Enhancing Cybersecurity for UAV Systems: Implementing NIS2 Provisions for Safe Drone Deployment in Albania

Vilma TOMCO[1], Klorenta PASHAJ[2]
[1] State Authority for Geospatial Information, Tirana, Albania
vimatster@gmail.com
[2] National Cyber Security Authority, Tirana, Albania
klorenta.pashaj@gmail.com

Abstract

Unmanned Aerial Vehicles (UAVs) have become essential tools in both military and civilian applications, from surveillance to infrastructure monitoring. However, their increased use has raised significant cybersecurity concerns, particularly regarding vulnerabilities to cyberattacks such as GPS spoofing, signal jamming, and data link interception. This paper reviews the key cybersecurity challenges facing UAVs and explores mitigation strategies to enhance UAV security, with a focus on potential applications in Albania. Drawing on recent studies, we examine common attack vectors, including man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, and unauthorized data interception. These vulnerabilities pose risks not only to the safe operation of UAVs but also to the integrity of the critical infrastructure they monitor. To address these issues, the paper proposes robust encryption protocols, real-time monitoring systems, and the integration of machine learning-based intrusion detection techniques to safeguard UAV communications and operations. Furthermore, this research highlights the importance of aligning UAV security measures with the EU's NIS2 Directive, offering recommendations on regulatory frameworks tailored to the Albanian context. The findings emphasize the need for a comprehensive approach to UAV cybersecurity, combining technological innovation with stringent regulatory oversight to ensure safe and secure UAV deployment in Albania's rapidly evolving digital landscape.

Index terms: Cybersecurity, GPS spoofing, Intrusion detection, NIS2 Directive, Unmanned Aerial Vehicles (UAVs)

1. Introduction

Unmanned Aerial Vehicles (UAVs), or drones, are gaining widespread use in Albania across sectors such as border surveillance, infrastructure monitoring, and agriculture. Originally developed for military purposes, UAVs are now essential in civilian domains due to their flexibility and cost-effectiveness. However, as UAV deployment grows, so do the associated cybersecurity risks, particularly in critical areas like energy infrastructure inspection and disaster management.

UAVs are vulnerable to a range of cyber threats, including GPS spoofing, signal jamming, and man-in-the-middle attacks, which can compromise their operations. A cyberattack on a UAV system could lead to unauthorized control, service disruption, or data breaches, posing significant risks to national security. Given these challenges, ensuring the security of UAV communication networks and data exchange is crucial for maintaining their integrity and functionality.

The European Union's NIS2 Directive offers a regulatory framework that Albania can align with to strengthen its cybersecurity measures. Although not an EU member, Albania is adapting its cybersecurity policies to meet EU standards, particularly in sectors involving UAV technology. This paper explores how the NIS2 Directive can be applied to enhance UAV cybersecurity in Albania, proposing strategies to safeguard these systems from evolving threats and ensuring their secure deployment in critical sectors.

2. Literature Review

2.1. Overview of Existing Cybersecurity Vulnerabilities in UAVs

The rapid proliferation of Unmanned Aerial Vehicles (UAVs) has created new cybersecurity concerns due to the increasing complexity and connectivity of these systems. UAVs, being cyber-physical systems, operate through interconnected components such as flight controllers, communication links, ground control stations (GCS), and various sensors [1][2]. These systems are prone to cybersecurity vulnerabilities that could be exploited by adversaries. Vulnerabilities in UAV systems can result from weak encryption protocols, unsecured data transmission, and inadequate protection of communication channels (Hartmann & Giles, 2016). These issues are especially problematic in civilian and commercial drones, where security mechanisms are often less robust than in military-grade UAVs [2].

One critical vulnerability lies in the GPS systems that most UAVs rely on for navigation. GPS signals are inherently weak and unencrypted, making them susceptible to spoofing and jamming attacks, which can cause UAVs to lose their way or be redirected by malicious actors [2][3]. Additionally, unencrypted communication links between the UAV and the GCS can expose UAVs to man-in-the-middle (MITM) attacks, where adversaries intercept and manipulate data [2].

Several studies have classified the common cyberattack vectors targeting UAV systems. The most prevalent among these include GPS spoofing, signal jamming, and man-in-the-middle attacks.

2.2. Cybersecurity Threats to UAVs

UAVs, being cyber-physical systems, are highly vulnerable to a variety of cybersecurity threats due to their reliance on real-time communication, navigation systems, and data exchange protocols. These threats can be categorized into several types, each targeting a different component of UAV operations.

GPS Attacks: One of the most common threats to UAVs is GPS-based attacks, which can include GPS spoofing and jamming. In a GPS spoofing attack, the UAV’s navigation system is deceived by broadcasting fake GPS signals, causing the drone to follow incorrect coordinates, potentially leading to crashes or unauthorized redirection. GPS jamming disrupts the communication between the UAV and GPS satellites by overwhelming the signal with noise, making it difficult or impossible for the UAV to navigate properly [2][1]. Since many UAVs rely on GPS for autonomous flight, attacks on these systems pose a significant risk to their operations.

Signal Jamming: UAVs depend on continuous communication with ground control stations (GCS) for command-and-control functions. Signal jamming involves the intentional disruption of these communication links, rendering the UAV unable to receive commands or transmit data back to the control station [3]. This type of attack can lead to loss of control, forcing the UAV into an unplanned landing or causing it to crash. In critical missions, such as search and rescue operations or infrastructure inspections, signal jamming could result in mission failure with potentially life-threatening consequences [2].

Data Interception and Man-in-the-Middle (MITM) Attacks: UAVs frequently transmit sensitive data, including real-time video feeds and telemetry information. In a data interception attack, adversaries capture these data transmissions, potentially gaining access to critical information such

as live video feeds or flight paths [2]. MITM attacks occur when an attacker intercepts and manipulates the communication between the UAV and its ground station [2][3]. These attacks can result in the unauthorized control of the UAV, allowing the attacker to issue commands, steal data, or even crash the drone.

Firmware Exploits: Firmware is responsible for the core functions of UAVs, including navigation, communication, and sensor data processing. Exploiting vulnerabilities in UAV firmware can allow an attacker to take full control of the drone's operations [2]. This type of attack is particularly dangerous because it can be difficult to detect and can be performed remotely if the firmware is not adequately secured.

3. Risks Posed to UAVs Used in Critical Infrastructure

The use of UAVs in critical infrastructure, such as energy grids, telecommunications networks, and border surveillance, has increased in recent years due to their efficiency in performing tasks like real-time monitoring, inspection, and data collection. However, the integration of UAVs into these vital sectors introduces substantial cybersecurity risks.

In critical infrastructure, UAVs perform missions where the reliability and security of their operations are paramount. For instance, UAVs are used to inspect power lines, monitor oil pipelines, and survey large areas of land for environmental protection. Any disruption caused by a cyberattack on these UAVs could lead to severe consequences. GPS spoofing or jamming during an infrastructure inspection could cause the UAV to fail in detecting faults in power grids or pipelines, resulting in undetected malfunctions that could escalate into widespread service outages [3]. Similarly, signal jamming during border surveillance could prevent UAVs from transmitting critical data on illegal activities, thereby compromising national security [2].

Moreover, data interception in UAVs used for infrastructure monitoring could lead to unauthorized access to sensitive information, such as energy usage patterns or vulnerabilities in physical infrastructure. This could give adversaries the information needed to carry out further attacks, such as targeting power stations or other key facilities [3]. The hijacking of UAVs used for critical infrastructure monitoring could also allow attackers to steal or destroy equipment, further disrupting services.

3.1. Real-World Incidents and Case Studies Relevant to These Threats

Several real-world incidents demonstrate the severity of cybersecurity threats to UAVs. One notable case occurred in 2011, when Iranian forces reportedly used GPS spoofing to capture a U.S. military UAV, the RQ-170 Sentinel, by tricking it into landing in hostile territory [2]. This incident highlights the vulnerability of even military-grade UAVs to GPS-based attacks and underscores the importance of securing navigation systems.

Another incident occurred in the United Kingdom, where signal jamming disrupted the operations of commercial UAVs used for surveying during the construction of a railway. The jamming not only caused delays in the project but also posed safety risks, as the UAVs lost communication with their operators and became uncontrollable [3]. This case illustrates how jamming attacks can affect UAV operations in civilian contexts, leading to both operational and safety concerns.

In a more recent example, researchers demonstrated the possibility of MITM attacks on civilian UAVs by intercepting and manipulating the communication between a drone and its controller [2]. The attackers were able to take control of the drone, alter its flight path, and access the video feed without the operator's knowledge. This case study exemplifies the growing threat of data interception and manipulation in the civilian UAV market, where encryption and secure communication protocols are often not as robust as in military applications.

These incidents highlight the pressing need for stronger cybersecurity measures in UAV systems, particularly in critical infrastructure and sensitive operations. The vulnerabilities exposed by these real-world attacks emphasize that UAV cybersecurity should be a top priority for both regulatory bodies and UAV operators. As Albania and neighboring countries increase their reliance on UAV technology in critical sectors, addressing these threats through effective mitigation strategies becomes essential to ensure the security and resilience of UAV operations.

3.2. Mitigation Strategies

To address these vulnerabilities, researchers have proposed several mitigation strategies aimed at strengthening UAV cybersecurity. Some of the key measures include:

Encryption Protocols: One of the most widely recommended solutions for enhancing UAV security is the implementation of strong encryption protocols for both GPS signals and communication links. By encrypting these data streams, attackers are less likely to intercept and manipulate critical information [1][2]. For instance, military-grade UAVs often use encrypted GPS signals to protect against spoofing, a practice that could be extended to civilian UAVs operating in sensitive areas.

Real-Time Monitoring and Intrusion Detection Systems (IDS): Advanced real-time monitoring systems combined with machine learning-based intrusion detection systems (IDS) have been proposed as effective ways to detect abnormal activities in UAV operations. These systems can monitor UAV behavior in real-time, flagging any deviations from expected patterns that may indicate an ongoing attack [2][3]. Implementing IDS in critical sectors where UAVs are used, such as border surveillance and infrastructure monitoring, can provide an early warning against cyber threats.

Resilient Communication Protocols: Some researchers have explored the use of resilient communication protocols, such as Frequency Hopping Spread Spectrum (FHSS), to defend against jamming and MITM attacks. FHSS changes the communication frequency rapidly, making it difficult for adversaries to jam the signal or intercept data [2][3]. Additionally, fail-safe mechanisms such as autonomous return-to-home functions can mitigate the impact of communication loss [1].

Authentication and Access Control: Strengthening authentication mechanisms for UAV systems, particularly for civilian and commercial drones, has been highlighted as a key strategy in the literature. Multifactor authentication, as well as cryptographic keys for UAV operators, can significantly reduce the likelihood of unauthorized access [3].

As UAVs become integral to critical infrastructure and civilian applications, the need for robust cybersecurity measures grows exponentially. The complexities of UAV systems, combined with their vulnerability to cyberattacks, have prompted the development of multiple mitigation strategies aimed at securing their operation. This section outlines key strategies, including encryption protocols, real-time monitoring, machine learning-based threat detection, incident response mechanisms, and UAV-specific cybersecurity frameworks and best practices.

Encryption Protocols and Secure Communication Techniques

One of the most critical defense mechanisms against cyberattacks on UAVs is the implementation of strong encryption protocols. These protocols ensure that communication between UAVs and their ground control stations (GCS) is secure, protecting data from interception and unauthorized access. End-to-end encryption of data transmission is vital in preventing man-in-the-middle (MITM) attacks, where attackers intercept and manipulate communication between UAVs and operators [1][2]. Encryption ensures that even if an attacker intercepts the communication, the data remains unreadable without the appropriate decryption key.

For GPS systems, which are prone to spoofing attacks, the use of cryptographically secure GPS signals can provide additional protection. While such encryption is more commonly used in military applications, extending its use to civilian and commercial UAVs operating in critical sectors could

significantly reduce the risk of GPS spoofing [2]. Additionally, secure communication techniques such as Frequency Hopping Spread Spectrum (FHSS) can help mitigate signal jamming by changing the communication frequency at rapid intervals, making it difficult for attackers to jam the signal [3].

The integration of Public Key Infrastructure (PKI) in UAV communication channels can further strengthen authentication mechanisms. PKI ensures that only authorized operators can access and control UAV systems, using cryptographic keys to verify the identity of both the UAV and the operator [3].

Real-Time Monitoring and Machine Learning for Threat Detection

The dynamic nature of UAV operations requires continuous monitoring to detect potential security breaches in real time. Advanced Intrusion Detection Systems (IDS), when integrated with UAV systems, can provide real-time threat detection by monitoring communication patterns, flight data, and system behavior for anomalies. IDS systems are particularly effective when combined with machine learning (ML) algorithms, which can learn from historical data and improve their ability to detect suspicious activities over time [2].

Machine learning-based threat detection has the advantage of being adaptive and responsive to evolving attack methods. ML algorithms can analyze vast amounts of data generated by UAV operations, identifying deviations from expected behavior that may signal a cyberattack. For instance, if a UAV's flight path is suddenly altered without input from the operator, or if communication latency increases unexpectedly, the IDS can flag these events as potential threats [2][3]. Such systems can also predict future vulnerabilities by analyzing patterns from previous attacks, allowing for preemptive countermeasures to be implemented.

Moreover, UAV systems equipped with real-time monitoring can automate certain security responses, such as switching communication channels in case of jamming or initiating a return-to-home sequence if a security breach is detected [4]. These proactive defense mechanisms minimize the time between detecting an attack and responding to it, reducing the potential damage.

Incident Response Strategies for Compromised UAVs

Given the critical functions that UAVs perform, especially in sectors like energy, telecommunications, and border security, having a well-structured incident response strategy is essential. Incident response for UAVs involves not only addressing immediate threats but also ensuring the continuity of operations with minimal disruption.

In the event of a cyberattack, such as a signal jamming or a MITM attack, the UAV must be equipped with predefined fail-safe mechanisms. For example, many UAVs are designed with an autonomous return-to-home function that activates when communication with the ground station is lost [1]. This mechanism ensures that the UAV returns to a designated safe location rather than being lost or hijacked. Furthermore, UAVs should have redundant communication channels, allowing operators to regain control if the primary communication link is compromised [3].

In the case of a more severe compromise, such as a successful MITM attack where the UAV has been hijacked, it is essential to have an immediate shutdown protocol. This would involve remotely disabling the UAV to prevent the attacker from using it for malicious purposes. Additionally, a robust forensic analysis should be carried out post-incident to determine the nature of the attack, assess damage, and implement corrective measures to prevent future breaches [2].

Incident recovery should also include a comprehensive review of the security protocols and systems in place, ensuring that any vulnerabilities are patched before the UAV is redeployed. Continuous updates to the UAV’s firmware and software are crucial in mitigating known vulnerabilities [2].

4. UAV-Specific Cybersecurity Frameworks and Best Practices

The increasing reliance on UAVs in critical infrastructure necessitates the development of UAV-specific cybersecurity frameworks. These frameworks provide a structured approach to UAV security, covering all aspects of their operation, from pre-flight to post-flight procedures. A comprehensive UAV cybersecurity framework should include guidelines on secure system design, regular maintenance, and operational best practices.

One of the primary components of such a framework is the enforcement of cyber hygiene practices for UAV operators. This includes ensuring that UAVs operate on updated software, that encryption keys are regularly rotated, and that strict access control measures are implemented [3]. Security audits should also be a routine part of UAV operations, with periodic checks to ensure compliance with security standards and regulations.

In line with the European Union's NIS2 Directive, the framework should include specific requirements for cyber resilience, ensuring that UAVs used in critical infrastructure can withstand and recover from cyberattacks. NIS2 provisions advocate for risk assessments, incident reporting mechanisms, and cross-border collaboration in cybersecurity [3]. By aligning with these standards, Albania and neighboring regions can ensure that UAV operations are secure and resilient against evolving threats.

The NIS2 Directive (Network and Information Systems Directive 2), introduced by the European Union, is a regulatory framework aimed at strengthening cybersecurity across critical sectors, including energy, transport, healthcare, and digital infrastructure. It builds on the original NIS Directive, placing greater emphasis on risk management, incident reporting, and cross-border cooperation. NIS2 requires entities in critical sectors to adopt stringent cybersecurity measures, conduct regular risk assessments, and ensure robust incident response mechanisms [3].

Finally, collaborative efforts between government agencies, private industry, and international bodies are critical in developing and enforcing these cybersecurity standards. Sharing threat intelligence, best practices, and new technologies can enhance the overall security of UAV operations across borders [3]. As UAV usage grows, especially in sensitive sectors, the implementation of these frameworks and best practices will be crucial in safeguarding operations and ensuring the security of critical infrastructure.

Current Adoption of UAVs in Albania and Neighboring Regions

In Albania, the adoption of UAVs has increased significantly, particularly in areas such as environmental monitoring, border security, and critical infrastructure inspections [2][1]. These UAVs are often used by government agencies, private companies, and research institutions to monitor large areas that would otherwise be difficult to reach. For instance, UAVs play an important role in surveillance missions along Albania's extensive coastal borders, aiding law enforcement in detecting illegal activities such as smuggling [2].

However, the increasing reliance on UAV technology brings with it the growing concern of cybersecurity threats, especially in sectors such as energy infrastructure and border control, where drones play a critical role [3]. Neighboring regions, such as Kosovo and North Macedonia, have similarly adopted UAV technologies in various sectors. As a result, Albania and its neighbors face shared challenges in securing UAV operations, especially given the regional focus on enhancing critical infrastructure protection under EU directives such as NIS2[3]. Albania's increasing integration with EU cybersecurity frameworks, including NIS2 provisions, presents an opportunity to build a robust cybersecurity posture for UAV systems, ensuring their secure deployment across key sectors.

After 50 years of communism, Albania has made substantial strides in building a multi-party democracy, establishing a market economy, and strengthening the rule of law. From 1990 to 2022,

the country has seen steady economic growth, with an average annual growth rate of 3.8%. Under the 2021-2025 Governing Program, the Albanian Government has committed to accelerating the country's EU integration process. A key development area in the 2021-2024 program is the creation of a "Digital Society" aimed at modernizing electronic systems in various sectors, including geospatial information, to enhance services for citizens and businesses. The Albanian Government has identified ICT infrastructure modernization as a priority over the last 12 years, and one of the steps taken in this direction was the establishment of the National Spatial Data Infrastructure (NSDI) under Law 72/2012. This law established the State Authority for Geospatial Information (ASIG) as the NSDI Administrator and National Mapping Authority for Albania. In 2020, the Government approved the "Geospatial Information Governance Policy for Albania, 2020-2030," recognizing ASIG's central role in managing the geoinformation system in Albania.

4.1. Remote Sensing Project

One of the core measures in this policy document is the increased use of Remote Sensing technology by government agencies to monitor and accurately plan territorial development. ASIG has been designated as the authority responsible for establishing the Remote Sensing Monitoring Center, which will handle processing, analyzing, and disseminating geospatial data generated by national remote sensing projects. Currently, two important projects are underway:

1. Satellite Service for Territorial Monitoring

This project uses advanced satellite technology to monitor Albania and is expected to continue until 2025. The Government of Albania has contracted Satellogic, an American company, to provide exclusive operational satellite services for three years. These satellites will capture multispectral stereoscopic imagery at 70 cm resolution and hyperspectral imagery at 25 m resolution. ASIG's Remote Sensing Monitoring Center will process this data into geospatial products such as orthoimagery, digital elevation models, and thematic maps, which will support local and central government authorities in:

- Emergency response to natural disasters
- Urban development and monitoring
- Environmental protection
- Tourism development
- Agriculture

2. Purchase of UAV Drones

Albania has also acquired a fleet of UAVs (Unmanned Aerial Vehicles) through a strategic partnership with Turkey, as part of the modernization efforts of Albania's Armed Forces within NATO. Besides national security applications, the UAV project will also serve civilian monitoring needs. ASIG contributed to the technical specifications and will receive an aerial photogrammetric camera with a resolution of 4 cm/pixel, mounted on the UAV, to capture high-resolution imagery. Like the satellite data, these UAV images will be processed by ASIG to produce high-accuracy geospatial data, such as orthoimagery and digital terrain models. This data can also be used for producing topographical base maps, thanks to expertise gained from a previous JICA-supported project, "Geospatial Information for Sustainable Land Development in the Tirana-Durres Zone" (2017-2019). Combined with satellite data, this imagery will support:

- Detailed urban planning
- Engineering projects
- Enhancing the Land Information System

Albania is also focusing on strategic satellite services, including the Albania 1 and Albania 2 satellites, for monitoring, geospatial data processing, and informed decision-making. ASIG, a part of

the Copernicus Relay network, actively promotes Copernicus Open Data, highlighting its benefits for local communities and businesses. ASIG is also running campaigns to raise awareness and improve public institutions' capabilities in utilizing satellite services.

Albania's comprehensive geospatial framework, established under Law No. 72/2012 [5], was recently updated by the Parliament on September 19, 2024, to fully align with the EU's INSPIRE Directive (2007/2/EC) [6]. This legislation regulates the creation, management, and use of geospatial data to facilitate effective data sharing among public authorities. The 2020-2030 National Policy on Geospatial Information sets strategic goals to improve access to, use of, and governance of geospatial information across Albania

4.2. How the NIS2 Directive Can Guide UAV Cybersecurity in Albania

Although Albania is not an EU member, it has demonstrated efforts to align with EU cybersecurity frameworks, including the NIS2 Directive [7], as it aspires to join the Union. The NIS2 provisions can serve as a valuable guide for establishing UAV cybersecurity standards in Albania, particularly for UAVs used in critical sectors such as border surveillance and energy infrastructure monitoring [3]. By adopting NIS2's risk management approach, Albania can enforce stricter controls on UAV operations, ensuring that vulnerabilities are addressed proactively, and incidents are reported promptly.

To align with EU standards, Albania should prioritize updating its cybersecurity legislation to incorporate NIS2's key provisions. This includes implementing mandatory risk assessments for UAV operators, requiring incident reporting within specified timeframes, and enforcing penalties for non-compliance. Additionally, Albania should foster cross-border collaboration with neighboring EU countries, sharing best practices and threat intelligence to enhance the resilience of its UAV cybersecurity posture [3].

A secure UAV cybersecurity framework for Albania should include several critical elements:

- Encryption protocols for secure communication between UAVs and ground control systems.
- Intrusion detection systems (IDS) and machine learning-based threat detection for real-time monitoring.
- Incident response strategies, including fail-safe mechanisms like return-to-home and automatic shutdown protocols in case of security breaches [2].
- Periodic security audits to ensure compliance with cybersecurity regulations.

Recommendations for Policy-Makers and Regulatory Bodies

Albanian policy-makers should:

- Mandate risk assessments for UAV operators in critical sectors.
- Establish penalties for non-compliance with cybersecurity standards.
- Encourage the adoption of best practices for UAV cybersecurity, such as strong encryption and secure communication protocols [3].
- Foster public-private partnerships to share threat intelligence and develop industry-specific guidelines.
- Integration of Best Practices and Alignment with the NIS2 Directive

By integrating best practices from the NIS2 Directive, Albania can ensure its UAV operations are secure and resilient. This includes adopting multi-factor authentication for UAV systems, ensuring that UAV operators are adequately trained in cybersecurity protocols, and requiring regular updates to software and firmware to address known vulnerabilities [2] [3].

5. Conclusion and Future Directions

This paper has highlighted the key cybersecurity challenges faced by UAVs, including GPS spoofing, signal jamming, and data interception. Effective mitigation strategies, such as encryption, real-time monitoring, and incident response mechanisms, are critical to ensuring the secure operation of UAVs in Albania. The NIS2 Directive offers a robust framework for guiding UAV cybersecurity, which Albania can leverage as it aligns with EU standards [2][3].

Future challenges for UAV cybersecurity in Albania include keeping pace with evolving threats and integrating emerging technologies like artificial intelligence for autonomous threat detection. Additionally, there is a need for increased investment in cybersecurity infrastructure to support UAV operations in critical sectors. As UAV usage expands, maintaining regulatory compliance and incident reporting will become more complex [3].

International cooperation will play a crucial role in securing UAV systems, as threats are often transnational. Albania should continue to collaborate with EU member states and regional partners to share intelligence, harmonize regulations, and strengthen its cybersecurity ecosystem. Evolving regulatory frameworks, such as the NIS2 Directive, will provide valuable guidance as Albania works to enhance its UAV cybersecurity measures and ensure safe and secure UAV deployment in critical sectors [3].

References

[1]. Costa, D. G., Bittencourt, J. C. N., Oliveira, F., Peixoto, J. P. J., & Jesus, T. C. (2024). Achieving sustainable smart cities through geospatial data-driven approaches. Sustainability, 16(640).

[2]. Dahlman, E., & Lagrelius, K. (2019). A game of drones: Cyber security in UAVs (KTH Bachelor Thesis Report). KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science.

[3]. Hartmann, K., & Giles, K. (2016). UAV exploitation: A new domain for cyber power. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), 2016 8th International Conference on Cyber Conflict (pp. 205-215). NATO CCD COE Publications

[4]. Sanghavi, P., & Kaur, H. (2023). *A comprehensive study on cyber security in unmanned aerial vehicles*. 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom).

[5]. "Law No. 72 of 28.6.2012." Accessed: Oct. 21, 2024. [Online]. Available: https://sane27.com/wp-content/uploads/Law-no.72-of-28.6.2012.pdf

[6]. "INSPIRE Directive." Accessed: Oct. 21, 2024. [Online]. Available: https://knowledge-base.inspire.ec.europa.eu/legislation/inspire-directive_en

[7]. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)." Accessed: Oct. 21, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555