Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining

Olena Veprytska[1,*,†], Vyacheslav Kharchenko[1,†]

[1] National Aerospace University KhAI, 61070, Kharkiv, Ukraine

Abstract

The research focuses on methods of assessing and providing cybersecurity methods for unmanned aerial vehicles (UAVs) considering AI-powered means. This article analyzes the primary threats and attacks against UAVs and AI in UAV systems, identifying key vulnerabilities and limitations of AI usage. Based on this analysis, a classification of countermeasures at both regulatory and technical levels has been developed, taking into account the AI aspect in UAVs for both attack and defense purposes. Examples of profiling AI quality models for UAV systems are presented as a means of AI standardization. Case study describes building a quality model and results of IMECA analysis to assess AI-based on-board systems and protection means for UAVs applied in intelligent mobile systems for humanitarian demining.

Keywords

UAV, artificial intelligence, security, safety, attacks, countermeasures, humanitarian demining

1. Introduction

1.1. Motivation

The use of modern UAVs encompasses various applications that can be divided into civil, military, and commercial sectors. In the civil sector, UAVs have found their place for [1, 2] disaster management, in agriculture, healthcare, for building inspections etc. In the military domain, UAVs play a critical role, becoming effective means to achieve objectives. In the Russian-Ukrainian conflict, The integration of all types of UAVs can be observed at tactical, operational, and strategic levels considering russian-Ukrainian war [3]. UAV functions include [4] reconnaissance, observation, and target engagement. Commercial use of drones is represented in the form of capturing photos and videos of events, concerts, sports, in the

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.

† These authors contributed equally.

o.veprytska@csn.khai.edu (O.Veprytska); v.kharchenko@csn.khai.edu (V. Kharchenko)

0009-0005-3161-4130 (O.Veprytska); 0000-0001-5352-077X (V. Kharchenko)

entertainment industry, cinematography. Besides legal drone usage, there are countless possibilities for criminal and terrorist use [5], including smuggling, propaganda, and attacks.

According to [6], the size of the global UAV market was estimated at approximately $26.8 billion in 2022, about $30 billion in 2023, and

more than $50 billion by 2032. Despite this impressive growth, it's essential to remember that there are both advantages and disadvantages to UAV usage [7]. One of the main concerns is security. Security is a fundamental aspect that includes measures to protect against data leaks, ensure flight safety, avoid collisions, etc. Additionally, addressing ethical and legal issues related to drone use, such as privacy and airspace access, is crucial. Governments and regulatory bodies are developing relevant standards, safety policies, and legislation to ensure security and safety.

In the development of UAV technologies, researchers and engineers have concluded that adding Artificial Intelligence (AI) systems can significantly improve the autonomy and functionality of these devices. AI allows UAVs to make decisions based on data analysis from sensors and cameras, optimize flight routes, respond to changes in the environment, and perform tasks without operator intervention. However, adding AI to UAVs also introduces vulnerabilities and risks. According to Web of Science indicators analysis for the past 5 years, significant attention is given to researching the cybersecurity of AI, ensuring the protection of UAV assets, but considerably fewer studies focus specifically on UAV safety with AI means (Figure 1).

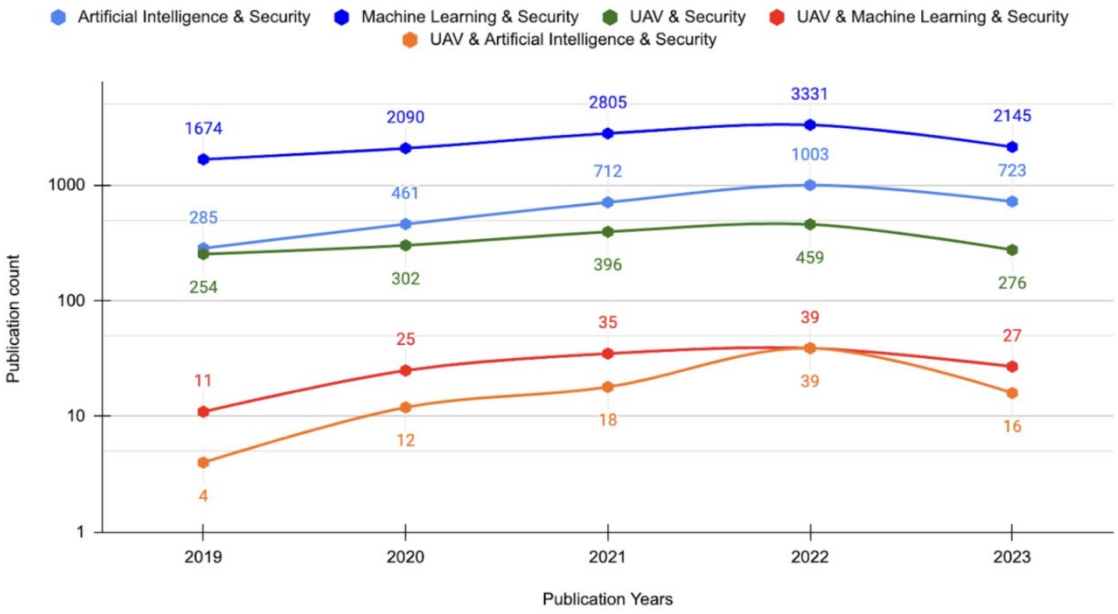


Figure 1: Number of publications on the UAV/AI/Cybersecurity related keywords.

1.2 Objectives and approach

UAVs have become a new field of research and development due to their versatile applications and accessibility. As the use of UAVs increases, concerns about their security and

safety grow. Within the scope of this research, review articles have been examined across various directions: the security and safety of UAVs, the integration of AI in UAVs, and the security and safety of AI. The current work is specifically focused on reviewing sources aimed at analyzing the functions of AI in UAVs, the security and safety of AI technology itself, and existing threats and vulnerabilities to UAV components.

The aim of the research is to analyze possible threats, attacks, interventions, and justify the selection of countermeasures to enhance the cybersecurity of UAV systems considering their vulnerabilities and the use of AI to amplify the power of attacks and protection. The objectives are the following:

- to identify the main barriers to the implementation of AI in UAV systems considering the safety risks of UAV application, technical limitations, and the cybersecurity of UAV systems equipped with AI models taking into account the specific vulnerabilities of technologies and AI components;
- to propose and classify countermeasures considering the aspect of AI; analyze countermeasures at the regulatory and technical levels and provide partial assessments of their impact on the overall risks of cybersecurity and safety;
- to analyze an example of implementing an AI system in UAVs and define requirements from the perspective of using it as a module for performing standard tasks and applying it as a countermeasure to ensure the safety of UAVs.

Approach to research is based on the several principles and previous results [8, 9], in particular:

- Extended set of scenarios for using AI for powering attacks and protection, which were previously considered in [8] for UAV systems;
- Applying the Security Informed Safety methodology and IMECA technique [9] for UAV systems taking into account the features of using AI means;
- Using AI quality models to justify the requirements for AI in UAVs [9] as a function that performs a specific task and AI as a means of protecting UAV assets.

The structure of the paper is as follows: Section 2 analyzes specific security and safety issues for UAVs and systematizes attacks on the vulnerabilities of UAV system components; Section 3 examines the challenges related to the implementation of AI in UAVs, the application options for AI in UAVs, and provides an analysis of AI vulnerabilities and attacks on AI in UAVs; Section 4 presents a taxonomy of possible countermeasures at the regulatory and technical levels; Section 5 describes a case study of building a quality model to assess AI-based on-board systems and protection means for UAVs applied for paramilitary demining; the final Section summarizes and describes directions for future research.

2. Attacks on UAVs

The main security problems in UAV systems involve attacks on drone operators, Ground Control System (GCS), drone components, communication, and cloud services [1, 10-14] presented in Figure 2.

Drone operators are responsible for controlling flight, navigation, executing imaging tasks, or remotely exploring areas, and ensuring flight safety. Threats/attacks on drone operators include unauthorized access, social engineering, privilege escalation, unrestricted administrative capabilities, accidental errors, and insider attacks.

The GCS performs mission planning, communication with the platform, and control functions for payload through communication systems and data transmission lines for interfacing with the airborne platform and its onboard systems. Possible breaches of the GCS include accidental virus infections: sometimes viruses or malicious programs may accidentally be loaded onto the control system, leading to compromising the security of the drone and information.

Components of UAVs can be separately targeted by attacks such as:

- Backdoor Attack: A malicious attack aimed at introducing harmful software into the UAV control system;
- Flooding Attack: An attack where the adversary sends a large number of packets to deplete the resources of the UAV and reduce the network bandwidth;
- Selfish Node Attack: This type of attack in the context of a UAV network involves one drone engaging in malicious actions, consuming more resources than necessary to optimize its own performance, to the detriment of other drones in the network;
- GPS Spoofing: An attack in which the adversary creates interference in the GPS satellite link sensor, generating fake GPS signals with high intensity compared to the original;
- Telemetry Spoofing: A type of cyberattacks in which attackers attempt to create and insert fake telemetry data into the stream of real telemetry data collected from devices or systems interacting with a cloud server or other networked systems.

Communication ensures the transmission and exchange of information among all system components. In the context of UAVs, this includes communication between the GCS and UAVs, UAV and UAV, UAV and Cloud Services. Communication between UAVs and the GCS (D2GS) is often publicly accessible and sometimes unprotected or relies on single-factor authentication, which can be easily compromised. Attacks on D2GS communication include:

- Single Point of Failure (SPOF): A type of cyberattacks aimed at one or several critical components or services in the network that serve as a single vulnerability point for disrupting or causing unavailability of other components of the system;
- Eavesdropping: Attacks where the attacker listens to unencrypted messages through a communication channel, or in the case of an encrypted channel, the eavesdropper aims to intercept and decrypt confidential information later;
- Jamming: Can be created for intentional or unintentional reasons. Jamming attack is a type of security threat in wireless communication where the attacker deliberately transmits interference (jamming signals) on the same frequency as the target communication channel, disrupting the normal functioning of the wireless channel;
- Man in the Middle (MITM): An attack where, unlike eavesdropping, the attacker actively manipulates the message after intercepting it;

- Replay: A type of attack where the attacker intercepts encrypted messages and then replays these messages to another UAV, masquerading as a legitimate sender.

Attacks on communication between UAVs in Drone-to-Drone (D2D) communication include both standard D2GS attacks (Eavesdropping, Jamming, MITM, Replay) and others:

- Sybil Attack: A type of cyberattacks where the perpetrator creates numerous fictitious nodes (in this case, UAVs) used to represent specially crafted false entities in the network. The goal of such an attack is to gain control over the network or inflict a destructive influence on its functioning, maximizing the number of false nodes;
- Impersonation: A threat in which a malicious UAV presents forged data and claims to have been a legitimate part of the network, attempting to gain unauthorized access to the system or resources.

Attacks on communication between the cloud and UAVs include:

- Black Hole Attack: A variant of a denial-of-service attack, where a malicious node pretends to have the fastest path to the cloud server, causing other nodes to route their data through it. The attacker then drops or ignores incoming packets, disrupting the connection between the UAVs and the cloud server;
- Grey Hole Attack: A type of malicious network attack where the attacker gains access to a network device and selectively controls the transmission or blocking of traffic on specific network links for a defined period;
- Deauthentication Attack: An attack initiated by a malicious actor who sends a certain number of deauthentication frames to the UAV and/or cloud system with the aim of disconnecting the UAV from the system;
- Data Tampering during Transmission: Falsification of data during transmission. This data could include session keys, operational information, or sensor readings from the UAV;
- Eavesdropping.

Attacks on cloud services and storage encompass a wide range. Key threats include data tampering and denial of service. To increase the payload capacity of UAVs, some commercial UAVs store data in cloud databases. Any unauthorized alteration of this data can expose personal information or impact the network's operation.

Therefore, despite the development of cybersecurity measures, UAV systems remain vulnerable to a broad spectrum of attacks and require improvements in regulations and standardization of cybersecurity requirements.

Operator	Ground Control System (GCS)	Drone-to-Ground Station (D2GS)	Drone Components	Drone-to-Drone (D2D)	Drone-To-Cloud (D2C)	Cloud Services
Unauthorized Access	Malware Infection	Eavesdropping	GPS Spoofing	Eavesdropping	Data Tampering	Data Tampering
Social Engineering		Jamming Attack	Backdoor	Jamming Attack	Eavesdropping	DoS/DDoS
Privilege Escalation		Man-in-the-Middle Attack	Flooding	Man-in-the-Middle Attack	Black Hole Attack	
Unrestricted Administrative Capabilities		Replay Attack	Selfish Node Attack	Replay Attack	Gray Hole Attack	
Accidental Errors		Single Point Of Failure (SPOF)	Telemetry Spoofing	Sybil Attack	Deauthentication Attack	
Internal Threat Attack (Insider Threats)				Impersonation Attack		

Figure 2: Attacks on UAV System Components.

3. Risk analysis of vulnerabilities, and attacks on AI solutions of UAV systems

3.1 Challenges of applying AI in UAV systems

The integration of AI in UAVs can enhance their efficiency and productivity. Machine learning algorithms enable UAVs to make real-time decisions and find optimal solutions that meet mission requirements. However, the integration of AI in UAVs poses certain challenges and security concerns, making it difficult to achieve complete automation of UAVs.

The Bletchley Declaration [15], signed by representatives of twenty-eight governments during the AI Security Summit, emphasizes the need for regulation and ethics in AI development. This declaration unites countries for collaborative research and the establishment of new rules governing the use of AI. The main identified issues include:

- Transparency of AI tools and models may be insufficient even for experts, which can lead to unforeseen results. Decisions made by AI may contain inaccuracies and embedded biases, potentially resulting in discrimination;
- The increasing use of AI-generated media negatively impacts social and political spheres, requiring careful consideration;
- The collection of personal data by AI systems raises concerns and emphasizes the need for privacy protection;
- Concerns about the uncontrolled or malicious use of AI.

AI can achieve excellent performance in ideal conditions, which are challenging to replicate in many real-world situations. AI typically operates in well-maintained data processing centers with a large number of computational resources and power. Currently, most high-performance AI models developed for vision and language tasks rely on these huge

resources. However, these resources are highly limited in many real-world systems, including drones, satellites, or ground transportation. This poses the challenge of "embedded artificial intelligence": running AI directly on a device or system without additional support from server-side computing. There are cases where running models on-board is optimal or necessary, providing several advantages. However, limitations in embedded computing can introduce significant constraints [16] or completely hinder the use of certain models in some systems. This creates a gap between the most efficient AI systems and those deployed in the real world, affecting the performance and reliability of many sought-after applications. Limitations of on-board AI systems depend on:

- Model Size: Models with a large number of parameters require more computation and memory to operate;
- Model Architecture: The connection of parameters in a neural network affects model computations, memory requirements, and speed;
- Input Data: Programs that require high-resolution input data or large input data volumes may demand an excessive amount of computation and memory;
- Decision-making Speed: The speed of making decisions should match the data input and initiate conclusions for a specific task according to requirements;
- Preprocessing of Input Data: Preprocessing input data according to the model and program requires significant computation;
- Number of Applied Models: Programs that use multiple AI models require the shared utilization of limited resources on the device.

There are also device-dependent and environmental-dependent limitations, such as:

- Computation: The device must be capable of performing a sufficient number of calculations per second to run AI models and other processes within an acceptable timeframe;
- Memory: Models require working memory for temporary storage and retrieval of information on the device. Memory can affect model speed, energy consumption, and overall functionality;
- Storage: Insufficient onboard memory may limit the choice of AI models;
- Power: Every computation or data movement requires energy. High-performance hardware operating on large models may surpass embedded power sources;
- Size and Weight: While processors are small, they typically require additional components that may exceed size and weight constraints of many systems;
- Auxiliary computations needed to run non-AI-related functions increase the resources required on the device;
- Environmental Characteristics: Environments with extreme temperatures, humidity, or radiation may lead to malfunctioning of computational equipment. Equipment designed for such conditions usually has lower performance, limiting AI models;
- Accessibility: Models may be constrained by hardware that is outdated or inaccessible, making it physically impossible to access, support, or replace it.

3.2 AI functions in UAV systems

To automate UAVs, various learning algorithms are employed, including Supervised and Unsupervised Learning, Reinforcement Learning, and Federated Learning. AI models in UAVs can operate at different levels and perform tasks such as (Figure 3):

- The task of optimal deployment involves strategically placing aerial base stations to reduce energy consumption by drones and alleviate the load on GCS, or creating a structured radio map [17, 18], especially in regions with complex terrain. The primary goal is to ensure effective network coverage in such conditions. To address this task, a structured radio map can be constructed, which is a detailed representation of radio signal propagation characteristics in the respective area;
- The task of enhancing communication efficiency [17] between UAVs and base stations. When a UAV transmits data and communicates with a base station, it may be affected by the wind, leading to drift or signal loss. To address this issue, methods supporting Recurrent Neural Networks (RNN) can be employed. They predict the future position and tilt angles of UAVs relative to the base station based on previous position and tilt angle data;
- The task of predicting path loss between UAVs. Signal loss is a phenomenon that occurs in wireless communication systems, describing the signal or energy loss as it traverses space with specific obstacles. When a radio signal is emitted from the transmitter and propagates through the air, it undergoes various influences, leading to signal attenuation at the receiver located at a certain distance from the transmitter. Algorithms such as "K Nearest Neighbours" (KNN) and "Random Forest" are used for predicting signal loss. Parameters such as signal propagation distance, transmitter height, receiver height, and elevation angle can be utilised for signal loss prediction;
- The task of monitoring and detecting anomalies [17, 18] in UAVs and their sensors that may occur during operation. Since UAVs are highly sensitive to any malfunctions or anomalies, it is crucial to have a system that can timely detect and respond to such events. Various methods for detecting anomalies in the operation of UAVs are proposed:
    - Using deep learning based on images from bird's-eye view and GPS data to detect unusual events in the drone's field of view;
    - Utilizing an anomaly detection algorithm to identify and isolate UAVs with malfunctions. This involves analyzing data from external sensors, such as humidity and wind speed;
    - Some methods include installing sensors on the motor to measure vibrations, analyzing vibration signals to determine the motor's condition and predict time to failure. Other systems use temperature sensors to identify motor overheating and the capability for automatic UAV landing in case of exceeding critical temperature.

- Tasks for solving computer vision problems for UAVs include:

    - Detection of safe emergency landing sites for drones

  - Real-time detection of other UAVs based on the analysis of sound data received from the drone and images
  - Detection and classification of specific objects

- The route planning task involves using RL to plan the route for UAVs in unknown or unpredictable environments. To navigate the drone in an entirely new environment, the model utilizes data about the initial state, environment, and target state. Drone sensors collect information about the surrounding environment, and the model uses this data to analyze possible routes. Computer vision tools and other sensors help the drone determine the most suitable route to reach its goal, enabling navigation, trajectory adjustments, and continuous learning during flight to adapt to environmental changes and improve navigation;
- Collision avoidance is crucial for the safe operation of UAVs. Drones may encounter obstacles in their path, such as terrain and air traffic. Various methods have been developed to avoid such collisions, including the use of GPS, obstacle detection and avoidance sensors (LiDAR, sonar, radar), and computer vision;
- Planning and resource management pose significant challenges due to resource constraints. The application of reinforcement learning allows for optimal decision-making in event planning and resource allocation [17];
- The content caching task involves utilizing data collected on board UAVs for training models. This enables devices to autonomously select which content to cache for further processing without the need for constant communication with the central network [17, 19];
- The optimization task for power distribution and planning in the UAV network relies on a comprehensive analysis of diverse data, including geographical information, sensor data, device status, task requirements, and network condition [17-18, 20]. Optimizing network resource utilization takes into account signal quality data, data transmission delays, and resource usage, contributing to making effective decisions in resource management and task execution in a timely and efficient manner. To achieve optimal efficiency, federated learning algorithms are employed on local data from each UAV.

3.3 Vulnerabilities and attacks on AI systems in UAVs

Attacks on AI technology encompass a broad spectrum of threats that can impact the security and reliability of information systems. These attacks include various methods, algorithms, and strategies aimed at exploiting and utilizing weaknesses in AI systems, creating potential threats to the confidentiality, integrity, and availability of data.

Attacks on AI technology can be conditionally divided into adversarial attacks, poisoning attacks, and model extraction attacks [8,21]. The goal of adversarial attacks is to deviate with maximum confidence, causing misclassification in the model with minimal perturbation of input data by altering input data. The goal of model extraction is to create a copy that will perform well on the original task (intellectual property theft) or that contains the same errors as the original model. The goal of poisoning attacks is to maximize the classification error of the entire dataset or a specific example by introducing poisoning samples into the training

data. This leads to an increase in the attack surface for both AI and UAVs. The application of AI-based methods for controlling and managing UAVs can be beneficial in terms of performance but raises concerns about the security of these methods and their vulnerability to adversarial attacks. Attacks on AI in UAVs are already being developed.

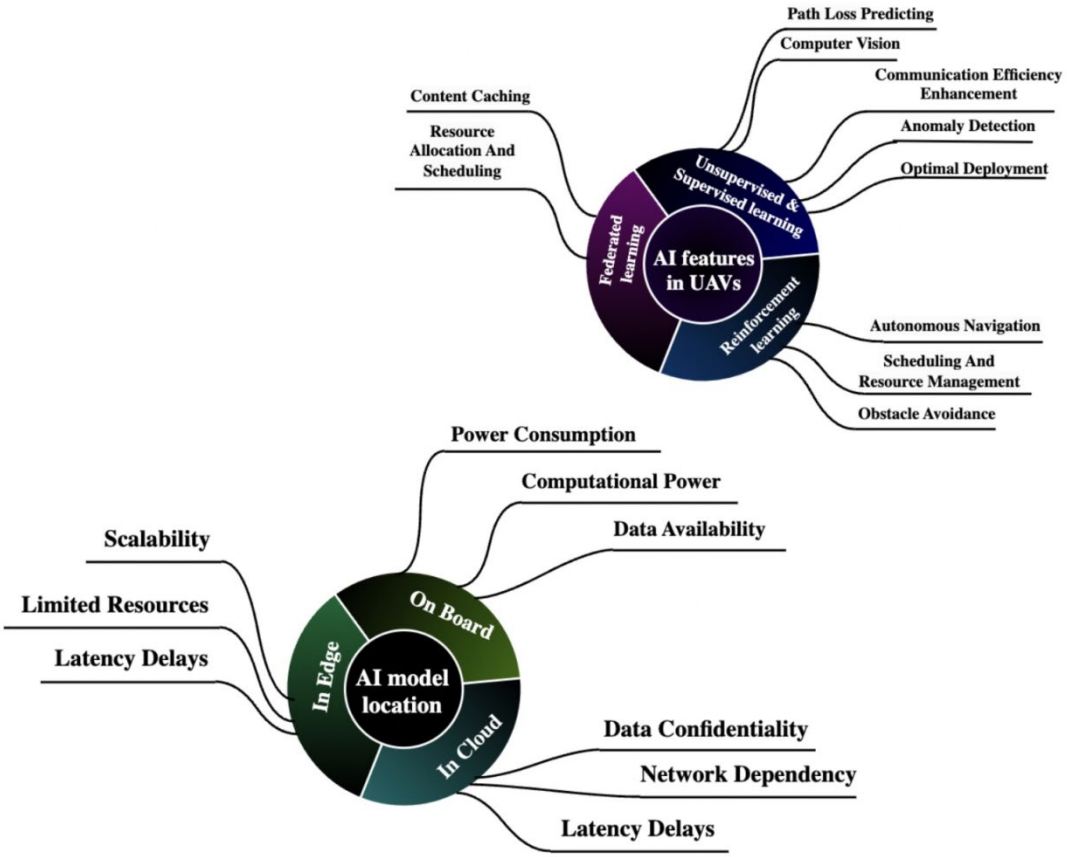


Figure 3: AI functions in UAVs and placement options for AI systems in UAVs with corresponding usage challenges.

This provokes an increase in the attack surface for both AI and UAVs. The application of AI-based methods for controlling and managing UAVs can be beneficial in terms of productivity but raises concerns about the security of these methods and their vulnerability to adversarial attacks. Adversarial attacks on AI in UAVs are currently under development.

Attacks on visual object tracking in UAVs are discussed in [22]. Such attacks generate adversarial examples that can lead to the loss of the tracked object for tracking systems. The Ad2Attack attack method proposes a new approach in which adversarial examples are generated during the regeneration of visual data in the object search process. This method allows determining how well the object is tracked in the current frame compared to the initial one by assessing the similarity between them. However, due to the vulnerability of deep neural networks (DNN) to adversarial attacks, Siamese trackers can be easily attacked by minor changes in the input image, resulting in incorrect position determination, posing a significant threat to UAV tracking tasks.

Authors [23] explore the attack of injecting adversarial perturbations into the bridge inspection process using UAVs. The attack operates by injecting adversarial examples into the bridge inspection process. These adversarial examples are generated by interfering with the data received by the UAV model during inspection. These artifacts are created by an adversarial model used to detect vulnerabilities in the UAV model. In this process, the adversarial model replicates the UAV model being attacked to identify possible vulnerabilities and alters them to cause incorrect results during inspection. The result of such attacks may involve neglecting certain risky areas of the bridge during inspection, leading to potential issues and safety threats.

Paper [24] examines the threats of adversarial attacks on UAVs operating in public spaces and the use of AI, particularly DL, to control these devices, taking into account the vulnerability of these methods to attacks. The authors propose a method based on deep learning solutions to create an effective detector that protects these methods and UAVs from attacks.

4. Countermeasures for providing UAV cybersecurity

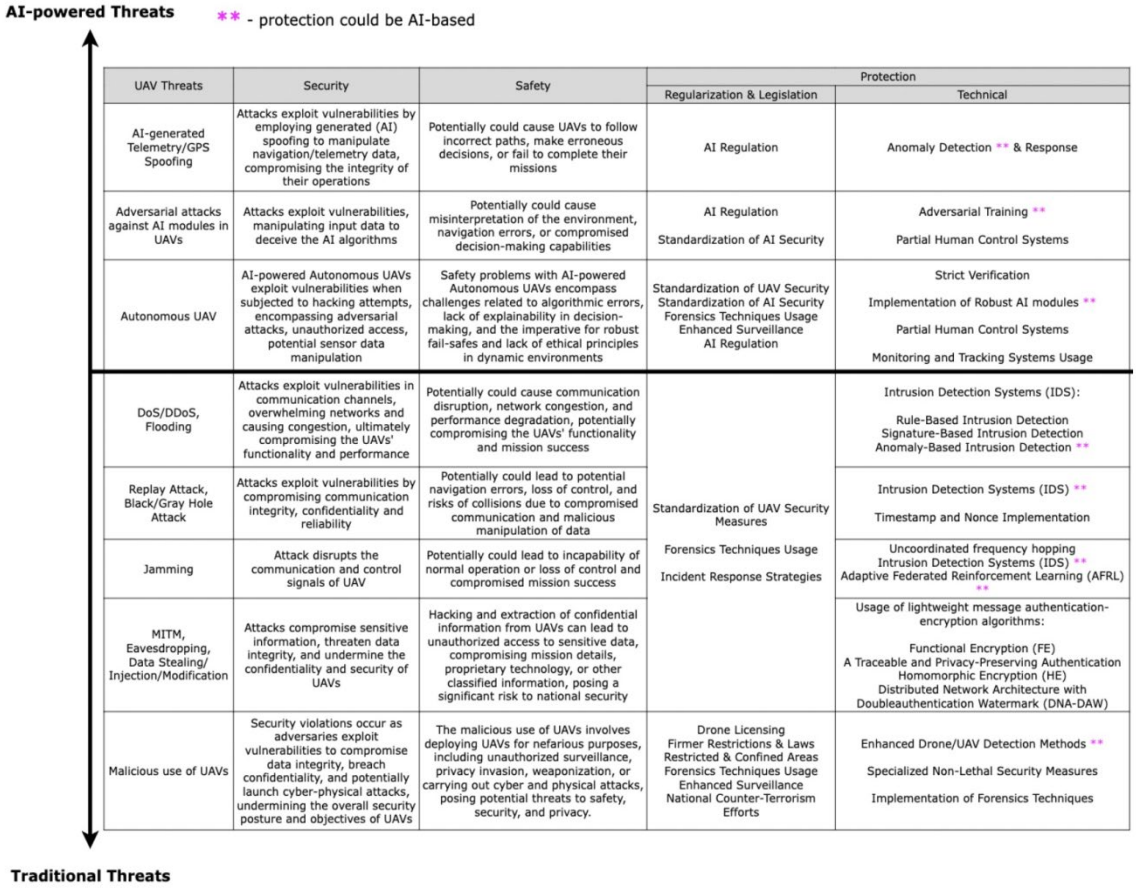
To mitigate the impacts of attacks or reduce the likelihood of their success, it is important to implement countermeasures. Based on the analysis of threats in UAVs and AI, it is proposed to divide the threats into two types: A powered and traditional, and to implement countermeasures for neutralizing these threats at levels of government regulation and technical application. The resulting systematization of countermeasures for the identified threats, along with a description of security breaches and their impact on safety (countermeasures that can be powered by AI are marked with **) is provided in Figure. 4.

4.1 AI-powered threats, attacks and countermeasures

AI can be maliciously used, thereby increasing the risks of attacks. Threats enhanced by AI can include AI-generated Telemetry/GPS Spoofing, Adversarial attacks against AI modules in UAVs, and the use of Autonomous UAVs.

It has been found that for AI-generated Telemetry/GPS Spoofing to create false data points, an attacker can use various techniques such as statistical modeling, machine learning, or signal processing. The spoofing algorithm can be trained on a dataset of telemetry and corresponding false data points using supervised or unsupervised learning. Training data can be created through simulation or by collecting real telemetry data from the UAV-cloud system. To assess the effectiveness of the spoofing algorithm, an attacker can use metrics such as success rate, attack efficiency, and computational complexity. In a centralized architecture, there is a high likelihood of GPS spoofing and telemetry spoofing attacks impacting if the central server is compromised, so a successful attack can have serious consequences [14].

At the regulatory level, it is proposed to implement technological standards and requirements for aviation systems that use AI, which take into account security measures against spoofing attacks. This will create a basis for developing effective detection and prevention methods for such attacks, increasing the overall level of security of aviation systems.



UAV Threats	Security	Safety	Protection	
			Regularization & Legislation	Technical
AI-generated Telemetry/GPS Spoofing	Attacks exploit vulnerabilities by employing generated (AI) spoofing to manipulate navigation/telemetry data, compromising the integrity of their operations	Potentially could cause UAVs to follow incorrect paths, make erroneous decisions, or fail to complete their missions	AI Regulation	Anomaly Detection ** & Response
Adversarial attacks against AI modules in UAVs	Attacks exploit vulnerabilities, manipulating input data to deceive the AI algorithms	Potentially could cause misinterpretation of the environment, navigation errors, or compromised decision-making capabilities	AI Regulation Standardization of AI Security	Adversarial Training ** Partial Human Control Systems
Autonomous UAV	AI-powered Autonomous UAVs exploit vulnerabilities when subjected to hacking attempts, encompassing adversarial attacks, unauthorized access, potential sensor data manipulation	Safety problems with AI-powered Autonomous UAVs encompass challenges related to algorithmic errors, lack of explainability in decision-making, and the imperative for robust fail-safes and lack of ethical principles in dynamic environments	Standardization of UAV Security Standardization of AI Security Forensics Techniques Usage Enhanced Surveillance AI Regulation	Strict Verification Implementation of Robust AI modules ** Partial Human Control Systems Monitoring and Tracking Systems Usage
DoS/DDoS, Flooding	Attacks exploit vulnerabilities in communication channels, overwhelming networks and causing congestion, ultimately compromising the UAVs' functionality and performance	Potentially could cause communication disruption, network congestion, and performance degradation, potentially compromising the UAVs' functionality and mission success	Standardization of UAV Security Measures Forensics Techniques Usage Incident Response Strategies	Intrusion Detection Systems (IDS): Rule-Based Intrusion Detection Signature-Based Intrusion Detection Anomaly-Based Intrusion Detection **
Replay Attack, Black/Gray Hole Attack	Attacks exploit vulnerabilities by compromising communication integrity, confidentiality and reliability	Potentially could lead to potential navigation errors, loss of control, and risks of collisions due to compromised communication and malicious manipulation of data		Intrusion Detection Systems (IDS) ** Timestamp and Nonce Implementation
Jamming	Attack disrupts the communication and control signals of UAV	Potentially could lead to incapability of normal operation or loss of control and compromised mission success		Uncoordinated frequency hopping Intrusion Detection Systems (IDS) ** Adaptive Federated Reinforcement Learning (AFRL) **
MITM, Eavesdropping, Data Stealing/ Injection/Modification	Attacks compromise sensitive information, threaten data integrity, and undermine the confidentiality and security of UAVs	Hacking and extraction of confidential information from UAVs can lead to unauthorized access to sensitive data, compromising mission details, proprietary technology, or other classified information, posing a significant risk to national security		Usage of lightweight message authentication-encryption algorithms: Functional Encryption (FE) A Traceable and Privacy-Preserving Authentication Homomorphic Encryption (HE) Distributed Network Architecture with Doubleauthentication Watermark (DNA-DAW)
Malicious use of UAVs	Security violations occur as adversaries exploit vulnerabilities to compromise data integrity, breach confidentiality, and potentially launch cyber-physical attacks, undermining the overall security posture and objectives of UAVs	The malicious use of UAVs involves deploying UAVs for nefarious purposes, including unauthorized surveillance, privacy invasion, weaponization, or carrying out cyber and physical attacks, posing potential threats to safety, security, and privacy.	Drone Licensing Firmer Restrictions & Laws Restricted & Confined Areas Forensics Techniques Usage Enhanced Surveillance National Counter-Terrorism Efforts	Enhanced Drone/UAV Detection Methods ** Specialized Non-Lethal Security Measures Implementation of Forensics Techniques

Figure 4: Systematization of threats and countermeasures in UAVs.

At the technical level, it is advisable to implement anomaly detection systems in telemetry data, which include the analysis of statistical parameters such as mean value and standard deviation, to assess the normality of data arrival followed by anomaly detection. The next step after detecting anomalies is to apply systems with automatic reaction activation, such as adjusting UAV control algorithms, blocking the source of spoofed signals, or activating additional systems to ensure UAV security. The proposed approach can be AI-based and will allow for effective evaluation of protection considering metrics such as performance speed and accuracy of attack detection.

As indicated in Section 4, there are potential threats from attacks on AI modules in UAVs, which can be either deliberate or accidental errors, leading to serious consequences. At the regulatory level, it makes sense to introduce standards and regulations regarding the use of AI in UAVs to ensure the reliability of these technologies [5]. Additionally, it is important to establish strict restrictions, especially regarding the illegal use of UAVs and their dangerous use near critical infrastructures such as airports or military installations. Furthermore, an improved surveillance system, particularly for drone supplies, considering their purchase history, can also help prevent the unwanted use of these technologies.

At the technical level, the implementation of specific technical measures is proposed to increase the resilience of AI systems in UAVs, such as:

- Applying Adversarial Training techniques to train AI modules on input data that may contain potentially attacking influences, with the goal of increasing resilience to adversarial attacks;
- Implementing systems of partial human control, where a human must participate in the management process and make decisions to provide an additional level of control and safety in situations that may be difficult for fully autonomous systems;
- Developing resilient AI modules and using strict methods of AI module verification, which include analysis and code verification, to ensure their correctness and absence of vulnerabilities before implementation in real-world conditions;
- Using monitoring and tracking systems for continuous observation of the AI modules' operation, detecting anomalies, and rapidly responding to possible deviations in their functioning.

The use of Autonomous UAVs poses a threat. The most obvious threat from the use of AI-powered UAVs arises from their potentially insufficient controllability and exceptional efficiency.

At the regulatory level, the introduction of safety standards for both UAVs and AI systems is being considered, along with the use of forensic methods to investigate incidents, improving surveillance systems to detect possible threats, and introducing effective regulations to govern the use of AI in these systems.

At the technical level, for protection, the implementation of strict verification of UAV software and hardware, the development of reliable AI modules, the creation of systems for partial human control for quicker response to unforeseen situations, and the use of advanced monitoring and tracking systems for continuous detection and tracking of UAV actions are proposed, with the aim of effective control and response to potential threats.

4.2 Standard threats, attacks and countermeasures

Despite the development of technologies, standard threats such as DoS/DDoS, Flooding, Replay Attack, Black/Gray Hole Attack, Jamming, MITM, Eavesdropping, still remain relevant. At the regulatory level, the solution proposed involves the implementation of security standards for UAVs and the use of forensic analysis methods to detect incidents and determine their causes. In the context of UAV security, forensic analysis is used to detect, investigate, and disclose crimes or incidents related to unmanned systems. This includes the application of forensic methods to digital data, specifically the collection, analysis, and interpretation of digital traces that may indicate unauthorized or anomalous activity [5]. Additionally, the development of incident response strategies helps improve the response to potential threats and the rapid detection and elimination of security issues in UAV systems.

Technical countermeasures against jamming attacks may include [12] the traditional approach of Uncoordinated Frequency Hopping (UFH), which allows two nodes to create and exchange a secret key using coordinated frequency hopping, complicating attackers' identification of the used frequencies. Another approach is Intrusion Detection Systems (IDS), automated with AI [5, 12], which use RL methods such as Adaptive Federated Reinforcement Learning (AFRL) for effective detection and protection against various types of jamming attacks. AFRL uses models without Q-learning and is capable of adapting to various scenarios,

training local models on UAV nodes, allowing effective counteraction against constant, random, and reactive jamming attacks [12].

Technical countermeasures against DoS/DDoS and Flooding attacks also use IDS. These systems are based on various approaches such as rules, signatures, and anomalies for detecting malicious interference. In rule-based IDS, clear norms and limitations are defined by which deviations from the system's normal behavior are identified. Signature-based IDS compare activity against known attack signatures for their detection. This method is effective for detecting known threats but not new attacks. Anomaly-based IDS, which use ML/DL, analyze changes in system behavior in real time and detect unusual or deviant actions. Combining different IDS methods is an effective approach to ensure comprehensive system protection against various types of attacks, complementing each other and detecting both known and new threats.23.

Technical countermeasures against Replay Attack include methods of implementing Timestamps and Nonce (a unique value) [12]. The use of fresh nonce during system initialization guarantees the absence of repeated messages, while Timestamps allow for correct time synchronization and the rejection of messages if the Timestamp has expired. For protection against Black/Gray Hole Attacks, Intrusion Detection Systems (IDS) based on AI can be utilized. For example, an Agent-based Hierarchical Intrusion Detection and Response System (HID-RS) [12] uses a centralized GCS node as a trusted element for packet monitoring. Each UAV sends a packet with neighboring data to the GCS, including the UAV type and information about neighboring and previous nodes.

For protection against MITM attacks and interceptions at the technical level, it is proposed to use lightweight message authentication-encryption algorithms. Functional Encryption (FE), Homomorphic Encryption (HE), and the Dual Authentication Watermark Network Architecture (DNA-DAW) are methods that can also be used to ensure data confidentiality and integrity [7, 9]. However, such approaches may present challenges related to computational complexity and efficiency, especially in conditions of limited resources in devices. Therefore, it is necessary to ensure a balance between security and performance, as well as to address the issues related to the size and weight of algorithms in the context of unmanned systems.

At the regulatory level to control this threat, it is necessary to implement licensing systems for UAV owners and strengthen legislation regulating their use. Stricter restrictions and legal norms are important parts of strategies to prevent unauthorized UAV use. Surveillance and national security efforts are identified as key for timely detection and prevention of potential terrorist or criminal actions using UAVs.

Regarding technical implementations for protection, the use of AI systems for improved detection and notification of any approaching UAVs is highlighted, providing a more effective approach to alarms and sufficient time for neutralizing the threat remotely. Another approach identified is considering the capabilities of specialized automated security measures that do not lead to lethal outcomes, to overcome threats from UAVs over areas where their use is prohibited, in order to prevent downing and injury. Also important is the development of forensic tools for the identification and investigation of illegal UAV use, allowing for the establishment of actual responsibility and the application of appropriate security measures.

5. Case study. Intelligent UAV System for Humanitarian Demining

5.1 Requirements for AI-Based Components and AI-Powered Protection Means for UAV System for Humanitarian Demining

One example of standardizing requirements for AI involves quality model based defining its characteristics [10], which allows assessing the trustworthiness and efficiency of AI platforms and improving the security and safety of the UAV systems.

As a case study, it is proposed to adapt a basic quality model, in which AI is used in unmanned systems for paramilitary demining [25], specifically for developing, first, onboard computer vision for UAVs, and second, protection of the UAV system assets.

The adaptation of the quality model for AI-based on board system considering the peculiarities of the demining tasks, includes (Figure 5a) the following marked characteristics:

- Verifiability (VFB) of AI in this case becomes crucial in ensuring accurate and reliable identification of explosive objects on the map, adapting to various environmental conditions and undergoing verification through a variety of tests aimed at realistic simulation of operational conditions;
- Ethics (ETH) is important for protecting the rights and safety of people during the use of demining technologies, as well as for avoiding negative impacts on the environment, which is a key aspect in the context of real demining operations;
- Explainability (EXP) and Transparency (TRP). Current issues regarding ethics, morality, privacy, and law due to the lack of "understandable functions" and knowledge representation; such absences undermine the ability of humans to control or even understand the proposed solutions. Since safety-critical systems must be traceable, there is a trend away from the Black-Box concept;
- Lawfulness (LFL). Since UAVs can be used in critical sectors, AI interacting with the system must comply with current legislation and consider rules and norms related to air traffic organization;
- Security (SCR). All components of UAV systems must be safe and secure, including AI systems onboard or in the cloud. Since many AI systems rely heavily on input signals from the external environment, their deliberate or targeted manipulation can lead to errors and corresponding negative unforeseen consequences;
- Safety, diversity, resilience, and robustness (SFT, DVS, RSL, RBS) entail not only preventing risks and damages due to failures but also minimizing potential consequences in case of unforeseen situations. AI models must detect and effectively respond to unexpected circumstances, also having built-in means for emergency shutdown or automatic management in dangerous scenarios, thereby ensuring safety and reliability in demining operations;
- Interactivity (INR) and Human Autonomy (HMA) are critical characteristics. It's important that operators can interact with the system and intervene in its operation if necessary, while still allowing autonomy for system decisions. Current research in human-machine interaction is driven by the increasing volumes of processed information and the complexity of automation, and this should improve human-machine coordination;

- Trustworthiness (TST) ensures that the system reliably performs its functions of recognizing explosive objects and meets safety standards, fostering users' confidence in its reliability;

Accuracy (ACR) is key to avoiding false identifications and ensuring that recognized objects correspond to the actual situation.

Adaptation of the quality model for UAV systems, where AI represented as a powered protection means for UAV system assets is illustrated by Figure 5b where significant characteristics marked:

- VFB is defined by the ability to subject AI to verification and testing through the application of various methods in real conditions for protecting UAV systems;
- ACR of the AI model is key for trustworthy detection and identification of potential threats or anomalies in UAV systems;
- TST provides the creation of reliable protection of UAV systems in conditions of high safety requirements. DVS allows the system to adaptively counter various attacks, and RSL and RBS ensure resistance to faults and changes in conditions;
- The use of AI as a means of UAV protection requires compliance with Security requirements, ensuring the integrity and confidentiality of the system, providing a high level of protection in conditions of constantly increasing cyber threats;
- EXP, TRP, and Interpretability (INP) aspects become important factors in the context of security, because the need for effective interaction and understanding of the decisions made is critical for ensuring the safety of UAV protection systems.

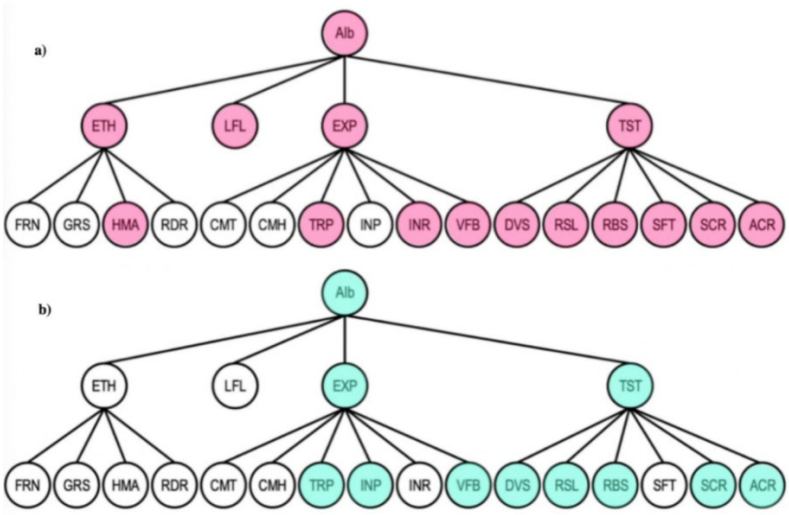


Figure 5: Basic quality model for AI a) for demining tasks, b) as a protection mean.

According to the specified characteristics, an assessment is made and compliance with the requirements, in particular, with regard to security and safety, is determined. An integral quality metric for AI tools can then be calculated using additive convolution.

5.2 Risk mitigation assessment

For quantitative risk assessment, various methods are applied, among which risk-oriented approaches, such as IMECA [8], are worth highlighting. Application of IMECA for multifunctional UAV fleets has been demonstrated in [26].

By analyzing various attacks and appropriative countermeasures, it is possible to determine how effective risk reduction will be after the implementation of AI powered protection measures at regulation and technical levels. Figure 6 presents information about potential threats and means of their protection based on the countermeasures mentioned in Figure 4. Column 2 determines whether there might be AI powered threats.

Column 3 determines whether there might be AI-based protection. The assessment scale includes three levels of consequence severity or attack probability: "Low," "Medium," and "High," denoted as L, M, and H, respectively. After applying protection means, one or both indicators decrease, thereby reducing the level of overall risk.

Threats	AI powered threats	AI-based protection	Probability change	Severity change	Risk change
Telemetry/GPS Spoofing	✓	✓	M → L	H → M	H → M
Adversarial attack against AI-based UAV	✓	✓	M → M	H → M	H → M
Autonomous UAV	✓	✓	M → L	H → M	H → M
DoS/DDoS, Flooding		✓	H → H	H → L	H → M
Replay Attack, Black/Gray Hole Attack		✓	M → M	M → L	M → M
Jamming		✓	H → L	H → M	H → M
MITM, Eavesdropping, Data Stealing/ Injection/Modification			H → L	H → H	H → M
Malicious use of UAVs		✓	H → M	H → L	H → L

Figure 6: Change of criticality indicators caused by AI-powered protection and countermeasures.

6. Conclusion and future work

The main contribution of this study is the classification of protection means considering the aspect of AI and an example of implementing standardization of AI components in UAVs depending on the specified functions. The implementation of AI in UAVs significantly improves their efficiency, while also unveiling new threats and opportunities for malicious actors. Within the assessment of effectiveness, safety, and security of UAV systems, AI technology must be considered as one of the factors of system unreliability due to the nature of the technology itself and viewed as a method to enhance current attacks. The proposed systematization consists of regulatory methods aimed primarily at legalizing use, standardization, and quality control of UAVs and AI, and the corresponding technical implementations of these methods. Additionally, provisional assessments of the impact of analyzed attacks on cybersecurity and safety risks are provided. The proposed approach can be extended to security-informed safety analysis of critical systems operated in aggressive information and physical environments and providing proactive defense against attacks strengthened by AI means [27].

Future research could be directed towards developing methods for assessing countermeasures and analyzing attacks on UAVs equipped with AI systems. An important direction is the study of combined attacks, development of attack graphs, as well as investigating the impact of parallel and sequential attacks, which could be independent,

homogeneous, or heterogeneous. The implementation of such approaches could significantly contribute to ensuring the resilience and dependability of systems in the context of the continuously increasing risk of cyberattacks and modern challenges in the field of unmanned mobile technologies and AI. Intelligent robotic-biological system [25] for humanitarian demining is a very interesting object of future research and development in context safety-security-performance tradeoff considering different explosive ordinance, conditions of cyber physical environment, and possibilities of dynamical reconfiguring IT-infrastructure.

References

[1] N. S. Labib, M. R. Brust, G. Danoy, P. Bouvry, The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles, IEEE Access 9 (2021) 115466–115487. doi:10.1109/access.2021.3104963.

[2] M. Sivakumar, N. M. TYJ, A Literature Survey of Unmanned Aerial Vehicle Usage for Civil Applications, J. Aerosp. Technol. Manag. 13 (2021). doi:10.1590/jatm.v13.1233.

[3] C.-A. Ciolponea, The Integration of UAS in Current Combat Operations, Land Forces Acad. Rev. 27.4 (2022) 333–347. doi:10.2478/raft-2022-0042.

[4] H. Wang, H. Cheng, H. Hao, The Use of Unmanned Aerial Vehicle in Military Operations, y: Man-Machine-Environment System Engineering, Springer Singapore, Singapore, 2020, c. 939–945. doi:10.1007/978-981-15-6978-4_108.

[5] J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab, Security analysis of drones systems: Attacks, limitations, and recommendations, Internet Things 11 (2020) 100218. doi:10.1016/j.iot.2020.100218.

[6] Global Unmanned Aerial Vehicle Market Size, Share 2032. URL: https://www.custommarketinsights.com/report/unmanned-aerial-vehicle-market.

[7] M. A. Baballe, et al. 'The Unmanned Aerial Vehicle (UAV): Its Impact and Challenges'. Global Journal of Research in Engineering & Computer Sciences, vol. 2, no. 3, Zenodo, June 2022, pp. 35–39, doi:10.5281/zenodo.6671910.

[8] O. Veprytska, V. Kharchenko, Extended IMECA Technique for Assessing Risks of Successful Cyberattacks: 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2023. doi:10.1109/dessert61349.2023.10416447.

[9] O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, F. Di Giandomenico, Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection, Entropy 25.8 (2023) 1123. doi:10.3390/e25081123.

[10] M. Kolisnyk, Vulnerability analysis and method of selection of communication protocols for information transfer in Internet of Things systems, Radioelectron. Comput. Syst. № 1 (2021) 133–149. doi: 10.32620/reks.2021.1.12.

[11] B. Ly, R. Ly, Cybersecurity in unmanned aerial vehicles (UAVs), J. Cyber Secur. Technol. (2020) 1–18. doi:10.1080/23742917.2020.1846307.

[12] K.-Y. Tsao, T. Girdler, V. G. Vassilakis, A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks, Ad Hoc Netw. 133 (2022) 102894. doi:10.1016/j.adhoc.2022.102894.

[13] O. Laccourreye, H. Maisonneuve, French scientific medical journals confronted by developments in medical writing and the transformation of the medical press, Eur. Ann. Otorhinolaryngol., Head Neck Dis. 136.6 (2019) 475–480. doi:10.1016/j.anorl.2019.09.002.

[14] G. Airlangga, A. Liu, A Study of the Data Security Attack and Defense Pattern in a Centralized UAV–Cloud Architecture, Drones 7.5 (2023) 289. doi:10.3390/drones7050289.
[15] Prime Minister's Office, 10 Downing Street, The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023, 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.
[16] K. Miller, A. Lohn, Onboard AI: Constraints and Limitations, Center for Security and Emerging Technology, 2023. doi:10.51593/2022ca008.
[17] M.-A. Lahmeri, M. A. Kishk, M.-S. Alouini, Artificial Intelligence for UAV-Enabled Wireless Networks: A Survey, IEEE Open J. Commun. Soc. 2 (2021) 1015–1040. doi:10.1109/ojcoms.2021.3075201.
[18] P. McEnroe, S. Wang, M. Liyanage, A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges, IEEE Internet Things J. (2022) 1. doi:10.1109/jiot.2022.3176400.
[19] B. Brik, A. Ksentini, M. Bouaziz, Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems, IEEE Access 8 (2020) 53841–53849.
[20] S. Sai, A. Garg, K. Jhawar, V. Chamola, B. Sikdar, A Comprehensive Survey on Artificial Intelligence for Unmanned Aerial Vehicles, IEEE Open J. Veh. Technol. (2023) 1–26. doi:10.1109/ojvt.2023.3316181.
[21] Rajashree Manjulalayam Rajendran, Bhuman Vyas, Cyber Security Threat and its Prevention Through Artificial Intelligence Technology, International Journal For Multidisciplinary Research (2023) 5(6), 1-18
[22] C. Fu, S. Li, X. Yuan, J. Ye, Z. Cao, F. Ding, Ad2Attack: Adaptive Adversarial Attack on Real-Time UAV Tracking, y: 2022 IEEE International Conference on Robotics and Automation (ICRA), IEEE, 2022. doi:10.1109/icra46639.2022.9812056.
[23] A. Raja, L. Njilla, J. Yuan, Blur the Eyes of UAV: Effective Attacks on UAV-based Infrastructure Inspection, y: 2021 IEEE 33rd International Conference on Tools with Artificial Intelligence (ICTAI), IEEE, 2021. doi:10.1109/ictai52525.2021.00105.
[24] T. Hickling, N. Aouf, P. Spencer, Robust Adversarial Attacks Detection based on Explainable Deep Reinforcement Learning for UAV Guidance and Planning, IEEE Trans. Intell. Veh. (2023) 1–14. doi:10.1109/tiv.2023.3296227.
[25] G. Fedorenko, H. Fesenko, V. Kharchenko, I. Kliushnikov, I. Tolkunov, Robotic-biological systems for detection and identification of explosive ordnance: concept, general structure, and models, Radioelectron. Comput. Syst. № 2 (2023) 143–159. doi:10.32620/reks.2023.2.12.
[26] H. Zemlianko, V. Kharchenko, Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique, Radioelectron. Comput. Syst. № 4 (2023) 143–159. doi:10.32620/reks.2023.4.11.
[27] A Kashtalian, S Lysenko, B Savenko, T Sochor, T Kysil, Principle and method of deception systems synthesizing for malware and computer attacks detection, Radioelectron. Comput. Syst. № 4 (2023) 112–151. doi: 10.32620/reks.2023.4.10.