functions. Despite the availability of advanced technical solutions, such as sophisticated encryption and the use of artificial intelligence, there is still an urgent need for clear and comprehensive legal and regulatory frameworks. Governments and organizations must establish legal structures that protect UAV data and define legal responsibilities in the event of breaches or cyberattacks. Additionally, fostering cooperation among various stakeholders through both international and local laws is crucial to ensuring the security of these systems.

This study highlights the security vulnerabilities in UAV systems, stressing the importance of implementing comprehensive security measures. These should focus on strengthening encryption, securing communication channels, ensuring the security of software and firmware, and adhering to established standards and regulations. By combining these technical measures with robust legal and regulatory frameworks, the protection of UAVs from increasing cyber threats can be significantly enhanced, ensuring their safe and reliable use across various sectors. Effectively addressing these challenges requires an integrated approach that combines advanced technological solutions with effective legislation, which will contribute to the continued security and protection of UAVs in the future.

5. Research Findings

The key findings of this research are as follows:

-Reliance on AI and Machine Learning Technologies for Real-Time Anomaly and Intrusion Detection: These technologies enhance security in sensitive environments, such as military surveillance, and are essential for providing an immediate and effective response to cyberattacks;

-Development of Secure Wireless Communication Protocols for UAVs: It is critical to ensure reliable and secure communication, even in hostile environments, protecting UAVs from interception and jamming;

-Development of Resilient UAVs: These UAVs should be capable of autonomously adapting to and mitigating cyberattacks, ensuring operational continuity in emergency situations such as search and rescue missions;

-Need to Strengthen Encryption and Authentication Protocols: Enhancing these protocols is essential to secure communication channels and protect UAVs from cyberattacks;

-Regular Software Updates and Secure Coding Practices: These practices help reduce vulnerabilities and improve the overall security of UAVs;

-Threat Intelligence and Forensic Investigations: These efforts contribute to proactive defense against cyberattacks and provide valuable insights for post-attack analysis and recovery;

-Enhancing Physical Security of UAVs: Implementing tamper-resistant technologies and access control measures can prevent unauthorized tampering with the UAVs;

-Compliance with Security and Legal Standards: Adherence to security standards and legal regulations is essential to protect UAVs, ensure their integration with existing security systems, and foster public and regulatory trust while reducing risks;

-Raising Awareness Among Operators About the Risks of Cyberattacks: Training programs and awareness campaigns should be implemented to ensure that operators follow safe and effective practices;

-Monitoring Internal Activities and Preventing Potential Threats from Authorized Personnel: It is crucial to monitor internal activities and prevent threats that may arise from within the organization or from authorized individuals.

References

References

1. Aissaoui, R., et al. (2023, February 28). A survey on cryptographic methods to secure communications for UAV traffic management. *ENAC, French Civil Aviation University, Toulouse, France.* (pp. 10-11) Retrieved from https://doi.org/10.1016/j.vehcom.2023.100661.
2. 2-Benkraouda, H., et al. (2018). Cyber-attacks on the data communication of drones monitoring critical infrastructure. *Academy & Industry Research Collaboration Center (AIRCC)*, (pp.87-89). Retrieved from https://doi.org/10.5121/csit.2018.81708 .
3. Caballero-Martin, D., et al. (2024). Artificial intelligence applied to drone control: A state of the art. *MDPI*. (pp. 23-24). Retrieved from https://tinyurl.com/3m9rrrzs.
4. Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, (p.264). Retreived from https://tinyurl.com/ycxmc2m4
5. Custers, B. (2016). Flying to new destinations: The future of drones. *In The future of drone use: Opportunities and threats from ethical and legal perspectives* (Chapter 19, p. 370). Springer. https://doi.org/10.1007/978-94-6265-132-6.
6. Grigore, L., & Cristescu, C. (2024). The use of drones in tactical military operations in the integrated and cybernetic battle field. *Land Forces Academy Review, 29(2)*, (pp.269–273). Retrieved from https://doi.org/10.2478/raft-2024-0029
7. Gupta, Y., et al. (2022, February 16). DRONES: The smart technology in modern agriculture. *SSRN*. https://tinyurl.com/69yx43rt
8. Herrera Velasco, J. A., & Delgado Guevara, H. S. (2024). Development of UAVs/drones equipped with thermal sensors for the search of individuals lost under rubble due to earthquake collapses or any eventuality requiring such capabilities. *International Council of the Aeronautical Sciences*, (p.1). Retreived from https://tinyurl.com/29jjwc3b
9. Kallenborn, Z. (2022, May). InfoSwarms: Drone swarms and information warfare. *The US Army War College Quarterly Parameters*, (p.87-88). Retrieved from https://doi.org/10.55540/0031-1723.3154.
10. Khan, A. (2023). The ambiguity in international law and its effect on drone warfare and cyber security. *Western University*. (p.54). Retrieved from https://tinyurl.com/4arca62x.
11. Kim, K., et al. (2024). Drone-assisted multimodal logistics: Trends and research issues. *Drones*, 8(12), 757. (pp. 1-2). Retrieved from https://doi.org/10.3390/drones8120757.
12. Klynge, C. (2021, 16 novembre). Cooperating against cybercrime: 20 years on from the Budapest Convention. Retrieved from https://tinyurl.com/4hcez787.
13. Koç, M. T. (2023). Drone technologies and applications. In Drones—*Various applications* (p. 1). Retrieved from https://bit.ly/4g6DZtU

14. Kutynska, A., & Dei, M. (2023, March). Legal regulation of the use of drones: Human rights and privacy challenges. *Journal of International Legal Communication*, (p.39). Retrieved from https://tinyurl.com/5c2efpu9.
15. Lynn, S. K., & al. (2020, May). Drone swarms: A transformational technology. *ResearchGate*, (p.3). Retrieved from https://tinyurl.com/2s4jxjme
16. Malik, S. (2024, August 1). Security of unmanned aerial vehicle systems through advanced penetration testing. *TechRegsiv*,(p. 5). Retreived from https://tinyurl.com/ch9c3jmt.
17. Majeed, R., et al. (2021). Drone security: Issues and challenges. *International Journal of Advanced Computer Science and Applications*, *12*(5), 720. Retreived from https://doi.org/10.14569/IJACSA.2021.0120584
18. Márquez Díaz, J. E. (2023, June 21). Technological developments and implications of autonomous military drones: Prospects in global geopolitics. *Revista Tecnológica ESPOL—RTE*, (p.138). Retrieved from https://tinyurl.com/yehvyfm2.
19. Martins dos Santos, B. (2022, May). Budapest Convention on Cybercrime in Latin America: A brief analysis of adherence and implementation in Argentina, Brazil, Chile, Colombia, and Mexico. *Derechos Digitales América Latina* (English Translation: Gonzalo Bernabó), (p.4). Retrieved from https://tinyurl.com/32sd9nej.
20. McNabb, M. (2024, March 27). Clarifying cybersecurity guidelines for drones: The DETECT Act. *DroneLife*. Retrieved from https://tinyurl.com/4avjsxpz.
21. National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis (OCIA). (2018, May 22). Cybersecurity risks posed by unmanned aircraft systems. *Homeland Security Digital Library*. https://www.dhs.gov/sites/default/files/publications/uas-ci-drone-pocket-card-112017-508
22. Ngoc-Bao-Van, et Al. (2024). Recent development of drone technology software engineering: A systematic survey. *IEEE Access,* (pp.*19-20*). Retrieved from https://doi.org/10.1109/ACCESS.2024.3454546.
23. Niyonsaba, S., et al. (2023). A survey on cybersecurity in unmanned aerial vehicles: Cyberattacks, defense techniques, and future research directions. *International Journal of Computer Networks and Applications (IJCNA)*, 10(5), (p.688). Retrieved from https://doi.org/10.22247/ijcna/2023/223417
24. Quamar, M. M., & al., et. (2023, October 20). *Advancements and applications of drone-integrated geographic information system technology—A review*. MDPI. Retreived from https://doi.org/10.3390/rs15205039
25. Restas, A. (2015). Drone applications for supporting disaster management. *World Journal of Engineering and Technology*, *3*(3), (p.316-321). Retrieved from https://doi.org/10.4236/wjet.2015.33C047
26. Seger, A. (2012, 16 février). The Budapest Convention on Cybercrime: A framework for capacity building. *Global Forum on Cyber Expertise.* Retrieved from https://rm.coe.int/16802fa3e0.
27. Shah, K. (2024, March 8). The evolution and future of drone battery technology. *Drones Technology*. Retrieved from https://tinyurl.com/yhp8bs3v
28. Sharma, V. (2019, February 23). Advances in drone communications, state-of-the-art and architectures. *MDPI*. Retrieved from https://tinyurl.com/57ucd7p3.
29. Spalevic, Z., & Vićentijević, K. (2022). GDPR and challenges of personal data protection. *The European Journal of Applied Economics*, *19*, (pp.55-56). Retrieved from https://doi: 10.5937/EJAE19-36596
30. Stoner, J. (2024, August 27). What is GDPR (General Data Protection Regulation)? *Flyeye*. Retrieved from https://tinyurl.com/25a6kesn
31. 26-Tychola, K. A., et al. (2024). Beyond flight: Enhancing the Internet of Drones with blockchain technologies. *Drones*, *8*(6), 219. https://doi.org/10.3390/drones8060219
32. Vaheed, M., et al. (2023). Drone technology for smart agriculture. In *Emerging trends in biosciences* (pp. 105-106). *InfoCapsule LLP*. https://tinyurl.com/jwc9tyf5.
33. Veprytska, O., & Kharchenko, V. (2023). Analysis of AI powered attacks and protection of UAV assets: Quality model-based assessing cybersecurity of mobile system for demining. *CEUR-WS*, (pp.3-9). Retrieved from https://tinyurl.com/jkkz2ek8.
34. Veprytska, O., & Kharchenko, V. (2024,March 28). Analysis of AI powered attacks and protection of UAV assets: Quality model-based assessing cybersecurity of mobile system for demining. *CEUR-WS*. (p. 2) Retrieved from https://tinyurl.com/jkkz2ek8.
35. Wasswa, S., et al. (2023). Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems*, (p.1-2). Retrieved from https://tinyurl.com/yajf2ft3.

36. Yaacoub, J.-P., et al. (2020, May 8). Security analysis of drone systems: Attacks, limitations, and recommendations. *Internet of Things.* (p. 1). Retrieved from https://tinyurl.com/3632ch5u.

37. Yassine Mekdad, et al., "Exploring Jamming and Hijacking Attacks for Micro Aerial Drones", *arXiv*, 6 Mar 2024 17, link: https://doi.org/10.48550/arXiv.2403.03858

38. Amrami, D. (2023, avril 13). Drones: Sécurité, vulnérabilité, exploitation, sensibilisation et atténuation (Translated by the author). *LinkedIn*. https://bit.ly/4fUPCnV.

39. Krichen, M. (2022). Défis de sécurité pour les communications par drones: Menaces, attaques et contre-mesures possibles(Translated by the author). *HAL Open Science*, (p. 5). https://tinyurl.com/3uv63psu.

40. Gery, A. (2018). Droit international et prolifération des cyber armes (Translated by the author). *Institut Français des Relations Internationales (IFRI)*, 83(2), (p.47). https://tinyurl.com/mtx6w9yb.

41. Al-Ashqar Jbour, M. (2016), Cybersecurity: The Concern of the Era (Translated by the author), *Arab Center for Legal and Judicial Research*. (pp. 106-115). Retrieved from https://tinyurl.com/mrymuhaa

42. Abis, N. F. (2018). Cyberattacks: A Legal Analytical Study on the Challenges of Their Contemporary Regulation (Translated by the author). *Zen Legal and Literary Publications*, p. 105.

43. Al-Radhi, S. M. A. (2019, August). Cybercrime and the Integration of National, Regional, and International Texts (Translated by the author). *Journal of Law and International Business*, Series of Publications and Works of Hassan II University, Morocco, (23), p. 31.

44. Al-Bidri, A. W. (2021). Cybersecurity Strategy: A Case Study of Morocco (Translated by the author). *Journal of Strategic and Military Studies*, Democratic Arab Center for Strategic, Political, and Economic Studies, Berlin, (1st ed.), pp. 105-106.

45. Antar, Y. (2019). Moroccan Digital Security in the Face of Growing Cyberattacks (Translated by the author). *Moroccan Journal of International and Strategic Studies*, (01), pp. 22-23.

46. Suleiman, Q. (2022, May 3). Combating Cybercrime in Light of International Agreements (Translated by the author). *Research Laboratory in Law and Political Science*, Ammar Thliji University, Algeria. (p. 82).Retrieved from https://tinyurl.com/4e8st9zk

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.