Review

Counter Drone Technology: A Review

Higinio Gonzalez-Jorge *, Enrique Aldao, Gabriel Fontenla-Carrera, Fernando Veiga-López, Eduardo Balvís, Eduardo Ríos-Otero

Posted Date: 9 February 2024

doi: 10.20944/preprints202402.0551.v1

Keywords: counter-UAS; drone threat; unmanned aircraft system; malicious drone

Review

Counter Drone Technology: A Review

Higinio González-Jorge *, Enrique Aldao, Gabriel Fontenla-Carrera, Fernando Veiga-López, Eduardo Balvís and Eduardo Ríos-Otero

Instituto de Física e Ciencias Aeroespaciais (IFCAE), Universidade de Vigo, Campus de As Lagoas, Ourense, E-32004, Spain; higiniog@uvigo.gal; enrique.aldao.pensado@uvigo.gal; gabriel.fontenla@uvigo.gal; fernando.veiga@uvigo.gal; ebalvis@uvigo.gal; eduardo.rios@uvigo.gal

* Correspondence author

Abstract: Unmanned Aerial Vehicles (UAVs), commonly known as drones, have experienced a significant surge in both civilian and military applications, owing to their versatility and cost-effectiveness. However, a negligent use or the operation with harmful intent of these aircraft poses a potential risk to public safety and the privacy of individuals. In response to this threat, counter-drone systems have been developed in recent years, including technologies to detect, position, and neutralize these aircraft. This paper presents a review of different existing commercial counter-drone systems, the technologies behind detection, tracking, and classification, as well as soft and hard kill mitigation.

Keywords: counter-UAS; drone threat; unmanned aircraft system; malicious drone

1. Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, refers to aircraft operated either autonomously by a computer or remotely controlled by a human operator [1]. These vehicles come in various shapes and sizes, ranging from small quadcopters to large fixed-wing aircraft. Initially developed for military purposes [2], drones have now expanded into numerous civilian applications including, but not limited to, aerial photography, precision agriculture [3], surveillance [4], search and rescue [5], delivery services [6], infrastructure inspection [7], and more. They are typically equipped with cameras, sensors, and sometimes other specialized equipment based on their intended uses. Their versatility and relatively low operating costs have contributed to their widespread adoption across various industries.

Drones have significantly impacted the military industry [8-10]. They have transformed modern warfare by offering new capabilities and strategies. Drones provide real-time aerial surveillance, enabling military forces to gather intelligence, monitor enemy movements, and assess battlefield situations without risking human lives. They can cover large areas and gather data from different altitudes, providing a comprehensive view of the terrain. Armed drones, such as Predator [11] and Reaper [12], have the capability to carry and launch precision-guided missiles or bombs. This allows for targeted airstrikes against enemies with reduced collateral damage compared to traditional methods. Drones act as force multipliers by enhancing the effectiveness of military operations. They can be deployed quickly and operate for extended periods, providing continuous support to ground forces. Drones are also used for logistical purposes, transporting supplies and equipment to remote or inaccessible areas, reducing the risk of human transporters.

The military drone industry continues to evolve with ongoing advancements in technology, aiming to improve flight endurance, stealth capabilities, and payload capacities. This is also linked to a decrease in production costs and greater accessibility to the different actors in a conflict as can be observed in the recent Ukraine war [13, 14]. Drones played a significant role in the conflict, particularly in the eastern region, where there has been intense fights between Ukrainian government forces and Russia. Drones have been utilized by both sides, including both commercial off-the-shelf models and more sophisticated military-grade UAVs. Drones have added a new dimension to the conflict, influencing tactics and strategies employed by both sides. Some examples of drones that

 doi:10.20944/preprints202402.0551.v1

have been reported to be used in the conflict are Raven [15], Orlan-10 [16], Bayratkar TB2 [17] or Forpost [18].

Special attention in the conflict of Ukraine should be paid to the loitering munitions, also known as kamikaze or suicide drones [19]. These weapons differ from traditional drones in that they are not solely intended for reconnaissance or surveillance; rather, they are specifically designed to carry explosive payloads and engage targets directly. One notable example is the Israeli-made Harop [20] or the USA-made AeroVironment Switchblade 600 [21] loitering munitions. They are capable of loitering in the air for an extended period, searching for targets. Once a target is identified, they can be directed to dive and strike with precision. Most of them are designed as "fire-and forget" weapons, capable of destroying both stationary and moving targets. The primary focus often includes specific enemy positions, such as artillery emplacements or vehicles. Their employment in conflicts underscores the evolving nature of warfare and the integration of advanced technology into military strategies. However, the use of such munitions also raises ethical and humanitarian concerns, especially regarding civilian casualties and the potential for indiscriminate harm [22].

Technological capabilities of drones (especially those acquired from the military scenarios) could be used for situations in the civilian sphere which are considered illicit, harmful, or illegal. These are the considered malicious drones [23]. They can be modified versions of commercial models or intentionally designed ones for illicit purposes. Some of the potential malicious activities involving these drones include:

- Surveillance and privacy invasion: Drones equipped with cameras can invade privacy by peeping into private spaces, spying on individuals, or capturing unauthorized footage.
- Security threats: They can breach security perimeters of sensitive locations, such as airports, government buildings, or events, posing risks of espionage, smuggling, or even terrorist attacks.
- Harassment of disruption: Drones may harass individuals, disrupt public events, or interfere with emergency services by flying in restricted areas or causing disturbances.
- Delivery of harmful payloads: Malicious drones can be used to transport and deliver illegal substances, weapons, or hazardous materials to specific locations.

The European Union Aviation Safety Agency (EASA) categorizes drone incidents in three main groups: negligence, gross negligence, and criminal / terrorist motivation [24]:

- Negligence can be performed by clueless or careless individuals. The first group do not know or understand the applicable regulations and they fly their drones in sensitive or prohibited areas. The second one knows the applicable regulations but may breach them through either fault or negligence. Consequently, their drones fly over sensitive of prohibited areas, but have no intent to disrupt or affect activities of critical infrastructures or others.
- Gross negligence can be committed by reckless individuals or activists/protesters. The first group knows the applicable regulations and restrictions, but deliberately does not follow the rules to pursue personal of professional gain. They can disrupt critical infrastructures or other activities by totally disregarding the consequences of their actions. The second group consists of individuals who, regardless of whether they know the applicable regulations and restrictions, actively seek to use drones to disrupt critical infrastructures or other activities. They have no intent to endanger human lives, although their acts could have unintended consequences to safety.
- Criminal / terrorist motivation. They are individuals who, regardless of whether they know the applicable regulations and restrictions, actively seek to use drones to interfere with the safety and security of critical infrastructures and other activities. Their acts are deliberate and show no regard for human lives and property. These individuals are to be regarded as being criminally motivated or even as terrorists.

The Federal Aviation Administration (FAA) develops a quarterly report of drone sightings from pilots, citizens, and law enforcement [25]. They currently receive more than 100 reports each month and detect a dramatic increase over the past two years. Wang et al. used the FAA data to perform a spatial analysis to determine the distribution of drone sightings in the USA [26]. They concluded that

 doi:10.20944/preprints202402.0551.v1

the vast majority of malicious operations occurred in the most densely populated states (e.g., New York, Florida, California, Texas).

Authorities and organizations have been responding to these challenges by implementing regulations, deploying anti-drone technology, and establishing no-fly zones to prevent malicious drone activities. Developing effective counter-drone measures remains a priority to mitigate the potential risks posed by their misuse [27]. Law enforcement agencies and security authorities are consistently developing and implementing strategies to detect and address potential threats arising from the misuse of drones, protecting public security and privacy. Counter-Unmanned Aircraft Systems (C-UAS) are designed to detect, track, and mitigate unauthorized or potentially threatening drones. C-UAS technologies can include a variety of methods such as radio frequency jamming, signal interception, net-based capture, or even kinetic methods to neutralize or disable drones that pose security risks or penetrate restricted airspace. These systems are becoming increasingly important as drone technology advances and their accessibility grows, raising concerns about their potential misuse.

C-UAS systems are dual technologies, which are important in the military industry, but also in the civilian sector (e.g., critical infrastructure protection, mass events, official buildings). Although the technology is relatively recent, there are many research institutions and companies working on the development of this type of systems. This work provides a review of the status of C-UAS technology. The review is focused mainly on the technologies used for target detection, classification, and tracking, in combination with a section related with mitigation technologies. The structure of the manuscript is the following: Section 2 is focused on the different commercial counter drone solutions presented in the market, Section 3 is related to technology involved in drone detection, tracking and identification, Section 4 presents the mitigation technologies, and Section 5 the conclusions.

2. Commercial counter drone solutions

Counter drone technology has come to the market approximately in the last decade. Although still under development, several companies are currently selling such products for both military and civilian applications. Table 1 presents different state-of-the-art C-UAS systems, outlining their main characteristics, and technologies they employ.

Table 1. C-UAS commercial solutions.

Company / product / country	Technology
Lookheed Martin Morfius [28] USA	A reusable defensive C-UAS. Enables multi-engagement and swarm defeat at longer ranges than ground-based systems. No specific information about detection sensors, classification and tracking is provided. Mitigation action is categorized as hard kill.
Raytheon Coyote [29] USA	A drone used for a near-term C-UAS solution. It is equipped with an advanced seeker and a warhead. It can be operated up to one hour and is designed for interchangeable payloads. No specific information about detection sensors, classification and tracking is provided. Mitigation actions are categorized as hard kill.
Northrop Grumman M-ACE [30] USA	M-ACE is a modular ground-based C-UAS solution. It utilizes three-dimensional radar, radio frequency sensors, electro-optical/infrared cameras, global positioning systems, and secure radio for transmitting information over command-and-control networks. Mitigation actions (hard kill) are conducted by kinetic/non-kinetic defeat options (e.g., bushmaster cannon with advanced ammunition, directed energy solutions).
General Dynamics Dedrone [31] USA	Denominated as Expedicionary Kit, it was developed in response to a mission need for a mobile ground C-UAS capability. It can be deployed in less than an hour. The system includes radio frequency sensors with a range up to 1.5 km (ideal conditions). It uses a classification engine which recognizes and classifies

 doi:10.20944/preprints202402.0551.v1

	commercial, consumer and hobbyist drones. It is based on drone RF signature. Mitigation action (soft kill) is done by GNSS (Global Navigation Satellite Systems) and remote-control disruption of the system.
Highpoint Aerotechnologies Liteye [32] USA	It is a portable perimeter defense system against autonomous, unmanned and multi-domain threats. The solution can be containerized for a rapid deploy. No specific information about sensing systems is provided. It includes AI & analytics for threat classification. Drone mitigation can be carried out through soft kill (high-precision directional RF jamming) or hard kill (hunter-seeker drones or kinetic weapons).
Blighter Surveillance Systems AUDS [33] UK	AUDS is a strategic C-UAS system, designed to disrupt and neutralize drone threats. It includes detection, tracking and defeat capacities. It uses an air security radar (Ku-band) with a detection range of 10 km and minimum target size of 0.01 m^2; and a digital camera tracker (color HD camera with 2.3 MP and optical zoom x30 and thermal camera with 640x512 pixels). Mitigation actions are performed with an intelligent software-defined RF inhibitor with a high gain quad-band antenna system (includes GNSS frequencies).
MSI-Defence Systems Terrahawk Paladin [34] UK	It is a containerized, modular, remote-controlled and re-deployable C-UAS system. It includes sensors (electro optic) and effectors mounted under NATO-standard. Drone tracking is done using AI algorithms. Mitigation is carried out using the MSI-DS Terrahawk LW Series gun mount (hard kill).
Thales Group EagleShield [35] France	It is an integrated nano, micro, mini and small drone countermeasures solution to protect and secure civil and military sites. It combines different sensors, such as radars and cameras, along with warfare technologies to detect, monitor and neutralize drones in the airspace. No specific information about the sensing and mitigation systems is provided.
Elistair Orion 2.2 TW [36] France	It is a tethered drone station that can provide continuous surveillance and security for sensitive sites, offering a passive defense against unauthorized drones. Although it has no mitigation systems and is mainly based on an elevated observation platform, it is included in this work as it presents a disruptive concept far from most existing C-UAS systems.
Elbit Systems ReDrone [37] Israel	ReDrone is a multi-layered defense against UAV threats. It presents multiple deployment options in mobile or stationary configurations. It utilizes different sensing technologies for detection and tracking, such as: 3D radar, electro-optical / infrared (EO/IR) day & night cameras, Signals Intelligence (SIGINT) and acoustic sensors. Mitigation actions are based on soft kill (jamming actuating through GNSS and communications channels).
Israel Aerospace Industries Drone Guard DG [38] Israel	It is a multi-layer, multi-sensor, flexible and scalable solution designed to protect ground sites and mobile convoys. It presents an open architecture which enables the integration of radars, passive Communications Intelligence (COMINT), and EO sensors. Drone Guard DG5 incorporates AI based decision-making tools for target classification, thereby decreasing operator workload. It offers soft and hard kill mitigation. Soft kill is based on the disruption of drone communication and/or navigation protocol. Hard kill is performed with a drone-kill weapon system and high accuracy stabilized gunfire.
Rafael Advanced Defense Systems Drone Dome [39] Israel	Drone Dome is a modular system which can be deployed as C-UAS mobile or stationary unit. The solution integrates radar, SIGINT/RF sensor, and EO sensor. Mitigation actions are based on a jammer (soft kill) which blocks the signal and command from the remote control. It also jams the video transmitted by the drone to the operator and the GNSS signal to disrupt the drone navigation and control. It can also be equipped with hard kill capacities.

 doi:10.20944/preprints202402.0551.v1

CONTROP Precision Technologies TORNADO-ER [40] Israel	It can detect and track drones from large distances up to 12 km. The system was developed for diverse land environmental conditions. Detection system is based on a gyro-stabilized electro-optical and thermal imaging sensors in combination with real-time video algorithms. Mitigation actions can include kinetic or non-kinetic countermeasure.
MCTECH RF Technologies MC Horizon [41] Israel	This system includes a 3D pulse-Doppler radar, RF detection unit and EO/IR tracker. It provides a detection range between 3 km and 15 km with 360º coverage and a recognition range among 1.5 km and 10 km. Mitigation action is based on high power outdoor jamming system (soft kill) with an effective disruption range of 3 km.
INDRA Crow [42] Spain	C-UAS system designed to detect and neutralize drone threats from microdrones (e.g., DJI Phantom) to large drones. It combines a detection radar, RF analysis, a EO sensors. Mitigation is carried out through RF and GNSS jamming (soft kill).
SDLE Antidrone [43] Spain	A portable handheld solution that can be installed in vehicles and moving platforms. The manufacturer does not provide information about detection sensors, threat classification or tracking systems. Mitigation action are done disrupting remote control, telemetry, video link and GNSS navigation.
Leonardo FalconShield [44] Italy	It is a scalable and modular system oriented to slow and small drones. It utilizes a radar and Electronic Surveillance Measures (ESM), combined with Electro Optical (EO) sensors and advanced Radio Frequency (RF) effector technology. Threat detection and tracking includes automatic capabilities to minimize the operator workload. Mitigation actions include electronic attack (capable to deny, disrupt or defeat UAV command, control, navigation) and UAV data downlinks.
SAAB AB 9LV [45] Sweden	It enables the integration of a range of sensors for drone localization, classification, and recognition. These sensors integrate RF protocol detection, micro doppler radar, passive radar and EO/IR to support detection capabilities. Saab classification enables a hierarchy of drone sub-classification based on size, propulsion, and autonomy. It uses a multiple attribute decision making method to combine simple or complex rules, organic sensor classifications including image recognition, signature analysis and protocol detection, kinematic model-based classification, and movement pattern analysis. The threat identification function utilizes positive drone identification with associated trust metrics. It employs non-cooperative kinematic threat intent assessment and incorporates both anomaly detection and spatio-temporal movement pattern analysis. Mitigation actions support the integration of a variety of effectors to enable drone capability, including RF jammers and GNSS denial systems (soft kill) and high energy laser systems, physical capture, fouling drones and small to medium caliber guns with a high rate of fire and air-burst ammunition.
HENSOLDT Xpeller [46] Germany	It is a modular system with includes radar for airspace monitoring and digital cameras, in combination with radio detectors, RF and GNSS countermeasures (soft kill). The system can be deployed in static, mobile and wearable form.
Rheinmetall AG Drone Defence Toolbox [47] Germany	Rheinmetall deploys a combination of different radars in X and S band mode, passive emitter locators, commercial identification technologies (ADSB) and 360º cameras with laser range finders as well as infrared and time of flight cameras in various spectrums. The generated signals are processed, fused and classified in the command-and-control system. The mitigation is provided by a C-UAS jammer (soft kill). In the near future, they will provide autonomous catcher drones and high-energy lasers.

 doi:10.20944/preprints202402.0551.v1

Department13 Map13 [48] Australia	They offer a C-UAS solutions designed to detect, identify and mitigate drone threats using radio frequency-based techniques. There is not specific information about the detection sensors, classification algorithms and tracking capabilities, as well as the mitigation technologies used. No images of the system were found.
EOS Slinger [49] Australia	The system combines 4-Axis electro optical sensor unit with an echodyne radar for drone detection and tracking. Mitigation action is done by a M230LF cannon with proximity sensing ammunition.
Zala Aero Group Aerorex [50] Russia	It is mainly a mitigation system (soft kill) with three signal suppression modules for 2.4 GHz and 5.8 GHz frequencies, as well as for satellite navigation signal suppression.
Roselektronika Zaschita [51] Russia	It consists of a set of passive sensors that do not emit any radiation. To detect the target, they use external signals, such as those from digital television, which bounce off the drone. Permission is not required for the use of radio frequencies, facilitating civilian use. However, passive sensors present lower detection capabilities. EO / IR sensors are likely not integrated in the system. Drone mitigation is performed by radio waves jamming.
China Electronic Technology Group Corporation YLC-48 [52] China	YLC-48 system combines 3D S-band low-altitude surveillance radar and jamming technology to detect and counter unauthorized drones (soft kill).
DJI Aeroscope [53] China	Aeroscope system is designed to identify and monitor drones in restricted areas, providing authorities with information to manage and control UAV operations. It covers a range up to 50 km. It analyzes the electronical signals between drones and remote control. The datasheet does not provide information about the sensing unit and the mitigation actions provided by the system
ASELSAN iHTAR [54] Turkey	C-UAS system to neutralize mini and micro drone threats in urban and rural environments. It is used for protection of critical facilities, prevention of illegal border infiltration and safety of highly populated events. The system includes a Ku-band, pulsed Doppler radar with pulse compression (360º continuous or sector scanning, 30 rpm rotation speed and 40º instantaneous elevation coverage), thermal imaging system developed for long distance surveillance, and high-definition daytime cameras. Mitigation action is provided by a programmable RF jammer system (soft kill).
Kongsberg CORTEX Typhon [55] Norway	It integrates a radar, electro optic and Teledyne FLIR thermal cameras for drone detection. The system works in combination with the Kongsberg Remote Weapon Station for threat mitigation (hard kill).

Table 1 may not list all the C-UAS available on the market, but it is a representative example of the main technologies employed in these systems. It has been challenging to find detailed information on Chinese or Russian military systems. We assume these countries maintain a culture of stringent secrecy around their military and defense capabilities, particularly concerning cutting-edge technological advancements. This difficulty to achieve information could be further compounded by language barriers, with much of the information and documentation predominantly available in Chinese or Russian, limiting accessibility for global researchers and analysts, typically using English as main or second language. Consequently, the scarcity of openly available and detailed insights into Chinese or Russian C-UAS systems poses a challenge for comprehensive comparative analysis and a

 doi:10.20944/preprints202402.0551.v1

nuanced understanding of the global landscape of defense technology. The present work has to confine itself to this limitation.

The review conducted on commercial C-UAS systems showcases a diverse range of solutions for threat detection, target classification, tracking, and threat mitigation. Within the detection and tracking phase, most manufacturers present a combination of radar technologies (with some emphasizing the use of passive systems) and passive image sensor technologies (typically electro-optical and thermal sensors). Conversely, few incorporate acoustic sensors, or at least, their presence in the specifications is not clearly indicated. Active optical systems such as LiDAR, used in other applications (e.g., autonomous robotics or surveying), are not typically included in C-UAS technology, despite their ability to quickly provide target range, azimuth, and elevation. Regarding classification, several manufacturers propose the utilization of AI systems. However, specific details about the algorithms employed are not provided. When it comes to the mitigation phase, typically two options are showcased: soft kill and hard kill approaches. The former mainly focuses on jamming the GNSS navigation system and the RF connection between the drone and the remote control. Soft-kill approaches are designed with a dual nature, aiming to defend critical infrastructure or safeguard gatherings of people (civil domain), as well as to protect military assets. On the other hand, hard-kill solutions are specifically oriented towards military applications, and they typically employ armament systems such as machine guns or cannons. Figures 1 and 2 show a selection of commercial C-UAS systems. The first one is more oriented to the protection of critical infrastructures or threats to the civil society, while the second one includes military systems.

Figure 1. C-UAS commercial systems with civil orientation (sources: manufacturers web datasheets [34,35,41,42,44,51]).

 doi:10.20944/preprints202402.0551.v1

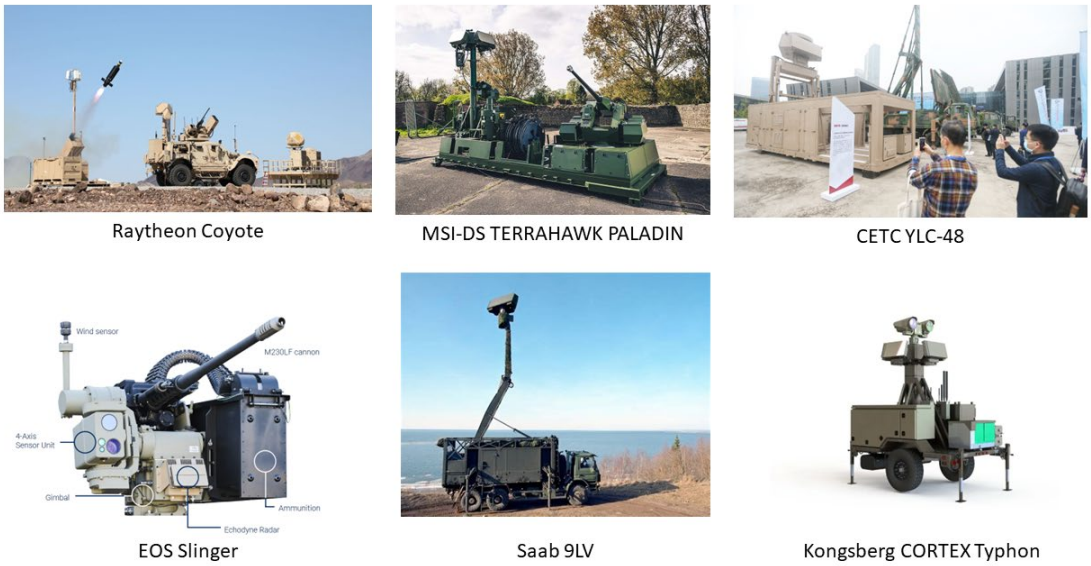

Figure 2. C-UAS commercial systems with military orientation (sources: manufacturers web datasheets [29,34,45,49,52,55]).

3. Technology behind detection, tracking and identification

The existing technology behind counter drone includes different active and passive detection sensors, as well as algorithms for tracking and threat classification. The fundamental principles of these technologies are described below.

3.1. Passive radar

Passive radar systems exploit existing electromagnetic signals like TV or radio broadcasts, emitted by other sources [56,57]. These systems use these signals as "illuminators of opportunity" to detect and track objects like drones, by analyzing the echoes or reflections caused by those objects on the ambient signals. The specific range of frequencies can vary based on the system and its intended application. However, these devices often utilize frequencies within the UHF (Ultra High Frequency) and VHF (Very High Frequency) bands, which generally span from about 30 MHz to 3 GHz.

Research activities in passive radar technology focus on the detection of small air vehicles in high-density target scenarios such as airport terminals, where strong reflections by high radar cross-section targets are likely to prevent the detection of very weak target echoes [58]. Other works employ real-time bistatic passive radars, utilizing software-defined radio and signal processing capabilities to detect and track UAVs in areas near critical infrastructures [59].

There are two primary types of passive radar systems:

- Cooperative systems use signals from collaborative sources, like commercial radio or TV stations, where the broadcaster is aware and agrees to support the radar function.
- Non-cooperative systems work with ambient signals from untended sources without their explicit cooperation. They are more challenging as they need to extract information from signals not meant for radar purposes.

Passive radar has several advantages such as cost-effectiveness (no need for expensive dedicated transmitters); stealth and low observable operations (harder to detect or jam since they do not emit their own radar signals); and reduced vulnerability (lack of a transmitted signal reduces the risk of being targeted by adversaries). The architecture of passive radar systems (Figure 3) involves several key components working together to detect and track targets using ambient electromagnetic signals.

- Receivers: These are the main primary components that capture and process the incoming electromagnetic signals. They consist of antennas, RF (Radio Frequency) from-ends and

 doi:10.20944/preprints202402.0551.v1

digitizers. Receivers are designed to cover a broad spectrum of frequencies to capture signals from various sources like FM/AM radio, TV broadcasts or other radar systems.

- Signal processing units: Once the signals are captured, sophisticated signal processing algorithms are employed to extract relevant information. This includes filtering, correlation, waveform analysis, and target detection algorithms. Advanced digital signal processing techniques are crucial to separate the desired echoes from background noise or clutter.
- Target detection and tracking: After processing, the system identifies potential targets by analyzing the echoes or reflections within the received signals. Tracking algorithms then determine the position, velocity, and trajectory of the detected targets over time. These algorithms can employ techniques like Kalman filtering or data association methods to track multiple targets accurately.
- Database and signal library: Passive radar systems often rely on databases containing information about known transmitters and their characteristics. These data assists in target identification and discrimination, especially in non-cooperative systems. Signal libraries help in cross-referencing detected signals with known patterns to identify specific aircraft.
- Calibration and synchronization: Ensuring accurate detection and tracking requires precise calibration of receivers and synchronization of signals. Calibration procedures are essential to compensate for differences in receiver characteristics and environmental factors affecting signal propagation.
- Integration and networking: Depending on the application, passive radar systems may need to be combined with other sensor systems or radar networks for comprehensive situational awareness. Networking capabilities enable data sharing and integration with broader defense or surveillance systems.
- Power and cooling systems. Passive radar systems, especially those deployed in mobile or remote locations, require adequate power supply and cooling mechanisms to ensure continuous and reliable operations.

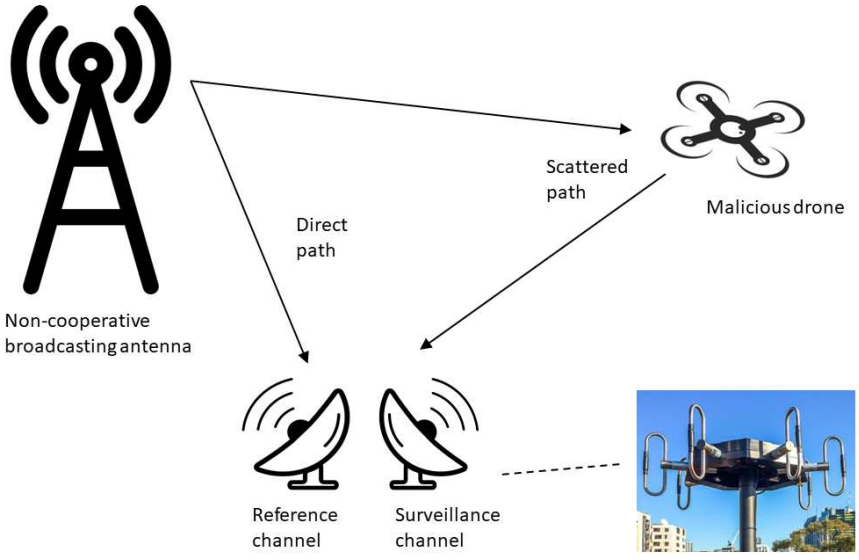

Figure 3. Diagram and image of the system (passive radar).

3.2. Microphones

Acoustic sensors play a crucial role in C-UAS, particularly for detecting and identifying small drones. These sensors are designed to capture and analyze sound waves emitted by drones, helping in their detection, classification, and tracking.

 doi:10.20944/preprints202402.0551.v1

Siewert et al. (2019) conducted an initial evaluation to assess the potential reduction of false alarm cues generated by digital cameras [60]. They explored the integration of supplementary acoustic cues and proposed future work concepts for the fusion of visual and acoustic data. The study presented experimental results to establish the feasibility of the camera system in narrowing the EO/IR re-detection search space, both with and without acoustic data fusion for slew-to-cue message generation.

Dumitrescu et al. (2020) explored the development of an intelligent, flexible, and reliable acoustic system designed to discover, locate, and transmit the position of drones [61]. The system utilized a dedicated spiral microphone array with MEMS microphones. Detection and tracking algorithms were implemented based on spectrogram decomposition and adaptive filters. Various techniques, including Cohen class decomposition, log-Mel spectrograms, harmonic-percussive source separation, and raw audio waveforms, were employed for drone classification within the perimeter of interest.

Ahn and Kim (2021) proposed a drone position estimation algorithm using an acoustic array to complement the challenges faced by vision cameras in detecting sudden directional shifts, occurrences, and speed of drones [62]. They emphasized the significance of integrating acoustic sensors, particularly when a drone is not visible to the camera due to factors such as building occlusions. The proposed algorithm converted sound data into images via a mel-spectrogram, facilitating the fusion of image and sound sensors. The drone's position was estimated using a Convolutional Neural Network, specifically the A-shape network. With this approach, they achieved a RMSE (Root Mean Square Error) of approximately 13 pixels.

Kadyrov (2022) designed and built a system with multiple acoustic sensors for drone detection and tracking using Steered-Response Phase Transform (SRP-PHAT) and narrow-band frequency classification [63]. The system, equipped with seven microphones, underwent testing with different multi-rotor drones, and acoustic signatures were collected to estimate detection distances. The acquired data were then used to develop a straightforward method for estimating acoustic detection distances using the passive sonar equation.

Ding et al. (2023) presented a 64-channel microphone array, providing semispherical surveillance with a high signal-to-noise ratio for sound source estimation [64]. The system, combined with a long-range LiDAR and digital camera, employed a coarse-to-fine, passive-to-active localization strategy for wide-range detection and high-precision 3D tracking. An environmental denoising model was trained to enhance fidelity and overcome traditional sound source location drawbacks in the presence of noise interference. The solution effectiveness was validated through field experiments.

Ivancic et al. (2023) reported on the design, modeling, analysis, and evaluation of a micro-mechanical acoustic vector sensor array [65]. The system, validated in the laboratory using multiple acoustic sources like drones, operated at resonances, providing high acoustic sensitivity and a high signal-to-noise ratio. The array demonstrated unambiguous, 360-degree, in-plane, azimuthal coverage, and during tests, provided an acoustic direction of arrival with an average error within 3.5º.

Fang et al. (2023) employed Distributed Acoustic Sensing (DAS) using optical fibers for drone surveillance [66]. The system demonstrated ultra-high measured sensitivity and the capability for high-fidelity speech recovery. Using a series of Fiber-Optic Acoustic Sensors (FOASs) over a long distance via optical fiber, the DAS enabled intrinsic synchronization and centralized signal processing. Drone detection and localization were successfully demonstrated in tests using a sensing array of four FOASs, achieving accurate drone localization with a RMSE of 1.47 degrees through acoustic field mapping and data fusion.

The architecture of microphone sensing applied to counter drone (Figure 4) presents the following main elements:

- Detection mechanism: Acoustic sensors detect drones by capturing the distinct sound signatures produced by their motors, rotors, or propellers. Each drone type has a unique acoustic fingerprint, which helps in distinguishing between different models.

 doi:10.20944/preprints202402.0551.v1

- Microphone arrays: These sensors often use arrays of microphones strategically placed to capture sound from various directions. The use of multiple microphones enables to determine the direction and location of the drone based on the differences in sound arrival times and intensities.
- Signal processing: Similar to passive radar systems, signal processing plays a vital role. Advanced algorithms analyze the captured sound data, filter out background noise, and extract relevant features to identify and classify drones. Machine learning and pattern recognition techniques are often employed for more accurate drone classification.
- Integration with other sensors: Acoustic sensors are frequently integrated into multi-sensor C-UAS systems. Combining acoustic sensors with radar, electro-optical or RF sensors enhances overall detection capabilities and provides redundancy in case of sensor limitations or environmental factors.
- Operational considerations: Acoustic sensors can operate effectively in various environments and conditions, including urban settings or areas with relatively high ambient noise. They offer a covert detection method, as they do not emit any signals, making them harder for adversaries to detect or evade.
- Challenges: Acoustic sensors may face challenges in environments with high background noise levels, weather effects, or when drones employ stealthy techniques like flying at low speeds or hovering quietly.
- Scalability and deployment: These sensors are often deigned to be scalable, allowing deployment in various configurations, from fixed installations to portable or mobile units suitable for rapid deployment in different scenarios.
- Regulatory considerations: Deployment of C-UAS systems, including acoustic sensors, often involves compliance with local regulations and privacy concerns regarding the interception of audio signals.

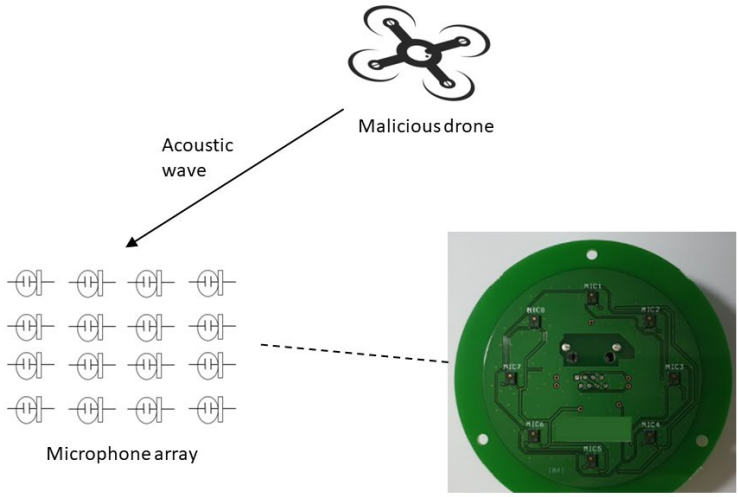

Figure 4. Diagram and image of the system (microphones).

3.3. Electro-optical and infrared sensors

Electro-optical / Infrared (EO/IR) sensors are pivotal components in C-UAS. These sensors leverage the electromagnetic spectrum, particularly the visible, infrared, and ultraviolet wavelengths, to detect, track, and identify unmanned aerial systems. EO sensors show a wavelength range between 400 and 700 nm (visible light). IR sensors can be divided in two main groups:

- Near Infrared (NIR) and Short-Wave Infrared (SWIR), with wavelengths between 700 to 1300 nm. These devices are effective in moonlit or starlit conditions and require some ambient light to function properly.

 doi:10.20944/preprints202402.0551.v1

- Thermal Imaging, which operates in the Mid-Wave Infrared (MWIR) and Long-Wave Infrared (LWIR), commonly in the 7 – 17 μm range. These cameras provide images based on temperature differences and are effective even in total darkness or adverse weather conditions.

Visible (EO) systems offer high-resolution imaging capabilities, typically measured in megapixels. The spatial resolution can vary from standard definition to high definition and ultra-high-definition levels, providing detailed visual information about the target. Infrared (IR) systems, particularly thermal imaging ones, present lower resolution compared to visible cameras, influencing the level of detail in thermal imagery. For instance, the TacFLIR 380-HD from TeledyneFLIR features a thermal sensor (range 3 – 5 μm) with a resolution of 640 x 512 pixels, a color high-definition camera with 720/1080 HD and NTSC/PAL resolution (zoom ratio 120x), and a SWIR camera with 720/1080 HD and NTSC/PAL resolution [67].

Sievert et al. (2018) demonstrated a conceptual architecture for integrating passive sensor nodes into a local sensor network for drone traffic management (UTM) [68]. The research aimed to assess the feasibility of using multiple passive sensor nodes, integrating Electro-Optical/Infrared and acoustic arrays networked around a drone traffic management operating region (Class G; uncontrolled airspace for general aviation). The system underwent testing using ADS-B data from a Micro Air Vehicle as the first ground truth. The validation method involved human review of triggered detection image capture, allowing for performance assessment for non-compliant drones and other aerial objects (birds and bugs). The networked passive sensors were designed to meet Class G and geo-fence UTM goals and assist with urban UTM operations.

Hao et al. (2020) presented the results of experiments using an Electro-Optical (EO) sensor to detect an aerial intruder based on a small unmanned aerial system [69]. They developed a simple drone detection algorithm tested in a series of field experiments to assess its effectiveness.

Goecks et al. (2020) combined visible and infrared spectrum imagery using machine learning for small unmanned aerial system detection [70]. This research utilized heightened background contrast from the LWIR sensor combined with higher resolution images from a visible spectrum sensor. A deep learning model was trained, demonstrating effective detection of multiple drones flying above heat sources. They achieved a detection rate around 70% and a false alarm rate around 3%. Authors proposed the use of arrays of these small and affordable sensors to accurately estimate the 3D position of UAVs.

Muller et al. (2022) presented a drone detection, recognition, and assistance system for C-UAS with visible, radar, and radio sensors [71]. It included four high-resolution visual optical cameras, offering full 360-degree observation at distances up to several hundred meters. Drones, visible as small dots in an image, were detected and tracked with a GPU-based point target detector. A full HD camera on a pan-and-tilt unit successively captured high-definition images of each target, which were classified using a Convolutional Neural Network (CNN). In this way, authors managed to identify UAVs and discard false alarms such as birds or other flying objects. All information was combined with radar and radio sensor subsystems and visualized in a 2D or 3D map.

Shovon et al. (2023) provided a comparative analysis of deep learning algorithms for optical drone detection [72]. They performed a comparative performance analysis of four state-of-the-art deep learning-based object detection algorithms, namely YOLOv5 small and large, SSD, and Faster RCNN. The study reveals that the YOLOv5-based models and the Faster RCNN model are very close to each other in terms of accuracy, while they outperform SSD. The YOLOv5-based models are also significantly faster than both SSD and Faster RCNN algorithms.

Ojdanic et al. (2023) presented a feasibility analysis of optical drone detection over long distances using robotic telescopes [73]. The system comprised a high-precision mount and a telescope equipped with a camera. Drones were detected in the video frames using a custom version of a YOLOV4 neural network. The proposed system, which used an f/10 telescope with a focal length of f = 2540 mm and a camera equipped with a 7.3 mm x 4.1 mm sensor, allowed for a significant increase in the optical detection range to more than 3 km of drones down to 0.3 m in diameter under daylight conditions and sufficient contrast, extending the reaction time significantly for C-UAS.

 doi:10.20944/preprints202402.0551.v1

The architecture of an electro-optical infrared system (Figure 5) presents the following main elements:

- Sensors (visible and infrared cameras). These are the primary devices capturing imagery in the visible and infrared spectra. Visible cameras provide visual information, while infrared cameras (thermal sensors) detect heat signatures emitted by drones or their components.
- Optics and lens assemblies: High-quality lenses and optical components focus and direct light onto the sensor arrays, ensuring clarity, sharpness, and optimal image quality.
- Signal processing units. Image and signal processors. These units process the captured data from the sensors. They perform tasks such as noise reduction, image enhancement, digital zoom, and fusion of visible and infrared imagery. Advanced algorithms analyze the processed data, extract relevant features, and aid in target detection, classification, and tracking.
- Tracking and identification: Target trackers use algorithms to maintain the position, trajectory, and other relevant information about detected drones in real-time. Identification features can be applied by analyzing shape, size, movement patterns, and thermal signatures.
- Data fusion and analysis: Fusion engines integrate data from various sensors (e.g., EI, IR radar, acoustic) to improve detection accuracy and reduce false alarms.

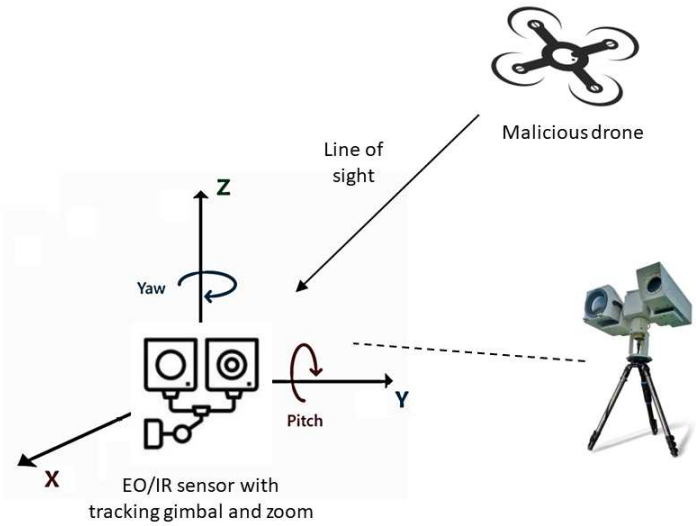

Figure 5. Diagram and image of the system (EO/IR sensors).

3.4. Radio Frequency (RF) signal analyzer

Radio Frequency (RF) signal analyzers are employed for detecting drone communications with remote control, mainly operating within the 2.4 GHz and 5.8 GHz frequency bands.

- The 2.4 GHz band is extensively used for various wireless communications, including Wi-Fi networks, Bluetooth devices, and consumer-grade drones. Its popularity stems from good signal penetration and range, making it a preferred choice for drone control.
- The 5.8 GHz band is often utilized by higher-end or advanced drones due to its capacity to handle more data, potentially offering better performance in areas with high interference.

These frequencies fall within the ISM, designated internationally for various radio-frequency devices, including those used in industrial, scientific, and medical applications. Although drones often use these frequencies, it is not a limiting factor, as some systems operate in other frequency ranges based on their design and purpose. C-UAS systems designed to detect and mitigate drone threats often focus their RF subsystems on monitoring and analyzing signals within these bands to identify drone communications.

Medaiyese et al. (2022) proposed a wavelet transform analytics for RF-based UAV detection and identification system using machine learning [74]. They exploited RF control signals from unmanned

 doi:10.20944/preprints202402.0551.v1

aerial vehicles for drone detection and identification. By considering each state of the signals separately for feature extraction and comparing the pros and cons for drone detection and identification, they built different models using various categories of wavelet transforms. Their study revealed that using the wavelet scattering transform to extract signatures (scattergrams) from the steady state of the RF signals at 30 dB SNR, and using these scattergrams to train SqueezeNet, achieved an accuracy of 98.9% at 10 dB SNR.

Alam et al. (2023) presented an RF-enabled deep-learning-assisted drone detection and identification system [75]. They utilized multiscale feature-extraction techniques without manual intervention to extract enriched features for the model. Residual blocks were employed to learn complex representations and overcome vanishing gradient problems during training. The model's performance was evaluated across various Signal-to-Noise Ratios (SNR), yielding an overall accuracy, precision, sensitivity, and f-score of 97.53%, 98.06%, 98.00%, and 98.00%, respectively, for RF signal detection from 0 dB to 30 dB SNR.

Aouladhadj et al. (2023) showcased a drone detection and tracking system using RF identification signals [76]. They presented a technique for detecting drone models using Identification (ID) tags in Radio Frequency (RF) signals, enabling the extraction of real-time telemetry data through the decoding of drone ID packets. The system, implemented with a development board, allowed efficient drone tracking, accurately estimating drone's 2D position, attitude, and speed in real time.

Almubairik et al. (2024) demonstrated RF-based drone detection with a deep neural network [77]. Their case study compared the impact of utilizing magnitude and phase spectra as input to the classifier, revealing that prediction performance was better when using the magnitude spectrum. However, the phase spectrum proved more resilient to errors due to signal attenuation and changes in surrounding conditions.

RF detectors in drone detection systems use various architectures to effectively identify and analyze radio signals associated with drone communications. Figure 6 presents a diagram of the RF detector architecture.

- Spectrum Analyzers: These devices analyze a wide range of frequencies to detect signals across the RF spectrum, providing a comprehensive view of the frequency spectrum for the identification of signals used by drones within specific frequency bands. Modern spectrum analyzers often use digital signal processing for more accurate and faster analysis.
- Software-Defined Radios (SDR): SDRs offer flexibility by using software to define the functionality of the radio system. They allow for versatile signal processing and analysis, making them suitable for detecting and decoding various RF signals, including those used by drones. SDRs can be reconfigured and updated through software, adapting to changing signal patterns.
- Direction Finding Systems: RF detectors may incorporate direction-finding capabilities to determine the origin of drone control signals. This can be achieved using antenna arrays or specialized antennas to detect signal angles, providing information about the drone's location or the control station direction.
- Signal Processing and Pattern Recognition: Advanced RF detectors use sophisticated signal processing algorithms and pattern recognition techniques to distinguish drone communication signals from background noise or other legitimate wireless communications. Machine learning and artificial intelligence can be employed to accurately identify and classify these signals.
- Networked Sensors: In some cases, multiple RF detectors are strategically positioned and networked to create a more comprehensive detection system. These detectors work together to provide coverage over a wider area, allowing for triangulation and better tracking of drone movements.
- Frequency Hopping and Spread Spectrum Analysis: Some drones use frequency hopping or spread spectrum techniques to avoid detection. RF detectors need to be equipped with the capability to handle and analyze signals that rapidly change frequencies or use wider bandwidths.

 doi:10.20944/preprints202402.0551.v1

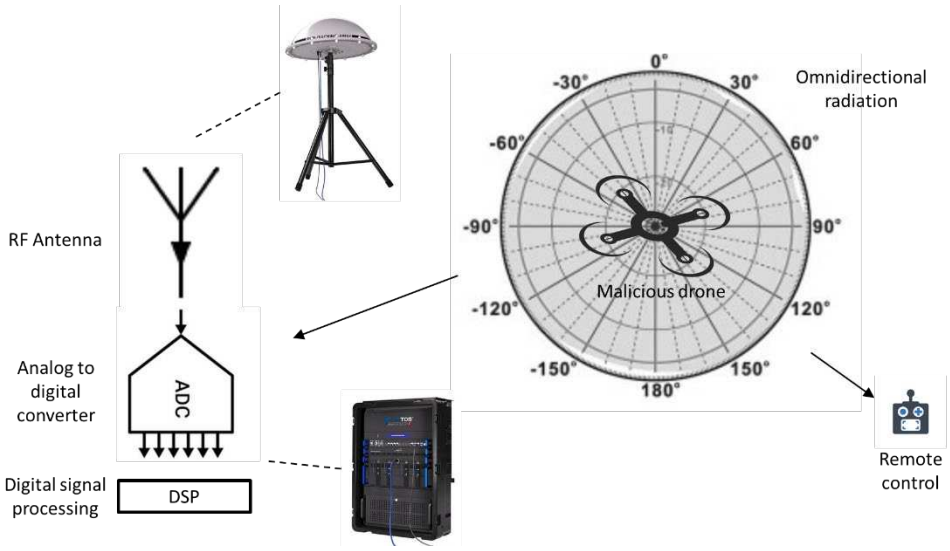

Figure 6. Diagram and image of the system (RF signal analyzer).

3.5. Active radar

An active radar system for drone detection operates emitting electromagnetic waves, typically in the radio frequency spectrum, and detecting the echoes reflected off aerial targets, such as drones. The main frequencies used for drone detection are Ka-band (26.5 GHz – 40 GHz), Ku-band (12 GHz-18 GHz, X-band (8 GHz – 12 GHz), C-band (4 GHz – 8 GHz) and S-band (2 GHz – 4 GHz). Higher frequencies provide high resolution and precision for short-range detection. On the other hand, they are more vulnerable to atmospheric attenuation and limited in range compared to lower frequencies. A balance between target cross-section and detection range is always necessary to select the radar frequency.

In their 2020 study, Riabukha et al. conducted a comprehensive review on the radar surveillance of Unmanned Aerial Vehicles (UAVs), an actively evolving field of scientific research [78]. This article offers an in-depth analysis of publications focusing on methods and radar systems for the detection and recognition of various classes and types of UAVs. Notably, the most challenging targets for radar detection are small-sized, low-speed UAVs flying at low and extremely low heights with respect to terrain. While modern radar systems effectively detect large and medium-sized UAVs; specialized, highly efficient, mobile, portable, and cost-effective active UAV detection radars are recommended for small UAVs. The technical requirements for such radars are defined, accompanied by recommendations for implementation. The article suggests employing high-performance protection systems based on adaptive lattice filters to safeguard UAV detection radars from noise jamming and passive interference. The research highlights that methods for recognizing UAV classes and types represent advancements in the existing theory and technology of radar target recognition.

In 2021, Wallentine et al. introduced an autonomous spherical passive/active radar calibration system [79]. This self-contained, multifunctional system served as a Passive Spherical Reflector, Active RF Repeater, Synthetic Target Generator, and UWB RF Sensor and Data Recorder for the radar under test or the localized RF environment. Leveraging technological advances in autonomous airborne drones, miniaturized digital RF Systems on Chips (RFSoCs), and other miniature electronics, this innovative calibration device facilitated precision calibrations over extensive open-air test volumes. The paper highlights early efforts to parameterize and develop the calibration system, emphasizing recoverable, reusable CDs for precision calibrations over open-air test volumes used for dynamic aircraft RCS measurement, test and verification, or Time-Space Position Information (TSPI) test range tracking radars. SPARCS promises unprecedented capabilities for radar instrumentation calibration, target emulation, environmental assessment, and in situ, real-time calibration.

In 2022, Scheneebeli et al. presented a drone detection system featuring a multistatic C-band radar [80]. The system detection capabilities were tested during two field campaigns in Switzerland.

 doi:10.20944/preprints202402.0551.v1

The C-band system, comprising one transmit and two receive nodes, underwent geometric and radiometric calibration using a specific multistatic target simulator. By comparing GPS trajectories of a DJI Phantom 4 drone to radar detections, it was discovered that inherent pointing angle and range biases in the radar system could be corrected straightforwardly using virtually generated radar targets as references. Post-correction, deviations between drone GPS positions and radar detections were found to be on the order of 5 meters.

In 2023, Abratkiewicz et al. addressed the challenge of target acceleration estimation in both active and passive radars [81]. The increasing maneuverability of flying targets poses a detection challenge for radars. Rapid acceleration blurs target echoes on the Range-Doppler (RD) map, reducing the signal-to-noise ratio. The article proposes a novel, nonparametric approach to efficiently estimate target acceleration on the RD map, applicable to both active frequency-modulated continuous wave radar and passive radar. The proposed solution is significantly faster, maintaining numerical stability and allowing simultaneous acceleration estimation for multiple targets. Simulation tests and real-life radar signals observing a jet fighter and a drone supported the effectiveness of the proposed technique.

In 2023, Lam et al. presented an initial work with radars operating in the V-band (40 GHz to 75 GHz) applied to drone detection [82]. The paper details drone detection data collected using a 66 GHz research radar. Micro-Doppler signatures of rotating drone rotors were extracted using Short-Time Fourier Transform (STFT) and Continuous Wavelet Transforms (CWT). The study determined that the complex Morlet wavelet provided more detailed micro-Doppler features, enabling the classification of different drones.

The architecture of active radar system (Figure 7) comprises several key components:

- Transmitter: Emits electromagnetic pulses or continuous waves in a specific direction and frequency range, often using a directional antenna. These emitted waves travel through space. When the radar waves encounter a drone, they interact with the drone surface. Some of the energy is absorbed, some scattered, and the rest is reflected back towards the radar system.
- Receiver: Antennas or receiver capture the reflected signal (echoes) that return from the drone. These signals contain information about the drone position, speed, size, and other relevant characteristics.
- Signal processing unit: Processes the received signals to extract meaningful information. This involves analyzing the time delay, phase shift, and amplitude of the returned signals to determine the drone attributes, such as its distance, velocity, and direction.
- Radar systems can employ different techniques like pulse-Doppler, Frequency -Modulated Continuous-Wave (FMCW) or phased-array radar for improved accuracy, range, and capability to detect and track drones. Signal processing algorithms and machine learning models may be used to classify and differentiate drones from other objects, reducing false positives and improving the system overall effectiveness.

 doi:10.20944/preprints202402.0551.v1

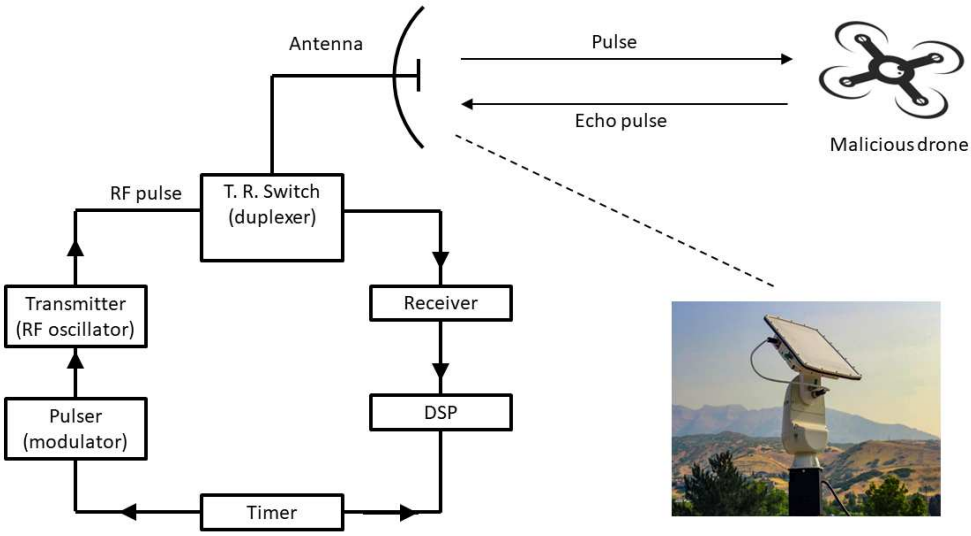

Figure 7. Diagram and image of the system (active radar).

Additionally, active radar systems for C-UAS may face challenges such as mitigating interference from other radar systems, weather conditions affecting signal propagation, and the need for adherence to regulatory constraints regarding spectrum usage and power emission limits. Radar detection of drones presents other problems:

- Small radar cross section: Drones often have small physical dimension and lightweight construction, resulting in a limited radar cross-section. This makes them harder to detect compared to larger objects, requiring radar systems with high sensitivity and resolution.
- Low altitude and maneuverability: Drones can fly at low altitudes and execute erratic maneuvers, apperaring as dynamic and unpredictable targets in radar systems. Tracking such agile and swift movements accurately becomes challenging, especially for traditional radar setups optimized for larger aircrafts with lower maneuverability.
- Clutter and false positives: Radar systems can encounter clutter from various sources such as buildings, trees, birds, and other objects in the vicinity. Distinguishing between drones and these background objects or false targets is crucial to avoid false positives that may lead to unnecessary alerts or alarms.
- Radar cross section variability: The radar cross-section of a drone can vary significantly based on its orientation, material composition, and even flight mode (e.g., hovering, moving forward). This variability makes consistent and reliable detection challenging.
- Stealth technology: Some drones may employ stealth technology or features like radar-absorbing materials, reducing their radar signature intentionally. This makes them even more challenging to detect using conventional radar systems.
- Electronic countermeasures: Advanced drones may be equipped with electronic countermeasures to disrupt radar detection by emitting jamming signals or employing techniques to confuse radar systems, thereby evading detection.

3.6. LiDAR

LiDAR stands for Light Detection and Ranging. It is a remote sensing method that uses light (400 nm – 1540 nm) in the form of a pulser laser to measure distances. The technology operates sending out laser pulses and measuring the time it takes for these pulses to bounce back after hitting objects or surfaces. By collecting millions of these distance measurements per second, LiDAR systems create highly detailed 3D maps or point clouds of the surveyed environment. These maps are used

 doi:10.20944/preprints202402.0551.v1

in various applications, including topographic mapping, urban planning, autonomous vehicle navigation, forestry, and importantly, in counter-UAS systems for drone detection and tracking.

In their 2022 study, Paschalidis et al. demonstrated the feasibility of employing 360º LiDAR in Counter-Unmanned Aerial Systems (C-UAS) missions [83]. The paper showcases results derived from field experiments involving low-altitude maneuvers by various small drones of different sizes and shapes, captured using a low-end Velodyne Hi-Res sensor. The study describes the current state-of-the-art of 3D 360º LiDAR and the algorithm developed to process point cloud data, aiming to reduce the probability of false drone detections, especially in rural environments. The paper also examines the limitations of small drone detection using LiDAR and the impact of low-end sensors on detection rates.

In 2022, Barisic et al. presented a multi-robot system designed for autonomous cooperative counter-UAS missions, encompassing design, integration, and field testing [84]. The authors detailed the hardware and software components of various complementary robotic platforms: a mobile Unmanned Ground Vehicle (UGV) equipped with a LiDAR sensor, a Unmanned Aerial Vehicle (UAV) with a gimbal-mounted stereo camera for air-to-air inspections, and an UAV with a capture mechanism equipped with radars and a camera. The proposed system boasted scalability to larger areas due to a distributed approach and online processing, suitability for long-term cooperative missions, and complementary multimodal perception for detecting multirotor UAVs. Field experiments demonstrated the successful integration of all subsystems, accomplishing a counter-UAS task within an unstructured environment. These results highlight the potential of multi-robot and multi-modal systems for surveillance applications.

Aldao et al. (2022) highlighted the feasibility of using LiDAR systems onboard drones for detecting other aircraft in urban air mobility applications [85]. They simulated a commercial LiDAR model using manufacturer specifications and empirical measurements to determine the scanning pattern. The system detected intruders and estimated their motion using the point cloud generated by the sensor, computing avoidance trajectories in real-time through a Second-Order Cone Program (SOCP). The method demonstrated robust results in different scenarios, with execution times of around 50 milliseconds, making real-time implementation feasible on modern onboard computers.

In 2023, Rodrigo et al. introduced a Continuous-Wave (CW) coherence detection LiDAR capable of detecting micro-Doppler signatures, specifically propeller movements, and acquiring raster-scan images of small unmanned aerial vehicles [86]. The system utilized a narrow-linewidth 1550 nm CW laser and leveraged cost-effective fiber-optics components from the telecommunications industry. Through collimated or focused probe beam geometry, the LiDAR detected characteristic periodic motions of drone propellers at distances up to 500 m. Raster scanning with a galvo-resonant mirror beam-scanner produced two-dimensional images of flying drones up to 70 m range, providing both LiDAR return signal amplitude and target radial speed information per pixel. The raster-scan images, obtained at up to 5 frames per second, enabled discrimination of various drone types based on their profile and even determining the presence of payloads. The study suggests that, with improvements, the anti-drone LiDAR proves a promising alternative to expensive EO/IR and SWIR cameras in counter-UAS systems.

Abir et al. (2023) conducted a study on the robustness of LiDAR-based 3D detection and tracking of drones [87]. They investigated effective detection ranges based on different drone construction materials and assessed the system's 3D detection performance at varying atmospheric visibility conditions. The study also examined the LiDAR-based system's capability to track drone trajectories through real-world experiments and point cloud data processing. Using the Livox Mid-40 LiDAR-based system, they performed a precise tracking of drones at distances up to 80 meters under various environmental conditions.

In comparison with radar there are some important differences to notice:

- Detection principle: LiDAR uses laser pulses to measure distances to objects calculating the time it takes for light to bounce back. It excels in providing highly accurate and precise 3D mapping of the environment. Radar utilizes radio waves to detect objects to detect objects by measuring the measuring the time it takes for radio waves to return after hitting the target. Radar has a

 doi:10.20944/preprints202402.0551.v1

longer detection range compared to LiDAR and can operate effectively in various weather conditions.

- Accuracy and resolution: LiDAR provides extremely high-resolution data, offering detailed 3D mapping of the environment with precise measurements. It is highly accurate in determining object shapes, sizes, and positions. Radar offers longer detection ranges compared to LiDAR but generally has lower resolution. While it can detect objects at greater distances, it generally provides less detailed information about the target characteristics.
- Target classification or differentiation: LiDAR can distinguish between different types of targets due to its high resolution. It can identify and classify objects more precisely, making it suitable for differentiating drones from other aerial or ground-based entities. Radar may struggle to differentiate between different types of objects at longer ranges due to lower resolution. It may detect objects but could have limitations in accurately classifying them.
- Environmental factors: LiDAR performs well in clear atmospheric conditions but might face challenges in adverse weather conditions like heavy fog or rain, as these conditions can interfere with light transmission. Radar is less affected by environmental factors like fog or rain compared to LiDAR because radio waves are less impacted by such conditions.

In the context of C-UAS, LiDAR high-resolution capabilities make it particularly effective for precise detection, tracking and classification of drones in clear weather conditions and environments where detailed mapping and differentiation between objects are crucial. Figure 8 presents a LiDAR signature from a Matrice 300 drone. Data obtained in University of Vigo, Spain. Radar, on the other hand, might excel in longer-range detection in adverse weather but potentially less detailed information about the detected objects. Integrating both technologies can offer a more comprehensive approach to counter-UAS systems, leveraging the strengths of each, for improved detection and mitigation capabilities.

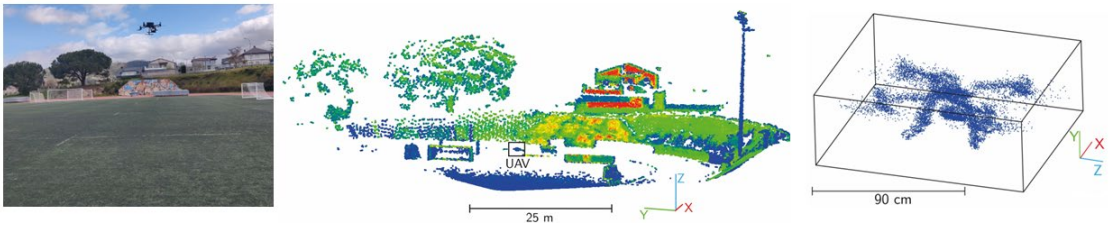

Figure 8. LiDAR signature obtained with Livox Avia from a Matrice 300 drone. Image of the drone flying in a sports court at Campus of Ourense, University of Vigo (left), LiDAR point cloud of the scenario (center), and detailed point cloud of the drone (right).

The architecture of a LiDAR system (Figure 9) used in counter-UAS operations typically involves several components working together to detect, track, and potentially mitigate unauthorized drones:

- Laser emitters: The system includes high-powered laser emitters capable of emitting laser pulses. These pulses are reflected in the environment and return to the sensor.
- Receiver unit: This component receives the reflected laser pulses from the environment, including any drones present in the monitored airspace. It measures the time it takes for the pulses to return.
- Digital signal processing: The received data undergoes signal processing to compute the time instant and intensity of the returning laser pulses. This processing includes calculating distances, angles, intensity, and other parameters necessary for 3D mapping and object identification.
- Scanning mechanism: The LiDAR system often includes a scanner that directs the laser pulses over a designated are. This mechanism can be static or rotating, enabling coverage of different angles and regions.
- Data fusion and analysis: The data collected from the LiDAR system are fused and analyzed to create a comprehensive 3D map or point cloud of the environment. This map includes the location and movement of detected drones.

 doi:10.20944/preprints202402.0551.v1

- Detection and tracking algorithms: Specialized algorithms are employed to detect and track drones within the collected data. These algorithms differentiate between drones and other objects, calculate their trajectories, speeds, and potential threat levels.

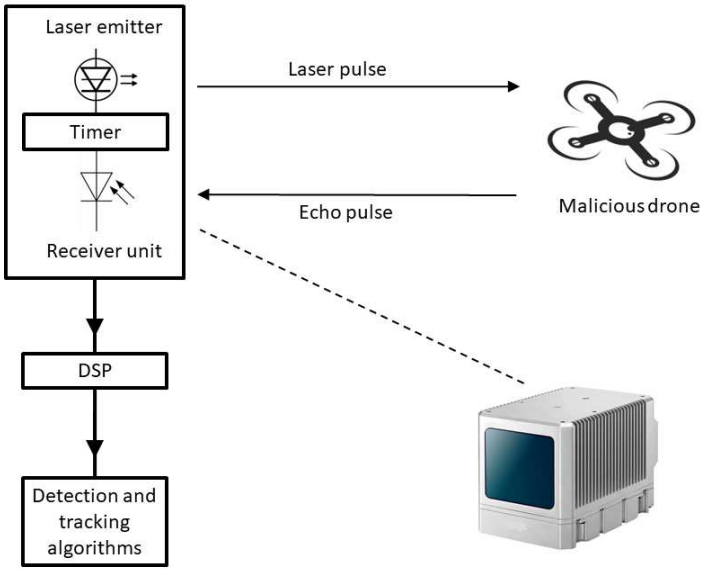

Figure 9. Diagram and image of the system (LiDAR).

3.7. Sensor fusion

Sensor fusion plays a significant role in C-UAS applications, particularly in detecting, tracking, and neutralizing unauthorized or potentially threatening drones. It enhances situational awareness and enable effective countermeasures.

In their study, Koch et al. (2018) presented an innovative approach that holds the potential for a paradigm shift in sensor data fusion: the utilization of tensor decomposition-based multiple sensors tracking filters [88]. This novel fusion engine methodology efficiently combined the complete informational content of advanced sensors and sophisticated dynamic models for drone motion. The application of powerful multilinear decomposition methods for tensors significantly reduced the computational efforts required to generate high-quality tracks for both dim and agile drones. Furthermore, the deterministic performance characteristics of tensor decomposition-based fusion offer beneficial implications for system design aspects. These advanced algorithms for multiple sensor data fusion play a pivotal role in the design of counter-drone systems.

In the realm of C5ISR systems (Command, Control, Communications, Computer, Cyber, Intelligence, Surveillance, and Reconnaissance), addressing technological challenges is feasible but necessitates close cooperation between military and police forces, research institutes, and relevant industries. Especially in safeguarding stationary equipment and mobile units in urban or open terrain, the integration of drone detection/tracking/classification in decision support systems proves to be crucial.

Kondru et al. (2018) contributed to the field by demonstrating the mitigation of target tracking errors and drone response through multi-sensor data fusion [89]. Their paper introduced methods and state estimation techniques based on multi-sensor data fusion to alleviate position errors induced by electronic countermeasures. The research entailed a comprehensive mathematical modeling and simulation of the proposed system for further exploration. The inclusion of two sensors, namely RADAR and FLIR (Forward Looking Infrared), along with their mathematical models, is a key aspect. The paper adopted a state variable approach to describe the motion characteristics of the target and the sensor measurement model, with a focus on evaluating the performance of tracking filters. Experimental results in MATLAB showcased fusion architectures that yield superior tracking results

 doi:10.20944/preprints202402.0551.v1

with fewer residual errors. Additionally, for nonlinear target motion, the robust particle filter demonstrated its efficacy and achieved the desired response.

Baptista et al. (2020) presented a surveillance system designed to detect malicious and/or illicit aerial targets [90]. The approach involved tracking moving aerial objects using a static camera. When a tracked object was deemed suspicious, the camera zoomed in to capture a snapshot, subsequently classified as an aircraft, drone, bird, or cloud. The authors proposed the classical technique of two-frame background subtraction for detecting moving objects. They employed the discrete Kalman filter for predicting the location of each object and the Jonker-Volgenant algorithm for matching objects between consecutive image frames. A deep residual network, specifically ResNet-50 retrained for the purpose, was utilized for image classification. The system's performance was evaluated under real-world conditions, demonstrating its capability to track multiple aerial objects with acceptable accuracy and achieve high classification accuracy.

Koteswara et al. (2020) showcased the implementation of the Unscented Kalman Filter for autonomous aerial vehicles in target tracking [91]. The study involved smoothing noise-corrupted measurements and simultaneously determining the vehicle's velocity components. A detailed Monte-Carlo simulation was conducted to compare the algorithm's outputs with those of the extended Kalman filter, providing valuable insights for releasing weapons onto the target.

Sie et al. (2021) introduced the use of Correlation Filters and Integrated Multiple Model (IMM) for filtering the position measurement of fast-moving drones acquired through computer vision [92]. Recognizing the non-linear nature of the maneuvering movement of drones, the paper opted for integrating multiple filters to estimate the drone's position at a low computational cost. The IMM switched between the Constant Velocity (CV), Constant Acceleration (CA), and Constant Turn (CT) models with a Markov Chain in different flight scenarios based on the drone's movement. Other filters, including Kernelized Correlation Filter (KCF), Particle Filter (PF), and Discriminative Correlation Filter (DCF) models, were also presented for direct comparison.

Liang et al. (2021) presented a multi-camera multi-target drone tracking system featuring trajectory-based target matching and re-identification [93]. The integrated system's algorithm combined target tracking, localizing, and identifying schemes, demonstrating the ability to use multiple cameras from different viewing angles to simultaneously track moving objects in the camera frames. The algorithm incorporated hybrid detection (motion-based blob detection and appearance-based detection) to detect moving objects. Trajectories of tracked objects were analyzed for motion-based detection, while Yolo V3 detection algorithm was employed for appearance-based detection. The integrated target identification algorithm successfully matched and re-identified targets within and among cameras, leading to subsequent 3D localization. The system was tested for tracking multiple aerial and ground targets in real-time.

Son et al. (2021) proposed a fast and accurate drone tracking system utilizing two trackers, a predictor, and a refinement process [94]. One tracker identified a moving target based on motion flow, while the other located the Region Of Interest (ROI) using histogram features. A Kalman filter was employed for trajectory estimation, with the predictor contributing to maintaining tracking even when trackers fail. The refinement process determined the target's location by leveraging ROIs from both trackers and the predictor. In experiments with a dataset containing tiny flying drones, the proposed method achieved a success rate 1.134 times higher than conventional tracking methods, operating at an average runtime of 21.08 frames per second.

Montañez et al. (2023) demonstrated an application of data sensor fusion using the extended Kalman filter algorithm for the identification and tracking of moving targets from LiDAR – Radar data [95]. To enhance data acquisition resolution, the study integrated data sensor fusion systems, measuring the same physical phenomenon from two or more sensors simultaneously. The paper employed the Constant Turn and Rate Velocity (CTRV) kinematic model of a drone, including angular velocity not considered in previous works. The Extended Kalman Filter (EKF) was applied to detect moving targets, and the performance was evaluated using a dataset that includes position data captured from LiDAR and Radar sensors. The study introducef additive white Gaussian noise to the data to simulate degraded conditions, evaluating the Root Mean Square Error (RMSE) against

 doi:10.20944/preprints202402.0551.v1

increased noise power. Results showed a 0.4 improvement in object detection over other conventional kinematic models that do not account for significant trajectory changes.

Zitar et al. (2023) provided an extensive review of objects and drone detection and tracking methods [96]. The article presents state-of-the-art methods used in drone detection and tracking, offering critical analysis and comparisons based on recent research material. The analysis includes comparisons for drone tracking using Linear Kalman Filters (LKF) versus Nonlinear Polynomial Regression (NPR) techniques. The findings suggest the need for both methods under different circumstances, depending on the noise conditions of the measurements. Additionally, the study highlights the emergence of new methods, such as Artificial Intelligence (AI)-based techniques, in drones' detection and recognition. Detection methods are discussed as separate entities or combined with tracking techniques, offering a comprehensive literature review.

Alhadhrami et al. (2023) introduced a reinforcement learning approach for the automatic adaptation of the process noise covariance (Q) in a Kalman filter tracking system [97]. The Q value holds a pivotal role in estimating future state values within this tracking framework. Proximal Policy Optimization (PPO), recognized as a state-of-the-art policy optimization algorithm, was utilized to determine the optimal Q value, thereby enhancing tracking performance as quantified by the Root Mean Square Error (RMSE). The results showcased the successful learning capability of the PPO agent over time, enabling it to suggest the optimal Q value by adeptly capturing the policy of appropriate rewards under varying environmental conditions. These findings were systematically compared with those obtained through feed-forward neural network learning, the Castella innovation/Q values mapping, and fixed Q values. Notably, the PPO algorithm demonstrated promising results. The researchers employed the Stone Soup library to simulate ground truths, measurements, and the Kalman filter tracking process.

4. Technology behind mitigation

Drone mitigation technologies aim to counteract unauthorized or potentially harmful drone activities [98, 99]. Various technologies have been developed to address the growing challenges posed by drones in different contexts, including security, privacy, and safety (Figure 10). In the upcoming sections, an analysis of some key technologies in drone mitigation is detailed. It is important to note that the effectiveness of soft kill technologies may vary depending on the type of drone, its capabilities, and the countermeasure employed. Additionally, regulations regarding the use of these technologies could vary by country, and careful consideration of legal and ethical implications is necessary.

 doi:10.20944/preprints202402.0551.v1

Figure 10. Image of soft kill (left) [109] and high-energy laser - hard kill (right) [110] mitigation strategies.

4.1. RF jamming (soft kill)

RF jamming disrupts communication between the drone and its operator by emitting signals on the same frequency band used by the drone's remote control [100]. It can prevent the drone from receiving commands or transmitting data, forcing it to enter a fail-safe mode or return to its point of origin. In radio frequency jamming, the following aspects are highlighted:

- Frequency spectrum: Radio-controlled drones typically operate within specific frequency bands for communication between the drone and its remote controller. RF jamming exploits this by transmitting signals within the same frequency range, disrupting the normal communication.
- Waveform generation: RF jammers generate radiofrequency signals with sufficient power to interfere with or overwhelm the signals exchanged between the drone and its remote controller. These signals can be continuous or modulated in various ways.
- Signal strength and interference. The effectiveness of RF jamming relies on the strength of the interfering signal. If the jamming signal is stronger than the drone's control signal, it can disrupt the communication link, rendering the drone unable to receive commands or transmit data effectively.
- Types of jamming: Wideband jamming involves transmitting interference across a broad range of frequencies, affecting multiple communication channels simultaneously. Narrowband jamming targets a specific frequency, or a narrow range of frequencies used by the drone, allowing for more precise disruption.
- Jamming techniques. Continuous Wave (CW) jamming uses a constant signal transmitted on the target frequency to create a steady interference. Pulse jamming is based on intermittent bursts of jamming signals transmitted, disrupting communication intermittently.
- Electronic warfare principles. RF jamming is a subset of electronic warfare, which involves the use of electromagnetic energy to deny or disrupt an adversary's use of electronic devices. In the case of counter-drone applications, the aim is to deny the drone's operator control and communication.
- Legal and ethical considerations: While RF jamming can be an effective soft kill method, its use is subject to legal and ethical considerations. Jamming signals can unintentionally affect nearby communication systems, potentially causing interference with other devices operating in the same frequency band.
- Evolving technologies: Counter-drone RF jamming technologies continue to evolve. Some systems are designed to intelligently scan for and adapt to the frequency and modulation characteristics of the target drone's communication, enhancing their effectiveness against more sophisticated drones.

4.2. GPS spoofing (soft kill)

GPS spoofing involves sending false Global Positioning System (GPS) signals to the drone, tricking it into believing it is in a different location [101]. This can lead to the drone losing its way or initiating a return-to-home procedure. The main scientific principles behind GPS spoofing are next described:

- Global positioning system basis: GPS is a satellite-based navigation system that provides location and time information to GPS receivers on Earth. The system relies on a network of satellites orbiting the Earth, each transmitting precise timing signals.
- GPS spoofing techniques: GPS Spoofing involves transmitting false GPS signals to deceive a drone's navigation system. The goal is to make the drone believe it is located in a different position than it actually is.
- Signal generation: Spoofing devices generate fake GPS signals that mimic the signals sent by GPS satellites. These signals are then transmitted to the targeted drone.

 doi:10.20944/preprints202402.0551.v1

- Timing and pseudorandom noise code: GPS satellites broadcast signals that include precise timing information and a Pseudorandom Noise (PRN) code unique to each satellite. The receiver on the drone uses this information to calculate its position.
- Overpowering genuine signals: The spoofer's signals must be strong enough to overpower the genuine signals from GPS satellites received by the drone. If successful, the drone will use the fake signals for navigation.
- Manipulating coordinates: By transmitting altered position data, the spoofer can manipulate the drone's perceived location. This can lead to the drone deviating from its intended course or entering a failsafe mode, such as initiating a return-to-home procedure.
- Dynamic spoofing: Advanced GPS spoofing techniques involve dynamically adjusting the fake signals to match the movement of the drone. This helps maintaining the illusion of a consistent, inaccurate location and makes the spoofing harder to detect.
- Implications to drone navigation: GPS is a crucial component of many drone navigation systems. Spoofing can disrupt a drone's ability to navigate accurately, potentially leading to unintended consequences such as collisions, straying into restricted airspace, or violating safety protocols.
- Mitigation challenges: Detecting GPS spoofing can be challenging because drones typically rely heavily on GPS signals, and sophisticated spoofing methods may be designed to avoid detection.
- Legal and ethical considerations: The use of GPS spoofing raises legal and ethical concerns, as it can impact not only the targeted drone but also other GPS-reliant devices in the vicinity. Unauthorized manipulation of GPS signals may violate laws and regulations.

4.3. Communication signal interception (soft kill)

Intercepting and analyzing communication signals between the drone and its operator can provide insights into the drone's mission and enable countermeasures [102]. This can be done to gather intelligence, track the drone's movements, or even take control of the UAV.

- Communication systems in UAS: Unmanned Aerial Systems rely on various communication protocols to function. This includes Radio Frequency (RF) communication for commands, telemetry, and possibly video transmission. Drones may use different frequency bands, such as 2.4 GHz or 5.8 GHz, for communication between the remote controller and the drone itself.
- Signal interception techniques: Intercepting drone signals involves the use of specialized equipment to capture and analyze the communication between the remote controller and the UAS. This equipment may include Software-Defined Radios (SDRs), antennas, and signal processing tools.
- Frequency spectrum analysis: Intercepting signals begins with a thorough analysis of the frequency spectrum used by the UAS. The interceptor needs to identify the specific frequencies on which the drone is communicating. This may involve scanning a range of frequencies to detect the signals emitted by the UAV and its controller.
- Decoding protocols: Once the signals are intercepted, the next step is to decode the communication protocols used by the drone. This involves understanding how commands are formatted, how telemetry data is transmitted, and, if applicable, how video signals are encoded. Decoding may require knowledge of encryption methods if the communication is secured.
- Data interpretation: After decoding the intercepted signals, analysts can interpret the data to understand the drone status, location, mission parameters, and any other relevant information. This intelligence can be crucial for assessing the threat level posed by the UAV and planning appropriate countermeasures.
- Counteraction strategies: Intercepted signals can be used to develop counteraction strategies. This may include deploying signal jammers to disrupt communication between the drone and its operator or taking over control of the drone by sending false commands. However, the latter approach requires a deep understanding of the drone's communication protocols.
- Legal and ethical considerations: Intercepting communication signals from drones raises legal and ethical concerns. Depending on jurisdiction, intercepting private communication may violate privacy laws, and interfering with drone operations could have legal consequences.

 doi:10.20944/preprints202402.0551.v1

Authorities must carefully consider the legality and ethical implications of using communication interception techniques.

4.4. Cyber-attacks (soft kill)

Soft kill methods may involve launching cyber-attacks on the drone's communication systems or exploiting vulnerabilities in its software [103]. This can include injecting malicious code into the drone's systems to disable or manipulate its functions. These attacks aim to disrupt or compromise the functionality of UAVs, providing an alternative approach to counter unmanned aerial threats.

- UAV control systems: Unmanned Aerial Vehicles are equipped with electronic control systems that manage their flight, navigation, and communication. These systems often include software, firmware, and communication protocols that can be potential targets for cyber-attacks.
- Cyber-attack vectors: Cyber-attacks on UAS can take various forms. Malware injection consists of introducing malicious software into the drone control system to compromise its integrity and functionality. Denial of Service (DoS) attacks overload communication channels of the drone processing capabilities to disrupt its normal operation. Man-in-the-Middle (MitM) attacks intercept and modify communication between the drone and its operator to gain unauthorized control or manipulate data. Finally, the exploitation of software vulnerabilities consists in the identification and exploitation of weaknesses in the software running on the drone control system.
- Targeting communication links: Drones rely on communication links between the operator and the aircraft itself. Cyber-attacks may focus on disrupting or manipulating these links. For instance, attackers might jam or interfere with Radio Frequency (RF) signals, or they could exploit vulnerabilities in the communication protocols.
- GPS spoofing via cyber means: Cyber-attacks can also be employed to conduct GPS spoofing, as discussed previously. By compromising the GPS signals received by the drone, attackers can manipulate its perceived location and potentially alter its flight path.
- Counteraction and mitigation: Cybersecurity measures to counter UAS threats involve implementing robust encryption, authentication, and intrusion detection systems. Regular software updates and patch management are crucial to fixing vulnerabilities that could be exploited in cyber-attacks. Additionally, network segmentation and firewalls can help isolating and protecting critical components of UAV control systems.
- Ethical and legal implications: Performing cyber-attacks on UAS for countermeasures must adhere to legal and ethical standards. Unauthorized access to or manipulation of drone systems may violate laws, and ethical considerations should be taken into account to ensure responsible and lawful use of cyber capabilities.
- Ongoing research and development: As the field of UAS evolves, ongoing research and development efforts are essential to stay ahead of potential cyber threats. This includes analyzing emerging attack vectors, developing robust cybersecurity solutions, and collaborating with experts in both drone technology and cybersecurity.

4.5. Directed energy weapons (DEW) (soft kill)

While DEWs can have lethal applications, in the context of soft kill technologies, they can be used to disable drones non-lethally [104]. DEWs comprise lasers or high-powered microwaves that disrupt the drone electronic systems without causing physical damage. This approach offers a precise and rapid-response method for countering UAS threats.

- Principles of directed energy weapons: Directed energy weapons utilize focused beams of electromagnetic energy, such as lasers or microwaves, to achieve their intended effects. These energy beams can be precisely directed and controlled, providing a high level of accuracy.
- Laser-based directed energy weapons: High-energy lasers, often based on solid-state, fiber, or chemical laser technologies, are employed in DEWs for countering UAS. The laser beam is

 doi:10.20944/preprints202402.0551.v1

focused onto the target, typically a vital component of the UAV such as its propulsion system, electronics, cameras, or structural elements.

- Microwave-based directed energy weapons: Microwave-based DEWs use generators to produce intense microwave radiation. Microwaves can interact with the electronic systems of the UAS, disrupting or damaging components like communication systems, sensors, or avionics.
- Target tracking and engagement: DEWs are equipped with advanced sensor systems, such as radar or optical trackers, to detect and track UAVs in real-time. The directed energy beam is precisely directed toward the UAV based on the real-time tracking data, ensuring accurate targeting.
- Effects on UAS: Directed energy weapons can cause structural damage to UAVs by heating and melting critical components. The intense energy can disrupt or damage electronic systems on board, rendering the UAS inoperable.
- Range and limitations: The effective range of DEWs varies depending on the type and power of the weapon. High-energy lasers can have relatively long ranges. However, atmospheric conditions, such as humidity and turbulence, can affect the performance of directed energy weapons.
- Non-lethal options: Directed energy weapons can be designed with varying power levels to offer non-lethal options. Low-power settings may be used for disabling or disrupting UAS without causing permanent damage.
- Ethical and legal considerations: The use of directed energy weapons for countering UAS raises ethical and legal considerations. Ensuring compliance with international laws and rules of engagement is essential.

4.6. Acoustic countermeasures (soft kill)

Loud sounds or acoustic signals can disorient or disrupt the drone inertial sensors and communication systems [105]. Acoustic countermeasures are designed to interfere with the drone's ability to navigate and communicate effectively.

- Principles of acoustic countermeasures: Acoustic countermeasures leverage the principles of sound propagation and detection to interact with unmanned aerial systems. These countermeasures typically include both detection systems and devices that generate acoustic signals for disruption.
- Acoustic detection systems: Acoustic countermeasures often involve the use of microphones and other sensors to detect the sound signatures produced by UAVs. These sensors can be strategically placed to cover areas where drone activity is expected. Advanced signal processing techniques are employed to distinguish the acoustic signature of drones from background noise and other sounds. This helps in accurate detection and identification of UAVs.
- Acoustic disruption devices: Devices capable of emitting intense sound waves are used as disruptive tools. These can include speakers or transponders that generate specific frequencies or patterns. Acoustic countermeasures may exploit the sensitivity of UAS components, such as inertial sensors and communication systems, to specific frequencies. By emitting disruptive frequencies, the countermeasures aim to interfere with the normal operation of the drone.
- Types of acoustic disruption: Acoustic signals can be designed to interfere with the communication links between the drone and its operator, disrupting control signals. Intense acoustic signals may interfere with the sensors on board the UAV, affecting its ability to navigate or gather information. Acoustic countermeasures can also perturb the flight stability of the UAV by affecting its propulsion system or control surfaces.
- Detection range and limitations: The effectiveness of acoustic countermeasures depends on the detection range of the acoustic sensors and the distance over which disruptive signals can be effectively transmitted. Environmental conditions, such as wind and atmospheric absorption, can affect the propagation of acoustic signals and impact the performance of acoustic countermeasures.

 doi:10.20944/preprints202402.0551.v1

- Integration with other countermeasures: Acoustic countermeasures are often used in conjunction with other counter-UAS technologies, such as radar systems, to provide a comprehensive defense against drone threats.
- Ethical and legal considerations: As with any counter-UAS technology, the use of acoustic countermeasures raises ethical and legal considerations. Authorities must ensure compliance with local regulations and international laws governing the use of such technologies.

4.7. Hard kill

Hard kill refers to a counter-UAS approach that involves physically destroying or damaging the drone to neutralize its threat [106–108]. This method contrasts with soft kill techniques, which focus on non-destructive means of countering UAS as was previously shown.

- Projective-based hard kill: Kinetic energy method of hard kill involves using projectiles, such as bullets or specialized ammunition, to physically impact and disable the UAS. This approach requires precise targeting and accurate ballistic calculations to ensure that the projectile intercepts the UAV.
- Directed Energy Weapons (DEWs): High-energy lasers can be employed as directed energy weapons to deliver a focused beam of energy onto critical components of the UAV, causing damage or destruction. Microwave-based directed energy weapons can generate intense microwave radiation to disrupt or damage electronic components on the UAV.
- Explosive-based hard kill: Explosive devices, such as missiles or other munitions, can be employed to physically destroy the UAV. These countermeasures are designed to inflict sufficient damage to render the drone inoperable. Explosive devices may produce fragmentation effects that can effectively disable or destroy the UAV within a certain radius.
- Projectile and missile guidance systems: Hard kill methods often involve advanced guidance systems, such as radar or infrared homing, to ensure the accuracy of projectiles or missiles. These guidance systems enable real-time tracking of the UAV, allowing for precise targeting and interception.
- Range and limitations: The effectiveness of hard kill methods depends on the range of the countermeasure, the speed and agility of the UAV, and the accuracy of the targeting system. Payload capacity of the countermeasure, whether it's a projectile or explosive device, influences the ability to neutralize different types of UAS.
- Integration with sensor systems: Effective hard kill systems often integrate with sensor systems, such as radar and electro-optical sensors, to enhance target detection and tracking capabilities. Rapid data processing and analysis are crucial to ensure timely and accurate responses to UAS threats.
- Ethical and legal considerations: The use of hard kill methods raises ethical and legal considerations. Rules of engagement must be established to govern the use of lethal force against UAS, considering potential collateral damage and adherence to international laws.

Hard kill methods applied to counter UAS involve physically destroying or damaging unmanned aerial vehicles. This can be achieved through projectiles, directed energy weapons, or explosive devices, each with its own set of technical considerations and limitations. Hard kill methods are typically employed in situations where other countermeasures may not be sufficient to neutralize the UAS threat.

5. Conclusions

This work provides a review of counter drone systems from a commercial and scientific point of view, including the detection, tracking and target classification phases, as well as the mitigation phase. The study shows a large number of threats in both the civilian and military spheres, which make the use of counter drone systems necessary.

Twenty-seven commercial systems from different countries and technologies were analyzed. Almost all of them feature a multi-sensor approach to detection of the unmanned aircraft, combining

technologies such as radio frequency and acoustic analysis or radar. Those oriented to the civilian sector show mitigation actions based on soft kill, mainly focused on interrupting the radio connection between the aircraft and the control station or disabling its satellite navigation signal reception. Those that are also focused on the military sector also show hard kill capabilities such as projectiles or directed energy weapons.

The study of commercial systems is complemented with a scientific review of the state of the art. It can be seen there are incipient technologies that are not yet commercially available. On the one hand there is the use of sensors such as LiDAR systems, which allow to obtain accurately and quickly the range, azimuth, and elevation of a target with a very high resolution. These systems would be very useful especially for the detection, tracking and classification of the drone threat at distances of less than 1 km, although the high computational requirements that would be necessary would have to be considered. On the other hand, it would also be interesting to transfer to the market all the knowledge that is currently being developed regarding artificial intelligence and algorithmics and their applications in the field of target classification. This is crucial to adapt mitigation actions according to the characteristics of the threat.

Author Contributions: Conceptualization, H. G.-J., E. B., and F. V.; methodology, E. A., G. F.-C., and E. R.-O.; investigation, E. A., G. F.-C., and E. R.-O.; writing – original draft preparation, E. A. and H. G.-J.; writing – review and editing, E. B., F. V.; funding acquisition, H. G.-J.; project administration, H. G.-J. All authors have read and agreed to the published version of the manuscript.

Funding: Authors would like to thank University of Vigo, CISUG, Xunta de Galicia, Gobierno de España, Agencia Estatal de Investigación and European Union—Next Generation EU for the financial support given through the next grants: FPU21/01176. PID2021-125060OB-100. TED2021-129756B-C31. Complementary R&D Plan. Galician Marine Sciences Program.

Data Availability Statement: Non applicable due to the manuscript scope.

Acknowledgments: The authors would like to thank the reserve commander, Mr. Luis Lorenzo, for all the support given and the discussions related to military technologies.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. González-Jorge, H., Martínez-Sánchez, J., Bueno, M., Arias, P., Unmanned aerial systems for civil applications: A review. *Drones* **2017**, *1(1)*, 1-19.
2. Konert, A., Balcerzak, T, Military autonomous drones (UAVs) – from fantasy to reality. Legal and ethical implications. *Transportation Research Procedia* **2021**, *59*, 292 – 299.
3. Mogili, U. R., Deepak, B. B. V. L., Review on application of drone systems in precision agriculture, *Procedia Computer Science* **2018**, *133*, 502 – 509.
4. Klemas, V. V., Coastal and environmental remote sensing from unmanned aerial vehicles: An overview, *Journal of Coastal Research*, **2015**, *31(5)*, 1260 – 1267.
5. Mishra, B., Garg, D., Narang, P., Mishra, V., Drone-surveillance for search and rescue in natural disaster, *Computer Communications*, **2020**, *156*, 1 – 10.
6. Goodchild, A., Toy, J., Delivery by drone: An evaluation of unmanned aerial vehicle technology in reducing CO2 emissions in the delivery service industry, *Transportation Research Part D: Transport and Environment*, **2018**, *61*, 58 – 67.
7. Jordan, S., Moore, J., Hovet, S., Box, J., Perru, J., Kirsche, K., Lewis, D., Tse, A. T. H., State-of-the-art technologies for UAV inspections, *IET Radar, Sonar and Navigation*, **2018**, *12*, 151 – 164.
8. Kreps, S. E., Wallace, G. P. R., International law, military effectiveness, and public support for drone strikes, *Journal of Peace Research*, **2016**, *53*, 830 – 844.
9. De Swarte, T., Boufous, O., Escalle, P., Artificial intelligence, ethics and human values: the cases of military drones and companion robots, *Artificial Life and Robotics*, **2019**, *24(3)*, 291 – 296.
10. Paucar, C., Morales, L., Pinto, K., Sánchez, M., Rodríguez, R., Gutiérrez, M., Palacios, L., Use of drones for surveillance and reconnaissance of military areas, *Smart Innovation, Systems and Technologies*, **2018**, *94*, 119 – 132.
11. General Atomics MQ-1 Predator: https://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator (accessed 16 01 2024).

12. General Atomics MQ-9 Reaper: https://en.wikipedia.org/wiki/General_Atomics_MQ-9_Reaper (accessed 16 01 2024).
13. Russia and Ukraine are fighting the first full-scale drone war: https://www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/ (accessed 16 01 2024).
14. How the drone war in Ukraine is transforming the conflict: https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict (accessed 16 01 2024).
15. AeroVironment RQ-11 Raven: https://en.wikipedia.org/wiki/AeroVironment_RQ-11_Raven (accessed 16 01 2024).
16. Orlan-10: https://en.wikipedia.org/wiki/Orlan-10 (accessed 16 01 2024).
17. Bayraktar TB2: https://en.wikipedia.org/wiki/Bayraktar_TB2 (accessed 16 01 2024).
18. Forpost ISR: https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1486 (accessed 16 01 2024).
19. Voskujil, M., Performance analysis and design of loitering munitions: A comprehensive technical survey of recent developments, *Defence Technology*, **2022**, *18(3)*, 325 – 343.
20. IAI Harop: https://en.wikipedia.org/wiki/IAI_Harop (accessed 16 01 2024).
21. AeroVironment Switchblade: https://en.wikipedia.org/wiki/AeroVironment_Switchblade (accessed 16 01 2024).
22. Bode, I., Huelss, H., Nadibaidze, A., Qiao-Franco, G., Watts, T. F. A., Prospects for the global governance of autonomous weapons: comparing Chinese, Russian and US practices, *Ethics and Information Technology*, **2023**, *25(1)*, 5.
23. Yaacoub, J. P., Noura, H., Salman O., Chehab, A., Security analysis of drones systems: Attacks, limitations and recommendations, *Internet of Things*, **2020**, *11*, 100218.
24. Drone incident management at aerodromes: https://www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf (accessed 17 01 2024).
25. UAS sightings report: https://www.faa.gov/uas/resources/public_records/uas_sightings_report (accessed 17 01 2024).
26. Wang, J., Liu Y., Song, H., Counter-unmanned aircraft systems (C-UAS): State of the art, challenges, and future trends, *IEEE Aerospace and Electronic Systems Magazine*, **2021**, *36(3)*, 4 – 29.
27. Kang, H., Joung, J., Kim, J., Kang, J., Cho, Y. S., Protect your sky: A survey of counter unmanned aerial vehicle systems, *IEEE Access*, **2020**, *8*, 168671 – 168710.
28. Lockheed Martin Morphius: https://lockheedmartin.com/content/dam/lockheed-martin/mfc/pc/morfius/mfc-morfius-pc-01.pdf (accessed 17 01 2024).
29. Raytheon Coyote: https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/coyote (accessed 17 01 2024).
30. Northrop Grumman M-ACE: https://cdn.prd.ngc.agencyq.site/-/media/wp-content/uploads/L-0900-MACE-Factsheet.pdf (accessed 17 01 2024).
31. General Dynamics Dedrone: https://gdmissionsystems.com/-/media/general-dynamics/ground-systems/pdf/counter-uas---dedrone/counter-unmanned-aerial-system-c-uas-datasheet.ashx (accessed 17 01 2024).
32. Highpoint Aerotechnologies Liteye: https://www.highpointaerotech.com/liteye (accessed 17 01 2024).
33. Blighter Surveillance Systems AUDS: https://www.blighter.com/wp-content/uploads/auds-datasheet.pdf (accessed 17 01 2024).
34. MSI-Defence Systems Terrahakw Paladin: https://www.msi-dsl.com/products/msi-ds-terrahawk-vshorad/ (accessed 17 01 2024).
35. Thales Group EagleShield: https://www.thalesgroup.com/en/markets/defence-and-security/air-forces/airspace-protection/counter-unmanned-aircraft-systems (accessed 17 01 2024).
36. Elistair Orion 2.2 TW: https://elistair.com/solutions/tethered-drone-orion/ (accessed 17 01 2024).
37. Elbit Systems ReDrone: https://elbitsystems.com/media/Redrone_45190331_25052023_WEB.pdf (accessed 17 01 2024).
38. Israel Aerospace Industries Drone Guard DG5: https://www.iai.co.il/p/eli-4030-drone-guard (accessed 17 01 2024).
39. Rafael Advanced Defense Systems Drone Dome: https://www.rafael.co.il/wp-content/uploads/2019/03/Drone-Dome.pdf (accessed 17 01 2024).
40. CONTROP Precision Technologies TORNADO-ER: https://www.controp.com/wp-content/uploads/2021/10/TORNADO-ER.pdf (accessed 17 01 2024).
41. MCTECH RF Technologies MC Horizon: https://mctech-jammers.com/products/mc-horizon/ (accessed 17 01 2024).
42. INDRA Crow: https://www.indracompany.com/en/anti-drone-system (accessed 17 01 2024).
43. SDLE Antridone: https://www.aeronauticasdle.com/products/ (accessed 17 01 2024).

44. Leonardo FalconShield: https://uk.leonardo.com/documents/64103/6765824/Falcon+Shield+LQ+%28mm08605%29.pdf?t=1671446128764 (accessed 17 01 2024).
45. SAAB AB 9LV: https://www.saab.com/globalassets/markets/australia/ip-23/20231030-auscms-cuas_final.pdf (accessed 17 01 2024).
46. HENSOLDT Xpeller: https://www.hensoldt.net/stories/xpeller-counter-uav-system/ (accessed 17 01 2024).
47. Rheinmetall AG Drone Defence Toolbox: https://www.rheinmetall.com/en/products/air-defence/air-defence-systems/drone-defence-toolbox (accessed 17 01 2024).
48. Department13 Map13: https://department13.com/map13/ (accessed 17 01 2024).
49. EOS Slinger: https://eos-aus.com/wp-content/uploads/2023/11/EOS-Defence-Slinger-flyer.pdf (accessed 17 01 2024).
50. ZALA Aero Group Aerorex: https://www.overtdefense.com/2019/06/27/zala-aero-rex-2-anti-drone-gun/ (accessed 17 01 2024).
51. Roselektronika Zaschita: https://www.unmannedairspace.info/counter-uas-systems-and-policies/russian-system-uses-passive-signals-to-provide-almost-undetectable-counter-drone-capability/ (accessed 17 01 2024).
52. China Electronic Group Corporation YLC-48: https://www.globaltimes.cn/page/202104/1221903.shtml (accessed 17 01 2024).
53. DJI Aeroscope: https://www.dji.com/es/aeroscope/info#specs (accessed 17 01 2024).
54. ASELSAN iHTAR: https://wwwcdn.aselsan.com/api/file/IHTAR_ANTI_DRONE_ENG.pdf (accessed 17 01 2024).
55. Kongsberg CORTEX Typhon: https://defence-industry.eu/kongsberg-to-produce-multiple-c-uas-air-defence-systems-for-ukraine/ (accessed 17 01 2024).
56. Griffiths, H., Baker, C., *An introduction to passive radar*, **2022**, Publisher: IEEE.
57. Mattei, F., Enhanced radar detection of small remotely piloted aircraft in U-space scenario, *Materials Research Proceedings*, **2023**, *33*, 15 – 20.
58. Martelli, T., Filippini, F., Colone, F., Tackling the different target dynamics issues in counter drone operations using passive radar, *IEEE International Radar Conference*, **2020**, *09114618*, 512 – 517.
59. Souli, N., Theodorou, I., Kolios, P. Ellinas, G., Detection and tracking of rogue UAS using a novel real-time passive radar system, *Conference on Unmanned Aircraft Systems*, **2022**, 181377, 576 – 582.
60. Siewer, S., Andalibi, M., Bruder, S., Buchholz, J., Fernandez, R., Rizor, S., Slew-to-cue electro-optical and infrared sensor network for small UAS detection, tracking and identification, *AIAA Scitech Forum*, **2019**, 225819.
61. Dumitrescu, C., Minea, M., Costea, I. M., Chiva, I. C., Semenescu, A., Development of an acoustic system for UAV detection, *Sensors*, **2020**, *20(17)*, 1- 17.
62. Ahn, J., Kim, M. Y., Positional estimation of invisible drone using acoustic array with A-shaped neural network, *International conference on Artificial Intelligence in Information and Communication*, **2021**, *9415272*, 320 – 324.
63. Kadyrov, D., Sedunov, A., Sedunov, N., Sutin, A., Salloum, H., Tsyuryupa, S., Improvements to the Stevens drone acoustic detection system, *Proceedings of Meetings on Acoustics*, **2022** *46(1)*, 45001.
64. Ding, S., Guo, X., Peng, T., Huang, X., Hong, X., Drone detection and tracking system based on fused acoustical and optical approaches, *Advanced Intelligent Systems*, **2023**, *5(10)*, 2300251.
65. Ivancic, J., Karunasiri, G., Alves, F., Directional resonant MEMS acoustic sensor and associated acoustic vector sensor, *Sensors*, **2023**, *23(19)*, 8217.
66. Fang, J., Li, Y., Ji, P. N., Wang, T., Drone detection and localization using enhanced fiber-optic acoustic sensor and distributed acoustic sensing technology, *Journal of Lightwave Technology*, **2023**, *41(3)*, 822 – 831.
67. Flir 380 hd: https://www.flir.es/products/tacflir-380-hd/ (accessed 18 01 2024)
68. Siewert, S., Andalibi, M., Bruder, S., Gentilini, I., Buchholz, J., Drone net architecture for UAS traffic management multi-modal sensor networking experiments, *IEEE Aerospace Conference Proceedings*, **2018**, *137510*, 1 – 18.
69. Hao, T. K. and Yakimenko, O., Assessment of an effective range of detecting intruder aerial drone using onboard EO-sensor, *International Conference on Control, Automation and Robotics*, **2020**, 9108102, 653 – 661.
70. Goecks, V. G., Woods, G., Valasek, J., Combining visible and infrared spectrum imagery using machine learning for small unmanned aerial system detection, *Proceedings of SPIE*, **2020**, *11394(113940)*, 161094.
71. Muller, T., Widak, H., Kollmann, M., Buller, A., Sommer, L. W., Spraul, R., Kroker, A., Kaufmann, I., Zube, A., Segor, F., Perschke, T., Lindner, A., Drone detection, recognition, and assistance system for counter-UAV with VIS, radar, and radio sensors, *Proceedings of SPIE*, **2022**, *12096(120960A)*, 180323.
72. Shovon, M. H. I., Gopalan, R., Campbell, B., A comparative analysis of deep learning algorithms for optical drone detection, Proceedings of SPIE, **2023**, *12701(1270104)*, 192563.

73. Ojdanic, D., Sinn, A., Naverschnigg, C., Schitter, G., Feasibility analysis of optical UAV detection over long distances using robotic telescopes, *IEEE Transactions on Aerospace and Electronic Systems*, **2023**, *59(5)*, 5148 – 5157.
74. Medaiyese, O. O., Ezuma, M., Lauf, A. P., Guvenc, I., Wavelet transform analytics for RF-based UAV detection and identification system using machine learning, *Pervasive and Mobile Computing*, **2022**, 101569.
75. Alam, S. S., Chakma, A., Rahman, M. H., Bin, M. R., Alam, M . M., Utama, I. B. K. Y., Jang, Y. M., RF-enabled deep-learning-assisted drone detection and identification: An end-to-end approach, *Sensors*, **2023**, *23(9)*, 4202.
76. Aouladhadj, D., Kpre, E. Deniau, V., Kharchouf, A., Gransart, C., Gaquiere, C., Drone detection and tracking using RF identification signals, *Sensors*, **2023**, *23(17)*, 7650.
77. Almubairik, N. A., El.Alfy, E. M., RF- based drone detection with deep neural network: Review and case study, *Communications in Computer and Information Science*, **2023**, *1969*, 16 – 27.
78. Riabukka, V. P., radar surveillance of unmanned aerial vehicles (Review), *Radioelectronics and Communications Systems*, **2020**, *63(11)*, 561 – 573.
79. Wallentine, S. K., Jost, R. J., Reynolds, R. C. Autonomous spherical passive/active radar calibration system, *Antenna Measurement Tchniques Association Symposium*, **2021**, 175277.
80. Schneebeli, N., Leuenberger, A., Wabeke, L., Klobe, K., Kitching, C., Siegenthaler, U., Wellig, P., Drone detection with a multistatic C-band radar, *Proceedings International Radar Symposium*, **2021**, *9466299*, 171132.
81. Abratkiewicz, K., Malanowski, M., Gajo, Z. Target acceleration estimation in active and passive radars, *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, **2023**, *16*, 9193 – 9296.
82. Lam, I., Pant, S., Manning, M., Kubanski, M., Fox, P., Rajan, S., Patnaik, P., Balaji, B., Time-frequency analysis using V-band radar for drone detection and classification, *IEEE Instrumentation and Measurement Technology Conference*, **2023**, 190690.
83. Paschalidis, K., Yakimenko, O., Cristi, R., Feasibility of using 360º LiDAR in C-sUAS missions, *IEEE International Conference on Control and Automation*, **2022**, *181353*, 172 – 179.
84. Barisic, A., Ball, M., Jackson, N., McCarthy, R., Naimi, N., Strassle, L., Becker, J., Brunner, M., Fricke, J., Markovic, L., Seslar, I., Novick, D., Multi-robot system for autonomous cooperative counter-UAS missions: Desings, integration and field testing, *IEEE International Symposium on Safety, Security, and Rescue Robotics*, **2022**, 186231.
85. Aldao, E., González-deSantos, L. M., González-Jorge, H., LiDAR based detect and avoid system for UAV navigation in UAM corridors, *Drones*, **2022**, *6(8)*, 185.
86. Rodrigo, P. J., Larsen, H. E., Pedersen, C., CW coherent detection lidar for micro-Doppler sensing and raster-scan imaging of drones, *Optics Express*, **2023**, *31(5)*, 7398 – 7412.
87. Abir, T. A., Kuantama, E., Han, E., Dawes, J., Mildren, R., Nguyen, P., Towards robust lidar-based 3D detection and tracking of UAVs, *Proceedings of the 9th ACM Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, **2023**, *189616*, 1 – 7.
88. Koch, W., Govaers, F., Counter drones: Tensor decomposition-based data fusion and systems design aspects, *Proceedings of the SPIE*, **2018**, *10799*, 107990.
89. Kondru, D. S. R., Celenk, M., Mitigation of target tracking errors and sUAS response using multi sensor data fusion, *Lecture Notes in Computer Science*, **2018**¸*10884*, 194 – 204.
90. Baptista, M., Fernandez, L., Chaves, P., Tracking and classification of aerial objects, Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, **2020**, 310, 264 – 276.
91. Kotesware, R. S., Jahan, K., Kavitha, L., Implementation of unscented Kalman filter to autonomous aerial vehicle for target tracking, *IEEE India Council International Subsections Conference*, **2020**, *9344509*, 204 – 209.
92. Sie, N. J., Xuan Seah, S., Chan, J. J., Yi, J., Chew, K. H., Hooi Chan, R., Srigrarom, S., Holzapfel, F., Hesse, H., Vission-based drones tracking using correlation filters and linear integrated multiple model, *International Conference on Electrical Engineering / Electronics, Computer, Telecommunications and Information Technology: Smart Electrical System and Technology*, **2021**, *170892*, 1085 – 1090.
93. Liang, N. S. J., Srigrarom, S., Multi-camera multi-target drone tracking system with trajectory-based target matching and re-identification, *International Conference on Unmanned Aircraft Systems*, **2021**, *9476845*, 1337 – 1344.
94. Son, Sohee, Kwon, J., Kim, H. Y., Choi, H., Tiny drone tracking framework using multiple trackers and Kalman-based predictor, **2021**, *20/(8)*, 2391 – 2412.
95. Montañez, O. J., Suarez, M. J., Fernández, E. A., Application of data sensor fusion using extended Kalman filter algorithm for identification and tracking of moving targets from LiDAR-Radar data, *Remote Sensing*, **2023**, *15(13)*, 3396.
96. Zitar, R. A., Mohsen, A., Seghrouchni, A. E., Intensive review of drones detection and tracking: Linear Kalman filter versus nonlinear regression, an analysis case, *Archives of Computational Methods in Engineering*, **2023**, *30(5)*¸2811 – 2830.

97. Alhadhrami, E., Seghrouchni, A. E. F., Barbaresco, F., Zitar, R. A., Drones tracking adaptation using reinforcement learning: Proximal policy optimization, *Proceedings International Radar Symposium*, **2023**, 177483.
98. Evaluating and comparing counter-drone (C-UAS) mitigation technologies: https://d-fendsolutions.com/wp-content/uploads/2022/08/Mitigation-White-Paper.pdf (accessed 19 01 2024).
99. Castrillo, V. U., Manco, A., Pascarella, D., Gigante, G., A review of counter-UAS technologies for cooperative defensive teams of drones, *Drones*, **2022**, *6(3)*, 65.
100. Ga-Hye, J., Ji-Hyun, L., Yeon-Su, S., Hyun-Ju, P., Jou-Jin, L., Sun-Woo, Y., Il-Gu, L., Cooperative friendly jamming techniques for drone-based mobile secure zone, *Sensors*, **2022**, *22(3)*, 865.
101. Mykytyn, P., Brzozowski, M., Dyka, Z., Lagendoerfer, P., GPS-spoofing attack detection mechanism for UAV swarms, *Mediterranean Conference on Embedded Computing*, **2023**, 190017.
102. Souli, N., Kolios, P., Ellinas, G., Multi-agent system for rogue drone interception, *IEEE Robotics and Automatic Letters*, **2023**, *8(4)*, 2221 – 2228.
103. Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M., Abdelhaq, M., Alsaqour, R., IoT empowered smart cybersecurity framework for intrusion detection in internet of drones, *Scientific Reports*, **2023**, *13(1)*, 18422.
104. Borja, L. J., High-energy laser directed energy weapons: Military doctrine and implications for warfare, *Routledge Handbook of the Future of Warfare*, **2023**, 353 – 363.
105. Gao, M., Zhang, L., Shen, L., Zou, X., Han, J., Lin, F., Ren, K., Exploring practical acoustic transduction attacks on inertial sensors in MDOF systems, *IEEE Transactions on Mobile Computing*, **2023**, 1 - 18.
106. Ameloot, C., Papy, A., Robbe, C., Hendrick, P., Desing of a simulation tool for C-sUAS systems based on fragmentation unguided kinetic effectors, *Proceeding of International Symposium on Ballistics*, **2023**, *1*, 1188 – 1199.
107. Taillandier, M., Peiffer, R., Darut, G., Verdy, C., Regnault C., Pommies, M., Duality safety – Efficiency in laser directed energy weapon applications, *Proceedings of SPIE*, **2023**, *194555*, 127390A.
108. Muhaidheen, M., Muralidharan, S., Alagammal, S., Vanaja, N., Design and development of unmanned aerial vehicle (UAV) directed artillery prototype for defense application, *International Journal of Electrical and Electronics Research*, **2022**, *10(4)*, 1086 – 1091.
109. Anti drone jammer: https://www.thesmartcityjournal.com/en/companies/indra-produces-the-arms-anti-drone-solution (accessed 20 01 2024)
110. High-energy laser: https://prd-sc102-cdn.rtx.com/raytheon/-/media/ray/what-we-do/integrated-air-and-missile-defense/hel/pdf/ray_hel6-panel_data_ic23.pdf?rev=d79c063a461246b7bb752674d3534cb0&hash=D3597E8AA47D344FF8CC1465B5C75C1B (accessed 20 01 2024)