drones

MDPI

Review

A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones

Vittorio Ugo Castrillo *, Angelo Manco, Domenico Pascarella and Gabriella Gigante

CIRA—Italian Aerospace Research Centre, Via Maiorise, 81043 Capua, Italy; a.manco@cira.it (A.M.); d.pascarella@cira.it (D.P.); g.gigante@cira.it (G.G.)
* Correspondence: v.castrillo@cira.it

Abstract: In recent years, the drone market has had a significant expansion, with applications in various fields (surveillance, rescue operations, intelligent logistics, environmental monitoring, precision agriculture, inspection and measuring in the construction industry). Given their increasing use, the issues related to safety, security and privacy must be taken into consideration. Accordingly, the development of new concepts for countermeasures systems, able to identify and neutralize a single (or multiples) malicious drone(s) (i.e., classified as a threat), has become of primary importance. For this purpose, the paper evaluates the concept of a multiplatform counter-UAS system (CUS), based mainly on a team of mini drones acting as a cooperative defensive system. In order to provide the basis for implementing such a system, we present a review of the available technologies for sensing, mitigation and command and control systems that generally comprise a CUS, focusing on their applicability and suitability in the case of mini drones.

Keywords: counter-UAS systems; sensing; neutralization; command and control; drones; cooperative systems

Citation: Castrillo, V.U.; Manco, A.; Pascarella, D.; Gigante, G. A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones* **2022**, *6*, 65. https://doi.org/10.3390/drones6030065

Academic Editors: Andrzej Łukaszewicz, Wojciech Giernacki, Zbigniew Kulesza, Jaroslaw Pytka and Andriy Holovatyy

Received: 24 January 2022
Accepted: 24 February 2022
Published: 1 March 2022

1. Introduction

In recent years, the drone market has had a significant expansion, especially in the consumer sector. Drones destined for this market are easily accessible thanks to their relatively low cost. In addition, the characteristics of weight, size, and the ability to carry a payload, such as a camera, allow them to be used in various fields, from the recreational to the professional sector. In addition, from a research point of view, the use of these flying platforms helps the development of technologies whose applications have a positive impact on the community, such as search and rescue operations, intelligent logistics, environmental monitoring or precision agriculture.

Given the increasing use of these technologies, the issues related to safety, security and privacy must be taken into consideration. Their use could cause damage to the community due to failures and improper or criminal use. A significant increase has been observed in the number of accidents involving drones or unmanned aerial systems (UAS) [1]. For example, improper use in the vicinity of an airport can represent a serious threat to public safety and a source of discomfort, as evidenced by the hundreds of flights canceled at London Gatwick airport in a few months of 2018 [2].

For this reason, the development of technologies for the detection, identification and mitigation of malicious drones has become of primary importance. A countermeasure system, also called a counter-UAS (C-UAS) or counter-UAS system (CUS), can identify and neutralize an intruder drone classified as a threat.

From an architectural point of view, an anti-drone system generally consists of the following fundamental sub-systems:

- Sensing system;
- Mitigation system;
- Command and control (C2) system.

The sensing system consists of one or more sensors capable of collecting information from the surrounding environment. The mitigation system consists of one or more mitigating elements capable of disabling, destroying or taking control of the drone identified as a threat. The C2 system collects data from sensors and executes detection algorithms, based on which it establishes the presence of a threat, identifies it (i.e., classifies its entity) and decides the most appropriate tracking and mitigation mode.

There are several C-UAS systems on the market. There are integrated systems that implement both the detection part and the mitigation part on the same platform, but the most adopted solution is to separate the mitigation part from the sensing one, distributing it on different platforms, giving rise to distinct commercial products. For example, most of the available solutions are ground-based, especially for the sensing part, while the sky-based part is typically relegated to mitigation. Thus, a single platform may implement only some of the sub-systems of the CUS (or part of them) and a network architecture is required to implement the interactions between the platforms.

In this paper, a multiplatform CUS, based mainly on a team of mini drones acting as a cooperative defensive system, has been used as a reference. Indeed, mini drones represent an effective solution for the implementation of a CUS, being the ideal platforms for the proximal sensing and tracking of moving targets (e.g., intruder drones) in high-mobility scenarios. Moreover, a team of mini drones may be arranged as a mobile sensor network: on the one hand, the single drones may act as mobile sensor nodes to keep the closeness with moving targets; on the other hand, a cooperative behavior may be established by means of the network of drones and a suitable coordination protocol. Such cooperative behavior may ensure the simultaneous perception and tracking of different moving targets, and may provide efficient coverage by balancing the load of the sensing and tracking tasks amongst the sensor nodes. In the end, defensive drones may also be equipped to implement proper neutralization actions with respect to intruder drones.

In order to provide the basis for the future implementation activities of a cooperative drone-based CUS, this work presents a review of the available technologies for sensing, mitigation and C2 systems by means of mini drones. In addition, the paper discusses some challenges about the key technological enablers for the effective implementation of these systems. This paper does not provide a review of the available technologies for the communication network and for the cooperation algorithms, which are exhaustively described in other works.

The remainder of this article is organized as follows. Section 2 presents the definitions and the basic concepts for cooperative drone-based CUSs. In Section 3, the sensing system is introduced, with a literature review and a comparison on the sensing techniques that could be used aboard drones. In Section 4, different neutralization techniques are discussed and neutralizers using mini drones are highlighted. A detailed description of the C2 system is provided in Section 5. Section 6 presents some of the technological challenges. Section 7 discusses the main results of the work, while the last section is about the conclusions.

2. Definitions and Basic Concepts for Cooperative Drone-Based Counter-UAS Systems

This section provides the main definitions and the basic concepts about cooperative drone-based CUSs.

2.1. Drones

A drone or unmanned aerial vehicle (UAV) is an aircraft with no human pilot on-board. It is the central element of a UAS, which is the set comprised of the aircraft and all the other elements supporting the service of a drone. In detail, a UAS is made up of the main following components:

- Airframe, which is the mechanical part of the vehicle, including the propulsion system;
- Navigation and motion sensors that collect the information about the drone position and its flight trajectory;

- Flight control system (FCS), which controls the propulsion system and the servos in order to apply a flight trajectory;
- Payload, which is the specific equipment to accomplish a given mission;
- Ground control station (GCS), which is a computer system or a network of computer systems on the ground, which monitor and control UAS operation;
- Communication infrastructure, which is the set of data links and related equipment for the communication between the vehicle and the GCS (or other external elements).

There are different classifications of drones according to several parameters, such as weight, altitude, endurance, degree of autonomy, etc. Reference [3] provides a survey of the main classification of drones. For example, the military domain includes a NATO UAS classification system, which is shown in Figure 1. It sets three classes, based on the weight. The classes are further divided according to other parameters, such as the employment, the operating altitude and the mission radius. According to such a classification system, mini drones are Class I drones with a weight less than 15 kg, whereas microdrones are Class I drones with a maximum energy state less than 66 J.

UAS CLASSIFICATION

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)	Strike/ Combat *	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Reaper
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150 kg - 600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Brigade	Hermes 450
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
	Mini (<15 kg)	Tactical Sub -unit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
	Micro ** (<66 J)	Tactical Sub -unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

* Note: in the event the UAS is armed, the operator should comply with the applicable joint mission qualifications in AP-3.3.7 (STANAG 4670) and the system will need to comply with applicable airworthiness standards, regulations, policy, and legal considerations.
** Note: UAS that have a maximum energy state less than 66 Joules are not likely to cause significant damage to life or property, and do not need to be classified or regulated for airworthiness, training, etc. purposes unless they have the ability to handle hazardous payloads (explosive, toxins, chemical/biological agents, etc.).

Figure 1. NATO's UAS classification system [4].

A slightly different classification for micro-, mini and small UAVs (sUAS, NATO Class I) is described in [5] and shown in Table 1. The latter also reports endurance and payload capabilities, as well as weight, altitude, range and same example platforms available on the market.

Table 1. Micro-, mini and small UAV classifications based on weight, altitude, range and payload.

Category	Weight (in kg)	Normal Operating Altitude (in m)	Mission Radius, Range (in km)	Typical Endurance (in h)	Payload (in kg)	Available UAV Models in Market
Micro	<2	<140	5	<1	<1	DJI Spark, DJI Mavic, Parrot Bebop2
Mini	2–25	<1000	25	2–8	<10	DJI Matrice600, DJI Inspire2, Airborne Vanguard
Small	25–150	<1700	50	4–12	<50	AAI Shadow 200, Scorpion 3 Hoverbike

2.2. Multi-Drone Missions

Without the need for an on-board pilot, drones were usually designed to accomplish the D-cube (dull, dangerous and dirty) envelope [6], which is the set of the following mission classes: dull, i.e., monotonous or requiring high endurance for human occupants; dirty, i.e., that could pose a health risk to a human crew; dangerous, i.e., that could result in the loss of life for the on-board pilot. However, if the region of interest of a mission is large and/or the mission objectives are several, the execution of a single-drone mission may solicit a considerable amount of time and may entail poor performance in terms of mission effectiveness.

Multi-drone missions may overcome this issue. They are essentially missions that engage two or more drones with some common objectives. Thus, a multi-drone mission aims at increasing the effectiveness with respect to the equivalent single-drone mission and requires a sort of collaboration amongst the involved drones.

There is no common agreement about the definitions for this multi-drone collaboration and the classification of the different levels of collaboration. For the purposes of this work, the definitions in [7] are adopted and the following levels of collaborations in a multi-drone setting are considered:

- Isolated individual—in this case, a drone independently acts. It may be piloted, or it may exhibit a given degree of autonomy for the execution of its mission on its own.
- Group—a group of drones comprised of several isolated individuals, each with their own mission without coordination, i.e., collaboration is not present.
- Team—a team of drones is a networked set of drones with a common mission, in which all members are assigned specialized and different tasks to accomplish the global mission.
- Swarm—a swarm of drones is a uniform mass of undifferentiated drones. Thus, a swarm is typically composed of a large number of homogeneous drones, which perform a single task.

According to the above classification, only drone teams and swarms envisage a significant collaboration level, which entails a cooperation within the overall system. Such cooperation should allow the achievement of more complex missions and/or effective results with respect to isolated individuals and groups of drones. Cooperation is mediated by coordination (or coordination protocol), which represents the mechanism ensuring that the activities of the single vehicles keep the desired relationships and that the collective behavior (intended as the set of individual behaviors in the system) achieve the objectives for the global system. The members of a swarm usually coordinate each other only through simple and local interactions, whereas the coordination of a team requires diverse mechanisms for the allocation of several, possibly heterogeneous, tasks. In regard to the coordination of a swarm, the emergency concept is usually adopted to indicate the ability of the swarm to achieve a collective behavior for a complex operation by exploiting limited interactions of the single vehicles, which individually accomplish simple behaviors and tasks.

Other definitions and classifications are possible for the collaborative sets of drones. Indeed, such sets may be also managed as an interoperable system of systems (SoS) in order to apply the interoperability concepts, as in reference [8]. In any case, the joint performance of a networked set of drones (teams or swarms) for a common mission is expected to exceed the sum of the performances achievable in the equivalent single-drone mission. In more detail, the following general advantages are expected for a typical multi-drone mission with teams or swarms of drones:

- Multiple simultaneous interventions—the system may simultaneously collect data from multiple locations.
- Efficiency—the system may split up in order to efficiently cover a large area, optimizing available resources.
- Complementarity—the system may perform different tasks with growing accuracy. Clearly, this feature holds for drone teams.
- Reliability—the system assures fault-tolerant missions by providing redundancy and capability of reconfiguration in the case of a failure of individual vehicles.
- Safety—the team or swarm may usually apply the smallest vehicles for a mission with respect to the equivalent single-drone mission. For a permit to fly, the usage of smaller drones is safer than a single great and heavy drone.
- Cost efficiency—a single vehicle to execute some tasks may be an expensive solution when compared with several low-cost vehicles.

2.3. Counter-UAS Systems

In the literature, it is possible to find numerous surveys that have explored the characteristics of anti-drone systems (see for example [5,9–13]). In this regard, the taxonomy presented in [9] is of particular interest, in which CUS are grouped into two categories: ground-based and sky-based, depending on their deployment, respectively, on the ground or in the air using drones or other flying platforms (for example, stratospheric platforms). Ground-based systems can be of the static type, if installed, even temporarily, in a fixed manner within the perimeter to be defended, or of the mobile type if installed on-board land vehicles or transported by hand by humans (human-handled). Sky-based systems are implemented on board drones, UAS, balloons or stratospheric platforms, and deployed as needed. They differ in high altitudes and low altitudes, depending on the operating altitude.

The two types of CUSs oppose each other with respect to the level of operational mobility and the characteristics of weight, size and energy required for operation (size, weight and power, SWaP). Ground systems have the clear advantage of being able to count on weak SWaP requirements (increasingly from static systems to human-handled ones), but have little flexibility in terms of adapting to the unpredictable behavior of malicious drones. On the other hand, sky-based systems have greater adaptability thanks to the inherent maneuverability and flexibility that are afforded with the much more stringent SWaP requirements due to the limited power of the batteries and the low payload capacity for the lighter flying platforms. In choosing the platform to be adopted, it is important to consider its advantages and disadvantages and the operational scenario in which the solution is used.

It is also possible to create a hybrid CUS as a heterogeneous and cooperative network of different platforms (both ground-based and sky-based) to balance the limits that each solution would have if used individually. Indeed, although a CUS can consist of a single platform, it is difficult for such a solution to deal with the threats represented by a malicious drone or even by several malicious drones, so solutions that offer greater reliability and spatial coverage are represented by CUSs comprised of multiple platforms. In this case, the platforms are networked to cooperate, maximizing the effectiveness.

2.4. Cooperative Drone-Based Counter-UAS Systems

This paper is focused on cooperative drone-based CUSs. These represent an instance of hybrid CUS (as defined in Section 2.3), including a cooperative set of drones. Thus,

according to the definitions reported in Section 2.2, such a cooperative set represents a team or swarm of drones.

For the purposes of this work, teams of mini drones (based on the NATO's UAS classification system, as shown in Figure 1, or on the classification reported in [5] and shown in Table 1) are considered as a reference subsystem of the hybrid CUS. This choice is due to the following expected advantages, which are added to the advantages of a generic multi-drone mission (described in Section 2.2):

Mobility—mini drones show extreme mobility; it is possible to bring them closer to the malicious drones and the sensing operations could be done in the proximity of the target. So, mini drones offer a mobile proximal sensing solution for a CUS, which can improve the detection and identification phases by lowering the probability of a false alarm.

Coverage expansion—it is possible to increase the coverage of the protected area. In fact, drones can be easily moved in order to circumvent obstacles and/or monitor areas that are not covered or not effectively covered by ground platforms. In other words, it is easy to extend the area protected by the CUS without increasing the number of used platforms. Nevertheless, proper bases allocation, jointly with re-charging issues, must be guaranteed. Coverage expansion can also be obtained using a single high-altitude platform, but supposedly with higher costs.

Deployment flexibility—compared to other flying platforms, they are simpler and faster to use, allowing lower response times to any threat.

Cooperative sensor network—the defensive team may be arranged as a cooperative sensor network, i.e., as a set of mobile sensor nodes, which may cooperatively perceive, identify and track one or more threats from different "perspectives". This is even more necessary for mobile proximal sensing to keep the closeness with different moving targets. Thus, a cooperative sensor network may be implemented for a distribution of the sensing tasks and a load balancing amongst the sensor nodes. Such network is expected to be reconfigurable for maintaining optimal performance. Clearly, the same concept may be applied also for mitigation purposes if the drones are equipped with the proper neutralization payloads.

Team coordination—as described in Section 2.2, a swarm requires a large mass of homogeneous vehicles and the coordination of a swarm occurs by means of the emergency concept. These features are not deemed suitable for a cooperative drone-based CUS. Indeed, the homogeneity of vehicles may be incompatible with the heterogeneous tasks in a CUS. Moreover, the large mass of vehicles and the emergency of a swarm imply a non-deterministic behavior and the absence of a specific organizational structure since they are based on individuals' reactions [7]. Thus, it may be difficult to estimate the probability of success of a mission, which is generally unacceptable for a CUS. To the contrary, a drone team usually exhibits an explicit organizational structure by means of a deliberated coordination. A team may also satisfy the requirement about the heterogeneous tasks for the cooperative drone-based CUS.

Automated decision-making—given the speeds involved in the operating environment for CUS systems, an automated decision-making capability is essential to aid an operator in the selection of the most proper actions to manage the given threat scenario or attack scenario and to enable the fastest possible reactions on the part of the defense system. Mini drones, with their well-known aptitudes for autonomous behaviors (also as a team), represent an ideal platform to support such capability.

Neutralization—if the intruder drone(s) did not immediately manifest the malicious intentions, the defensive team would act in proximity by physically chasing it and would be ready for mitigation when the threat has manifested [14], thus allowing a higher probability of success for the neutralization phase. In the literature, there have been several recent studies on the use of a drone team as a defensive tool (e.g., [15,16]). Indeed, the features for mobile proximal sensing may be adapted also for mitigation purposes, and some defensive drones may be equipped with specific electronic or kinetic-mechanical neutralization

systems in order to perform preliminary mitigation actions and to take advantage of the closeness to the moving targets.

Scalability—Traditional CUSs lack scalability and are not usually able to face intrusions of drone teams or swarms. To the contrary, a defensive team of drones inherently represents a scalable solution. Indeed, the coordination mechanisms usually exhibit a scalable computational complexity with respect to the cardinality of the team, especially when decentralized approaches (i.e., without central decision points) are applied. These approaches ensure self-configuration and robustness of the team in front of individual off-nominal events (i.e., failures, communication losses, etc.) or threats (i.e., attacks to the individual defensive drones). Moreover, with the proper sizing and payload configuration, a defensive team may detect and track a team or swarm of rogue drones.

The suitability of drone teams for CUS solutions has also been confirmed by state-of-the-art research works in the fields of autonomous multi-agent systems and cooperative robotics, which have proposed several applications with some similarities with CUSs' required capabilities. Indeed, examples of these applications are those related to multi-robot systems for the observation of multiple moving targets, for which different control approaches already exist, such as cooperative multi-robot observation of multiple moving targets (CMOMMT), cooperative search–acquisition–track (CSAT), multi-robot pursuit evasion (MPE) [17]. In addition, multi-drone systems have been analyzed in terms of distributed multi-agent systems for multi-target tracking problems [18]. In the end, the environmental domain presents some advanced multi-drone solutions for environmental monitoring of dynamic natural threats, such as the ones for tracking the dispersion of contaminant clouds [19]. Additionally, some current international projects are developing cooperative drone-based solutions for surveillance and situational awareness applications, such as the following European projects: ResponDrone [20], which aims at developing a multi-UAS platform for first responders to enhance their situation awareness in support assessment missions, search and rescue operations, forest fire fighting, etc.; ROBORDER [21], which aims at developing and demonstrating an autonomous border surveillance system with unmanned mobile robots, including aerial, water surface, underwater and ground vehicles, which will incorporate multimodal sensors as part of an interoperable network; LABYRINTH [22], which proposes a road traffic surveillance by means of a multi-drone system; 5D-AeroSafe [23], which aims at developing multi-drone solutions for the monitoring of airport and waterway daily operations; Drones4Safety [24], which aims at developing a system of autonomous, self-charging and collaborative drones that can inspect a big portion of transportation infrastructures in a continuous operation; RAPID [25], which aims at delivering a fully automated and drone-based maintenance inspection service for bridges, ship hull surveys and more. All these technologies and solutions represent a sound starting point for the future cooperative drone-based solutions in the counter-UAS domain.

Besides, some recent works have already analyzed multi-agent systems for CUS, although they were focused on the single phases of the counter-UAS process, i.e., sensing or mitigation separately. For example, reference [14] proposed a network of defense drones, which is capable of self-organizing its formation to intercept malicious drones. However, this work specifically focused on formation management algorithms to realize intercept and capture formations for the mitigation of drone intrusions, without considering neutralization aspects. Instead, reference [26] proposed a multi-drone framework for the autonomous detection of rogue drones in a defined airspace and detailed the preliminary development of a hardware and software testbed, based on commercial systems.

Other ongoing research activities are developing a cooperative drone-based CUS covering all the phases of the counter-UAS process. For example, the SWADAR (Swarm Advanced Detection And Tracking) project [27] has been awarded the Defense Innovation Prize 2020 (https://www.edrmagazine.eu/defence-innovation-prize, last accessed on 13 February 2022) (20.RTI.PRZ.080, "Innovative Solutions/Technologies for the Countering of Swarms of UAVs, specifically on the Protection of Static and Dynamic Land Facilities and Platforms"), assigned by the European Defense Agency (EDA). SWADAR builds an

intelligent drone-based network for mobile proximal sensing, tracking and neutralization of intruder swarms, as shown in Figure 2. Based on sensing and tracking data, SWADAR autonomously assesses the behavior of the rogue swarm by evaluating instantaneous and variational swarming metrics (i.e., cohesion, segregation, etc.) that can help in identifying the attack scenario and predicting the course of action of the swarm attack. Such information supports the selection of optimal neutralization actions to suppress the enemy swarming behavior. Moreover, SWADAR relies on on-board sensors, like LiDAR (light detection and ranging), optical and infrared sensors, etc., which are typically available on the market.

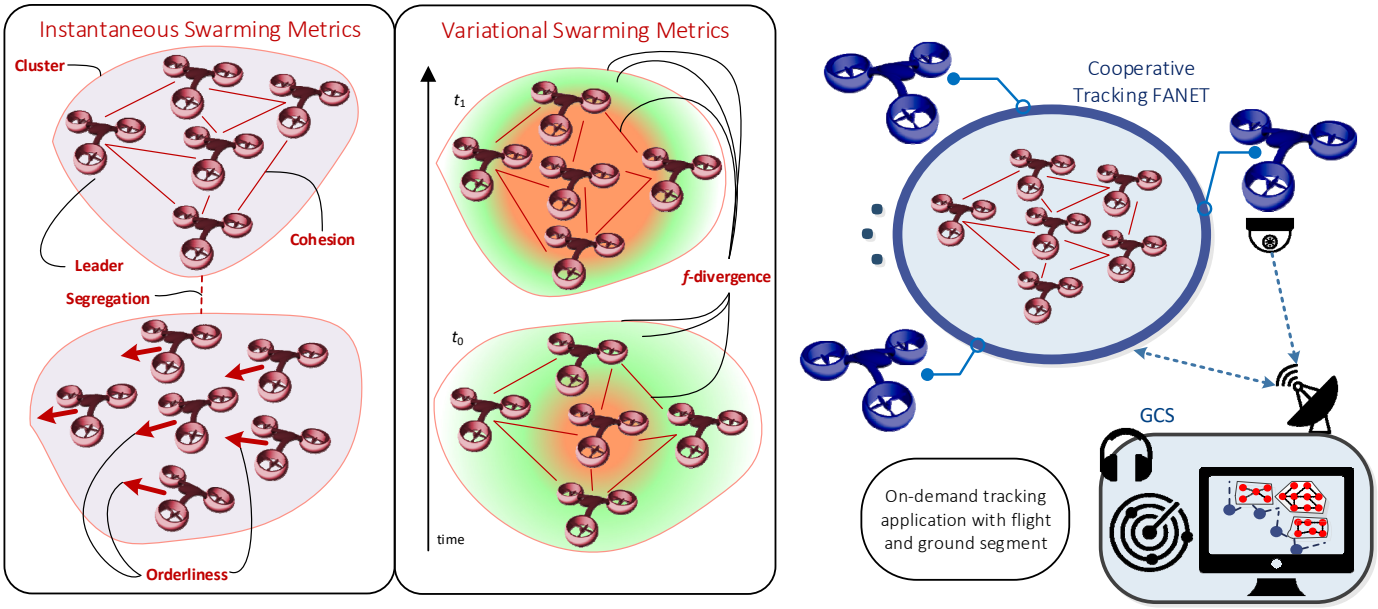

Figure 2. SWADAR concept for assessing swarming metrics (**a**) and for multi-UAV cooperative tracking (**b**) [27]. The left part shows some examples of useful metrics to measure the swarm behavior of intruder drones. Some of these metrics are: the cohesion, the segregation, the presence of hierarchical structures and clusters and the f-divergence (i.e., the temporal variation of the spatial distributions of the swarm).

In the US, the DARPA is funding the Aerial Dragnet program that seeks to perform persistent wide-area surveillance of multiple small drones in urban terrain on a city-wide scale. This innovative sensor array should be mounted on tethered drones, enabling a non-line-of-sight (NLOS) tracking and identification of a wide range of slow, low-flying threats [28].

Worthy of note is also the European project JEY-CUAS (Joint European System for Countering Unmanned Aerial Systems) [29], which will pave the way for the development of a joint European counter-UAS capability by developing a new-generation C-UAS system based on a modular and flexible plug'n'play architecture to include the emerging challenge of mini drones, increasingly used for defense purposes. The solution will contribute to an improvement of the situational awareness and reaction engagement by reducing the minimum reaction time.

However, not everything can be achieved through the use of mini drones. In some cases, ground systems are required—if we consider the case of early detection, it would be inefficient to keep drones in flight permanently to check for the presence of malicious drones in the area to be protected. Furthermore, with mini drones, we should consider SWaP constraints, and consequently, not all of the operations necessary to fight the threat could be performed via these platforms. For example, it is not possible to use strong

neutralizers (like high-power electromagnetics or high-power laser), which cannot be integrated on mini drones due to obvious SWaP constraints. However, mini drones can be a suitable solution, especially in civil contexts where protection is mainly required towards small drones.

3. Sensing System

The perception of a threat makes use of the sensing system, consisting of one or more sensors capable of collecting the information extrapolated from the electromagnetic or acoustic spectrum, depending on the technology and the signal processing involved. In general, the perception operation can be divided into the following phases:

- Detection: The finding of one or more object within the airspace to be monitored. In this first phase, the system is not yet able to distinguish whether the detected object is actually a drone. This phase can be characterized through the two indicators "Detection Rate" and "False Alarm Rate", which express the probability, respectively, of correct detection and false alarm.
- Classification: Once the detection event has occurred, it is necessary to verify that the detected object is actually present and that it is a drone. It could happen, for example, that the target detected in the previous phase is a bird, which has electromagnetic characteristics that can be similar to those of a drone (the radar cross section or the size and geometric shape that is possible recognize visually). This verification is also called "recognition" or "identification". Subsequently, the system extrapolates some salient attributes (features) of the drone, such as the type (size, type of propulsion, number of rotors, model), the possible location of a remote pilot, the presence of a payload and its typology. This phase may be found in the literature under the term "identification".
- Localization/Tracking: The target is located by estimating its position in terms of angle and distance. Triangulation techniques can be used to increase accuracy. Once the target has been locked in, it must be tracked throughout its flight. Flight trajectory could also be predicted.

The level of reliability of this information must be as high as possible so that the C2 system can perform the threat analysis and select and adopt the most appropriate mitigation measures in the shortest time interval. Detection, recognition and identification (or classification) could be performed by a single type of sensor if the technology and associated processing are compatible with the required output. Where this is not the case, it is possible to adopt a heterogeneous sensing system consisting of sensors with different technologies, which can contribute, thanks to data/sensor fusion techniques, to obtain a reliable level of identification and to improve performance in terms of range, detection time of the anti-drone system, detection rate and reduction of false alarms.

Clearly, to face an attack by a team or swarm of drones, the sensing system should be enriched with functionalities for the perception and the processing of information about the features that are strictly related to the teaming or swarming behavior of the attacker.

In more detail, one of the most complex scenarios that an anti-drone system can face is that relating to the attack of a drone swarm, e.g., for saturation attacks and to overwhelm the counter-capability of the target's defense. As for a hostile team, this scenario requires that the detection capabilities are also used for the extraction of "global" features that characterize the swarm and not only for the "local" features related to the drones that compose it. Moreover, specific information should be collected to quantify swarming metrics (e.g., consistency, cohesion, etc.) related to the swarming behavior. For this purpose, it may be useful to acquire both local information (e.g., flight configuration, geometry characteristics and speed) and global information (e.g., number of vehicles, relative distances, geometry of the swarm, etc.) [30]. Such information will be essential to infer the mitigation decisions, since they may support the identification of the drones that represent the "focal points" within the hostile swarm.

3.1. Sensing Technologies

An anti-drone system, to fulfill its purpose, must be equipped with a sensing system consisting of one or more sensors, including those of different technologies. There are, in fact, different types of sensors, which are characterized by the observed phenomenon, electromagnetic or acoustic, and by the spectrum band they use. For example, image sensors operate in the electromagnetic spectrum, in all visible frequencies, while a radar can operate at microwave frequencies.

The first technological distinction to which we can refer for the classification of sensors is between active and passive sensing. The substantial difference between the two types is based on the use of energy to "feel" the objects present in space. For active sensors, an electromagnetic or acoustic radiation is emitted, with which it is possible to directly measure the distance of objects in space through, for example, the measurement of the delay between the radiation emitted by the sensor itself and that received by the back-scattered reflections of the objects. Radars and LiDAR sensors belong to this category. On the other hand, passive sensors receive energy from the environment and from the object to be detected, which can be used to reconstruct useful information. Most of the passive sensors used are optical and infrared cameras.

There are many reviews on the current state-of-the art technology in this wide variety of sensors, both commercial and academic ones (for example: [31]). Instead, in the following subsections, we are focusing on the literature with drone-based-only use cases. So, it is possible to assume that all the following sensing technologies are suitable for use aboard mini and micro-drones.

3.1.1. Acoustic Sensors

The engine and propellers of the drones generate acoustic waves in the frequency range between 20 Hz and 20 kHz, which give rise to the acoustic signature of the vehicle. A single microphone can acquire this information and thanks to the comparison with a library of acoustic signatures, it can distinguish a drone from other objects and carry out the identification phase of the aircraft by obtaining information on the model. If the number of microphones is increased, it is possible to adopt spatial diversity techniques or use beamforming techniques by arranging the installation of an array of microphones onboard the drone. In this way, it is possible to estimate the azimuth and elevation of one or more targets through the direction of arrival (DoA), perform multiple target tracking and mitigate the ego-noise effects, i.e., the noises of the electric motors and the moving propellers of the drone itself.

This type of sensor is particularly economical, but is sensitive to environmental noise and climatic conditions related to wind or temperature and typically has a detection range that depends also on the microphone array size. This technology is typically used for ground-based counter-UAS platforms, but no airborne commercial products have been found. However, as the following articles demonstrate, the dimensions of a microphone array are compatible with the installation onboard a drone. For example, in [32] and in [33], some small-sized drones were set up with an array of microphones to locate a generic noise source. The ability to perform localization and tracking in terms of DoA and to identify noise sources were analyzed in [34], in which a circular array (ground-based) was used and, thanks to sound signal processing and array signal processing, an identification success rate of 80% was shown under the test conditions described in the article.

The detection range depends on the quality of the microphones, the characteristics of the array and the type of processing performed. In fact, the results that can be found in the literature vary in a fairly wide range, from 5 m of [35] up to 600 m of [36]. In [37], a ground-based system of two arrays of four microphones (spaced by 1 m) each was used for the location of a drone through the calculation of the DoA. Comparable results were obtained with GPS accuracy and a detection range of 100 m. In [36], a ground-based configuration was used with the arrangement of the array of tetrahedron microphones. In this case, a detection range of up to 600 m with a success rate of 99.5% was highlighted, at the same

time, however, the tracking capabilities were poor. In [38], on the other hand, an array of 120 elements arranged on a spherical structure allowed the detection and identification of various commercial drones up to about 290 m. It should be noted that the classification range may be lower than the detection range, as shown by the test campaigns carried out for the system described in [39].

Finally, an array of eight microphones was used in a scenario that is very similar to the one considered in this study ([35]), involving a tracker drone and an intruder drone. In this case, machine learning was used, and signal processing is done in real-time onboard the aircraft. The detection range was extremely small, equal to about 5 m, but there were excellent tracking capabilities.

3.1.2. Radio Frequency Sensors

Radio frequency (RF) sensors capture the electromagnetic signals radiated by a malicious drone or by the remote pilot's radio control, if present. It is, therefore, a passive method that does not require the transmission of electromagnetic waves and, therefore, has no restrictions on use (e.g., in an urban environment). Most commercial drones use an uplink radio channel for remote control commands and a downlink channel for telemetry and video signal. In the case of autonomous drones, there may be only direct downlink transmission to the ground control station (GCS) or communication between the nodes of the network in a swarm. The detection systems based on this technology make use of a RF receiver between 400 MHz and 6 GHz and an array of antennas for the possible exploitation of MIMO techniques. The receiver can be implemented through software-defined radio (SDR) due to the reconfigurability and flexibility characteristics of the radio frequency front-end and associated baseband processing. RF detection can be performed with techniques based on a known protocol or recognition of the spectral pattern. In this case, we refer to drones that communicate with the remote pilot through communication standards such as IEEE 802.11 (Wi-Fi), a case that covers a large part of commercial drones. In this way, it is possible to retrieve the MAC address of the device and trace the specific drone model.

In addition to the recognition of the spectrum and the communication protocol, it is possible to recognize the RF fingerprint of the radio controller and then carry out the classification of the drone through machine learning techniques, as described in [40]. These techniques are not very effective if a known pattern is not used, if the communication scheme has been customized or if the MAC address database is not updated ([41]).

For this reason, techniques based on the localization of the RF signal have been developed. So, the DoA estimation is carried out in two different ways: based on received signal strength (RSS) or spectral analysis. In the first case, the results are less accurate than in the second. For example, in [42], an architecture based on an array of four antennas and an SDR platform for processing was proposed, in which an angular precision between 1.9° and 6° was achieved over a coverage range between −60° and 60°. In [43], an experiment was presented in which, thanks to the use of commercial SDR platforms (FPGA-based), it was possible to localize small drones with a maximum range of 75 m. Although previous publications have been ground-based, they described techniques that could also be used on-board. In [15], a UAV-based system was described, in which a tracker drone can track an intruder drone by measuring RSS. The coordinated use of multiple drones for locating the RF source was also considered in [44,45]. In the latter, the air-to-air communication channel was simulated and compared with the ground-to-air one in an urban context. The research aimed to analyze the differences in terms of location accuracy vs. SNR. The results showed a clear advantage for the air-to-air solution.

3.1.3. Optical Sensors

Optical sensors detect electromagnetic waves in the range of frequencies from infrared (300 GHz) to ultraviolet (790 THz). It is a passive technology, therefore with low energy consumption, which can provide two-dimensional images of the surrounding environment. Optical sensors can be divided into two main categories, depending on the frequency

band in which they work: visible (VIS) or non-visible. For example, the first category includes optical cameras, which can detect electromagnetic radiation in the 430–790 THz frequency range, while the second category includes thermal cameras, which convert infrared radiation (300–430 THz) into images.

Thanks to image processing techniques based on computer vision (CV), it is possible to detect, classify and track drones that fall within the field of view (FoV) of the optical sensor. The aforementioned operations are similar to object detection and tracking, which is a much-studied problem in the CV field. An object can be detected thanks to features such as geometric shape or outline and features related to movement between consecutive frames. In the event that the sensing system is mounted on-board a drone, the dynamism of the scene must be considered, which introduces problems of variation in lighting conditions and background characteristics. The sensors that operate in the visible frequency band show their limits in the case of adverse weather conditions (rain and fog) and the case of low ambient light such as at night.

Infrared (IR) sensors allow us to overcome these limits ([46,47]) and offer greater robustness against rapid changes in illumination [48]. Two types of existing approaches in the literature are essential [49]: direct or feature-based techniques and machine learning methods. The first category includes algorithms that try to identify a specific region of interest in the image by looking at the best similarity with a reference representation of the target. In direct techniques, information on the local gradient is used in each pixel of the image, while in feature-based techniques, features are used that are followed in a sequence of frames through specific descriptors. The detection and tracking capabilities are good, as highlighted in [50], where the processing is based on techniques of background subtraction and optical flow calculation.

Machine learning techniques are very popular among the scientific community. The training of a neural network for target detection and classification is one of the most studied fields of CV. In fact, given the great accessibility of standard optical cameras, this research area has reached a fairly mature stage. Thanks to the large availability of public image datasets, UAV detection challenges are often organized at international conference workshops, such as Advanced Video and Signal-based Surveillance (AVSS) conference and International Conference on Computer Vision Systems (ICCVS).

Image classification with the deep learning paradigm is one of the most active fields of research. Most of the works that employ deep neural networks (DNNs) for drone classification problems utilize a generic object detection architecture, with a powerful DNN as a classification model targeted for drones. The most used architectures are:

- Single-shot multi-box detectors (SSD)
- Faster R-CNN

A particular SSD architecture is the You Only Look Once (YOLO) model, which has gained great popularity thanks to a particular computational efficiency that allows its use also on embedded systems in real time.

The adoption of different CNN architectures (e.g., Zeiler–Fergus (ZF), visual geometry group (VGG16)) for drone detection has been investigated in [51]. To overcome the limited amount of data available for training the deep networks, authors exploited transfer learning from ImageNet and performed a pre-training to fine-tune the models. The experimental results revealed that VGG16 with faster region-based convolutional neural network (R-CNN) achieved the best performance among all the considered architectures.

The authors of "Drone Detection in Long-Range Surveillance" [52] worked on a previous iteration of the same dataset, with quite good results in the detection of small objects. They applied a Faster R-CNN network with various backbones and showed that ResNet-101 had the best results.

In [53], a deep-learning-based detection method was adopted, termed YOLOv2, whose training is performed using an artificial dataset obtained by mixing images of real birds and drones, each with a different background. The obtained results demonstrated that

the diversity and the scale of the dataset have a positive impact on the detection and tracking processes.

The size, weight, required power and cost of the cameras is such that their use on drones does not find particular impediments and certainly makes it possible to use them as a sensing system for C-UAS for all operations of detection, identification and tracking.

3.1.4. LiDAR Sensors

LiDAR uses electromagnetic radiation at the optical and infrared wavelengths. It is an active sensor that emits electromagnetic waves and receives reflected waves, similarly to the operation of the radar, only at much higher frequencies, between 200 THz and 400 THz. Thanks to the calculation of the time difference between the emitted and received ray (time of flight), it is possible to process a 3D map of the surrounding environment and, thus, obtain the position, direction and speed of the objects in the scene. The speed can also be calculated from the doppler shift due to moving objects. These sensors are widely used in the automotive sector for safety systems related to autonomous driving (adaptive cruise control, lane-keeping, emergency braking). They can be used for simultaneous localization and mapping (SLAM), which allows robots to orient themselves in an unknown space and GPS-denied environment. The compact size allows it to be used on-board UAVs, both as a payload, for example for aerial mapping applications, and as avionics for collision avoidance systems.

There are different types of LiDAR sensors: those that measure only the range, called 1D, to those that measure the angle of arrival in the azimuth and elevation, as in an optical camera, and in addition, they obtain information on the range. It should be noted that the maximum operating range depends on the reflectivity value of the material and the color of the object hit by the light radiation. Given the wavelengths, the LiDAR (especially in the 1D case) can have a reduced operation in conditions of fog, clouds or rain, but offers the advantage of being able to be used also in conditions of low ambient light (at night, for example). The processing of the data acquired by this type of sensor requires a relatively low–medium processing effort compared to other types of sensors.

Most publications in the context of counter-UAS systems are ground-based. In [54], a LADAR (laser detection and ranging) is described, based on LASER, with a peak power of 700 kW, which allows for the increase of the operating range up to 2 km. In [55], an interesting experimental test campaign was carried out with a 3D LiDAR system mounted on a land vehicle to determine the probability of detection for mini drones. The results showed how, with sensors with a maximum operating range of 100 m, it is possible to have a high detection success rate for targets within 30 m. In [56], sensor fusion techniques were applied between a 3D LiDAR sensor and an RGB camera for detection, localization and tracking applications, with a maximum range of 50 m.

In addition to the CUS systems, publications in the field of collision avoidance systems (CAS) for UAVs that use sensing techniques based on LiDAR were also considered. The problem of obstacle detection is very similar to that of the detection/identification and localization of malicious UAVs. In [57], machine learning and data fusion techniques were used for the combined use of 3D LiDAR and optical cameras, obtaining an obstacle detection range of about 30 m. In [58], a 2D LiDAR sensor was used, obtaining a detection range of about 8 m compared to the sensor's maximum range of 25 m. The analysis of the state of the art shows how LiDAR-based technology is widely used for the detection of targets concerning CUS systems and obstacles concerning CAS. The ability to separate objects from the background and range measurement are interesting features for this category of sensors and can be used, for example, in the extrapolation of geometric features related to a possible scenario involving a hostile swarm.

3.1.5. Radar Sensors

A radar is an active sensor, consisting of a transmitting segment that radiates electromagnetic waves in the frequency range from 3 MHz to 300 GHz, depending on the

application. The waves are reflected by the target objects and are received by the receiving segment of the radar. By properly processing the received signal, it is possible, for example, to calculate the time of arrival and the frequency shift due to the Doppler effect to obtain information on the distance and speed of the target. The power of the received signal is directly proportional to the radar cross section (RCS), a parameter that measures how easily an object is detectable and which depends on the size, material, distance and angle of the incident and reflected wave. The RCS of mini-sized drones and their speed have lower values than that of larger drones and aircrafts for which classic radar systems are designed. To increase the detection possibilities of drones, the micro movements of vibrating and rotating structures, such as motors and propellers, can be taken into consideration. In fact, such structures have a characterizing micro-Doppler signature (mDS) [59]), thanks to which, they can be recognized. There is a category of radars, called passive, which are not equipped with a transmitter but use the electromagnetic radiation emitted by external sources, such as those of the towers for broadcasting the DVB-T television signal, normally already present in the communication channel. This category will not be taken into consideration because it requires a priori knowledge of these sources and a static installation of the passive radar.

The main advantages of the radar are related to the robustness against environmental conditions: the operation is independent of the light conditions and atmospheric conditions. The disadvantage is that to obtain a high detection range, it is necessary to increase the transmission power, the limit of which will depend on the power available on-board the drone. For this reason, it is not possible to use a classic surveillance radar, and the use of the FMCW type (frequency-modulated continuous wave) is preferred, which has, among other things, a more affordable cost. Signal processing can be done on software-defined radio platforms equipped with FPGA technology and RF front-end. The most popular radars in this area are mmWave and UWB radars, with one millimeter and ultra-wideband respectively.

The literature analysis ([60–62]) showed that the detection range is typically around 100 m for millimeter-wave radars. In [63], a pair of UWB radars were used to locate a drone up to about 80 m. The classification skills are very good ([64–67]), thanks to machine learning techniques. In particular, in [67], the authors were able to discern the weight of the payload of a commercial drone through the analysis of the mDS. Using a radar system operating at the 2.4 GHz frequency, the classification allowed recognition of the cases that belonged to the set {no payload, 200 g payload, 500 g payload} with 90% success and a maximum detection distance of 100 m. In addition to the analysis of the scientific literature relating to CUS systems, it is also possible to investigate that relating to the applications of radar for collision avoidance, as the detection problem is common to the two systems. In this regard, by deepening the survey proposed in [68], it is possible to confirm the feasibility of installing these systems on-board small drones, despite the stringent SWaP constraints.

3.2. Sensing Technologies Comparison

As seen, the proximal sensing capability of a team of mini drones is the main clear advantage over a static, ground-based CUS. For example, the optical occlusion problem could have a minor impact on a drone-based video sensing system thanks to the possibility to change the perspective, taking advantage of the mobility of the drone itself. On the other hand, there is the need for an accurate video stabilization to mitigate the blur effect due to the drone movement. In Table 2, some pros and cons of using sensing technologies integrated in mini-drone-based platforms with respect to the static ground case are summed up.

Table 2. Pros and cons of using sensing technologies on-board a drone.

Sensing Technique	Pros	Cons
Acoustic	Possibility to move close to the target and improve the identification task.	Need for proper ego-noise cancellation due to the propellers noise.
Optical	Possibility to change the perspective and to operate close to the target with a higher resolution and better identification capabilities.	Limited computational power; need for efficient video stabilization.
RF	Better conditions of the air-to-air channel with respect to the ground-to-air one.	
LiDAR	Possibility to move close to the target and improve the detection phase.	Limited on-board power.
Radar	Thanks to the proximal sensing, less power of the active sensor is required.	Limited on-board power.

Each technology has a different detection range, classification capacity and energy requirement. For example, the optical sensors in the visible work very well only in line of sight (LOS) conditions, while the RF sensors can work in non-line of sight (NLOS) conditions. It is, therefore, impossible to reach a satisfactory situational awareness level with the adoption of a single technology and, in this regard, the simultaneous adoption of different sensing techniques is the winning way, as previously addressed in the concept of the defensive team and the related cooperative sensor network. Using sensor or data fusion algorithms allows for better results than those that would be obtained individually. For example, in [69], test campaigns were carried out on a detection system that showed how the use of the data fusion technique increased the detection rate. These improvements were achieved at the expense of system complexity and computational effort. The identification of the technologies that best complement each other is a useful activity in order to optimize the level of situational awareness with respect to the complexity and cost of the system.

The following tables have been constructed to better highlight the characteristics of each technology. Table 3 contains a rough estimate of the performance in terms of "detection", "classification" and "global features characterization". It is not easy to establish the performance of each technology in absolute terms, which is why "low" to "high" range values have been indicated and express a qualitative judgment based on the literature reported in the previous paragraphs. It should be noted that the distances detected in the experimental setups can be numerically very different from the datasheet of the CUS products that can be found on the market. The explanation of this deviation could depend on the different level of optimization that an engineering product has in front of the experimental setup and the different requirements of ground- and sky-based devices. However, the relationship between the different technologies should be respected beyond the absolute numerical values.

Table 3. Sensing techniques' relative performances.

Sensing Technique	Detection Range	Classification Capability	Global Feature Characterization
RF Scanner	Higher than 150 m	High	Low
RF RSS	Higher than 150 m	Low	Low
Acoustic	Higher than 150 m	Medium	Low
Lidar	Between 50 m and 150 m	Low	Low
Radar	Higher than 150 m	Medium	Medium
VIS	Higher than 150 m	High	High
IR	Lower than 150 m	Low	Low

Table 4 is populated with the characteristics of localization/tracking and robustness against adverse environmental and meteorological conditions.

Table 4. Sensing techniques' tracking properties and robustness against environmental and meteorological conditions.

Sensing Technique	Localization	Multi-Tracking	Meteorological Conditions	Environmental Conditions
RF Scanner	DoA	Possible	-	RF Spectrum congestion
RF RSS	DoA	Possible	-	RF Spectrum congestion
Acoustic	DoA	Yes	Wind	Noise
Lidar	DoA/Range	Possible	Fog, rain	Direct Light
Radar	DoA/Range/Speed	Yes	-	-
Optical VIS	DoA	Yes	Fog, rain	Night
Optical IR	DoA	Yes	Fog, rain	Background temperature

The RF, acoustic, radar and optical VIS sensors have a wide detection range, in particular, the first two are able to work also in NLOS mode. Optical sensors, however, are not a good choice in the presence of adverse weather conditions, and, in particular, VIS sensors are unable to work in the absence of light.

As far as the classification process is concerned, optical systems are best expressed in conditions of proximal sensing. RF and acoustic sensors use machine learning-based pattern recognition techniques for the identification of remotely piloted amateur drones. RF systems also allow for the estimation of the position of the pilot in addition to the specific model of drone used. Radars have good classification capabilities based on the micro-Doppler signature.

Radar allows the direct estimation of the distance and speed of one or more drones; for this reason, it can be considered as an adequate technology for the extraction of the global features of a drone swarm, and for their localization and for operation of tracking. The use of optical sensors flanked by the ranging capability of the LiDAR allows, in this case, for the extraction of visual features that allow the determination of the geometric characteristics of the swarm, such as the occupied area and the flight configuration. Furthermore, tracking is a task that is typically dealt with via computer vision with a good level of reliability.

Table 5 proposes a subdivision into "main" and "complementary" technologies on the basis of the information developed so far.

Table 5. Main and complementary technologies.

Task	Main	Complementary
Detection	Radar, Acoustic, RF	Optical
Classification	Optical, RF, Acoustic	Radar
Global Feature	Optical, Radar	Lidar
Localization	Radar, Lidar	RF, Acoustic
Tracking	Radar, Optical, Acoustic	Lidar, RF

For each phase of the sensing, "main" technologies are indicated, which have a high probability of completing the task successfully. The "complementary" technologies were considered those that can improve the result obtained by the "main" ones.

4. Neutralization Systems

Neutralization systems are activated by the command-and-control system to respond to the threat posed by the detected malicious drone(s). Multiple neutralization systems can be activated simultaneously in order to cooperate to improve the effectiveness of the neutralization. Furthermore, these systems can be located on one or more distinct platforms according to the CUS physical architecture.

According to the classification reported in [9], neutralization systems can carry out the following actions: warning, control, interruption, disabling and destruction. These actions are implemented through neutralization techniques, more simply indicated as neutralizers (or mitigators). Neutralizers have been classified in different ways in the literature. In [9], neutralizers were divided into physical and non-physical based on whether there was physical damage to the m-drone. Moreover, in the case of non-physical neutralizers, there is no contact between the neutralizer and the m-drone, but some of them can actually cause damage to the m-drone. A similar subdivision was also shown in [10], even if some neutralizers fell into different classes. However, in [5], the subdivision was made between electronic neutralizers, based substantially on electromagnetic waves that do not cause direct damage to the m-drone (for example jamming), and kinetics neutralizers, which intercept the drone with physical means (for example nets), but the latter ones also include high power lasers and microwaves. Given that each definition described gives rise to some ambiguity, the following classification will be adopted:

- Electronic neutralizers, based on the use of electromagnetic waves capable of interrupting (operations), disabling or even destroying (at least partially) a drone;
- Kinetic-mechanical neutralizers, based on the use of mechanical means, which involve contact between the neutralizer (or a part of it) and the malicious drone.

4.1. Electronic Neutralizers

Electronic neutralizers allow instant actions, can easily aim at the target and are not affected by environmental agents (for example wind and gravity). They can be implemented with different techniques, such as cyber-attacks, high-powered electromagnetics and lasers. Cyber-attacks include jamming and spoofing techniques, which constitute the vast majority of neutralizers used in the context of UAVs, protocol-based attacks (for example, de-authentication and address resolution protocol (ARP) cache poisoning in the case of Wi-Fi networks) and replay attacks. Below a survey is reported.

4.1.1. Radio Frequency Jamming

Radio frequency (RF) jamming techniques allow users to disturb, lower the quality of or interrupt communications between the malicious drone and the respective remote-control station. They consist of generating an interfering signal in order to lower the SINR (signal-to-interference-plus-noise ratio) input into the receiver of the m-drone in order to make it difficult, if not impossible, to receive the information sent by remote control. Obviously, it is also possible to jam on the remote control in order to disturb any feedback data sent by the m-drone. A jammed drone can have different reactions depending on how it is designed [5]: it can make a landing in its current position, it can perform a return-to-home procedure, it can fall to the ground without control or it can fly in a random direction with no control.

RF jamming can be applied to other signals in addition to the remote control one. For example, in [70], jamming was applied to a video link used for the first-person view (FPV) function, showing the possibility of disabling this function and preventing the operator from maneuvering the drone in the absence of LOS conditions. Jamming can also be used to improve the robustness of a wireless communication in the presence of an eavesdropper. This is the case of cooperative jamming, in which a relay node transmits a jamming signal at the same time as the legitimate source transmits its message in order to disturb any eavesdropper [71]. By reversing the perspective, jamming can also be used to increase the probability of interception of a communication. In [72], for example, a legitimate drone,

used to follow the flight of two suspicious UAVs in order to prevent any threats, transmits jamming signals to the receiving UAV in order to force the decrease of the exchanged data rate and increase the likelihood of interception of information exchanged between suspicious drones.

There are several radio frequency jamming techniques. In this paper, we refer to the simplified taxonomy used in [10], but a more detailed one is available in [73]. The first technique, the noise jamming (also known as barrage jamming), is the simplest to implement and consists of applying a noisy signal to a portion or to the entire spectral band occupied by the signal which has to be jammed in order to reduce the channel capacity and increase the number of errors in the received data. Noise jamming can also be used in the presence of m-drones equipped with a synthetic aperture radar (SAR) able to offer autonomy thanks to SLAM techniques. In this case, the interference generated by the jamming signal may be sufficient to mask the echoes related to the SAR, making the latter unusable, as highlighted in [74]. The second technique is the tone jamming: in this case, one or more tones (i.e., narrow band signals) are employed for the purpose of generating interference. The effectiveness depends on the positioning of the tones and the transmitted power. The third technique, named sweep jamming, consists of transmitting a narrow band signal that sweeps the spectrum of frequencies of interest over time. At each instant of time, only a portion of the spectrum is covered, but in a certain period (the amount of time necessary to make a complete sweep) the whole band of interest is affected. The fourth, and final, technique is smart jamming, also known as protocol-aware jamming. It is applicable when the characteristics of the target signal are known a priori. For example, if the communication system under jamming uses frequency hopping spread spectrum (FHSS) and the hopping pattern is known, then the neutralizer can perform the same frequency hops as the target and reduce the bandwidth required by the interfering signal. Similarly, if the target communication system uses direct sequence spread spectrum (DSSS), the spreading properties of the signal to be attacked can be used to transmit a jamming signal possessing a high correlation with respect to the original one in order to increase the bit error rate of the communication to neutralize. Therefore, smart jamming is both effective, as it is calibrated precisely on the target signal to be disturbed, and efficient in power, as it operates only in correspondence with the target signal (in time and frequency). In any case, if no prior knowledge of the communication system to be neutralized is known, an analysis of the relevant signal must be carried out in order to identify its characteristics and weak points. Consequently, SDR technologies are well suited to the implementation of smart jamming; thanks to their flexibility, they allow for both the analysis of the target signal and the reproduction of an ad hoc signal to be used as an interfering signal ([75,76]).

The performance of the above jamming techniques can be assessed with respect to most available communications on commercial drones, i.e., the communications based on spread spectrum, like the transmission systems ACCST (Advanced Continuous Channel Shifting Technology), based on FHSS, and FASST (Futuba Advanced Spread Spectrum Technology), based on FHSS with the addition of Gaussian filtering and DSSS applied on the data. Furthermore, in order to consider even drones equipped with Wi-Fi connection, the IEEE 802.11b standard, based on DSSS, and the 802.11g standard, based on orthogonal frequency division multiplexing (OFDM), can be assessed. The listed systems cannot complete the panorama of implementable communications, but offer an early coverage of the transmission protocols (with reference to the physical layer) typically used by drones. The experimental evaluation of tone, sweep and smart jamming with respect to ACCST and FASST is shown in [75]. The results showed that smart jamming is significantly more efficient than tone and sweep jamming—the tone jammer can successfully jam a single channel of the link but is not sufficient to terminate the remote control link, and the sweep jammer requires relatively high jammer-to-signal ratios (JSRs) to completely prevent the communication, whereas smart achieves successful jamming at relatively low JSRs but requires significant knowledge about the targeted system. In the same work, noise jamming was also evaluated (with respect to an FHSS/DSSS hybrid system by means of simulations),

resulting in the techniques which require a higher JSR to prevent the communication. When considering the impact that the jamming signals have on WLAN devices, a comparison between noise and tone jamming is shown in [77]. If the jamming signal is stronger than the desired signal, the 802.11g system cannot operate in any mode unlike the 802.11b system, which uses lower rate DSSS modes, however, at the certain packet error ratio (PER) the 802.11g system can offer higher data rates than the 802.1lb system under wideband jamming. When tone jamming is used, the performance of the 802.11g system depends highly on the jamming frequency. In DSSS systems, the jamming frequency is not as important a factor as in OFDM, but higher JSRs are required to increase the PER with respect to the noise jamming. An experimental comparison between sweep and smart jamming for the WLAN case is shown again in [75]; in the most extreme cases, the sweep jammer halted the WLAN communication, while the protocol-aware jammer solely limited its maximum throughput.

Neutralizers based on RF jamming techniques, also known as jammers, can be integrated on static, mobile and/or portable ground platforms (examples are illustrated in [78–80]). It is also possible to integrate them on aerial platforms, like mini drones. Finally, they can be active, i.e., they continuously transmit interfering RF signals or randomly to save energy, or are reactive, i.e., they transmit interfering signals only after having determined that the monitored frequency spectrum is occupied by unknown signals (see [81]).

4.1.2. GNSS Jamming

GNSS (Global Navigation Satellite System) jamming is not a different technique from RF jamming, but simply refers to the jamming of GNSS signals. It is treated separately because of its relevance considering that GNSS signals are typically those most subject to neutralization. Signals received from satellites are characterized by low power value and, thus, are vulnerable to interfering signals; therefore, the technique under consideration can be effective. In fact, as reported in the study in [82], jamming the GPS receiver of a commercial drone can result in drifting and control difficulties, as well as preventing the return to home (RTH) procedure from working properly.

To implement GNSS jamming, the same radio frequency techniques illustrated in the preceding paragraph can be used. These techniques have been analyzed and evaluated in relation to GPS signals in [83], together with successive pulses jamming, which involves transmitting a sequence of pulses over time with a small duty cycle to the central frequency of interest and can be seen as a particular implementation of noise jamming. Best results are obtained with smart jamming and sweep jamming—the first technique is the most effective when compared to its purpose (making the GPS signal to the receiver unusable), while the strength of the second one is the simplicity of implementation, although it should be noted that the obtained efficiency depends on the speed used to sweep the frequency band.

GNSS jamming can be ineffective when malicious drones are equipped with IMU sensors. In this case, if the drone is equipped with a remote control link, RF jamming can also be useful. Similarly, GNSS jamming is highly important with m-drones not equipped with a remote control (i.e., RF jamming is not applicable), which follow a pre-programmed route with the aid of GNSS. Consequently, intrinsic weaknesses shown by RF and GNSS jamming can be compensated for by their simultaneous deployment in order to improve neutralization effectiveness.

Finally, considering the strategic importance of GNSS services, it should be noted that much research has been done in order to prevent and/or mitigate GNSS jamming; some methods, including those ones based on antenna arrays, are illustrated in the study reported in [5]. Therefore, a CUS shall pay attention to the effects obtained by means of such a neutralization.

4.1.3. Spoofing

Spoofing consists of generating a plausible fake signal with enough strength to trick the malicious drone receiver into believing it is the legitimate signal. The signals under spoofing

can be related to some different applications or devices: remote control communications, payload data communications, GNSS, sensors. In order to perform spoofing, it is necessary to know the communication protocol stacks used (not only the physical layer) so that they can be reproduced. If the stacks are known it is possible to analyze them a priori, otherwise first it is necessary to determine them in some way. Therefore, spoofing is a complicated method and not always a successful one. In any case, at least in theory, by using spoofing techniques, it could be possible to take control of the malicious drone and make it move away from a protected area. Some examples are shown in [84,85].

As mentioned above, a typical class of signals often involved in spoofing is represented by GNSS signals. In this specific case, it is possible to make the m-drone land, engage the autopilot, remain hovering or follow a desired path. Studies presenting methods for hijacking or disabling a drone using GNSS spoofing are reported in [86–88]. An interesting study is reported in [89], where the authors determined the necessary conditions for capturing a drone through GPS spoofing and examined a possible post-capture control system. Furthermore, two different strategies are depicted: overt spoofing and covert spoofing. In the first case, the spoofer (i.e., the spoofing-based neutralizer) does not hide its attempt to "subjugate" the target system and, therefore, does not align the forged signals with the legitimate ones. In particular, after a first phase in which it jams on the GPS receiver in order to force it to lose the lock and reacquire all the signals, it can take control, as long as the counterfeited signals have a power that satisfies two conditions: exceeding the receiver acquisition threshold and forcing the authentic GPS signals below the aforementioned threshold exploiting the receiver AGC (automatic gain controller) function. Experimental trials have shown that when the ratio between the counterfeit signal power (Pc) and the legitimate signal (Pl) is equal to 10 dB, the previous conditions are satisfied (as confirmed also in [90]). Instead, in the case of covert spoofing, the spoofer assumes that the GPS receiver and the navigation system are equipped with spoofing detection techniques, which must be evaded using appropriate counterfeit signals. Experimentally, it has been verified that if the spoofer can estimate the speed and position of the target drone with errors under certain thresholds (respectively below 10 m/s and 50 m), then it can reliably and covertly take control of the tracking loops of commercial receivers using small Pc over Pl ratio (of the order of units of dB). Notice that covert spoofing can be generalized and applied to any type of communication, especially if it has been assumed that the malicious drone receiver is equipped with anti-spoofing technology. In these cases, the counterfeit signal should be correlated to the legitimate signal as much as possible and with a similar power level trend over time, so that it can be confused with the legitimate one.

Rather than generating compatible counterfeit signals, GNNS spoofing can also be accomplished by meaconing ([10,90]), a technique consisting in interception and retransmission (at higher power) of the original signal to the malicious drone's receiver. Whereas the GPS signal is encrypted, a technique similar to meaconing, called security code estimation and replay (SCER) ([10,90]), can be used. It provides for the estimation of each symbol of the used coding by observing the signal received in the corresponding symbol period. The symbol estimation is continuously updated and is used simultaneously in the spoofing signal, trying to replicate the encoding as closely as possible.

Finally, spoofing applied to on-board sensors also deserve some attention. In this case, the spoofing source sends false signals to sensors, which can lead to the destabilization of the malicious drone control system. For example, as indicated in [91] and in references reported there, gyroscopes and accelerometers are sensitive to ultrasound at their resonant frequency and this vulnerability can be attacked. In [92], the authors spoofed the gyroscope of a drone, causing it to land. However, these attacks require powerful speakers and are limited in range due to the degradation of the sound wave with distance. Furthermore, a reference for a possible solution to an acoustic attack is always present in [91]. Other sensors that can be spoofed are those of the optical flow type. Their vulnerability was demonstrated in [93], where a method was presented to hijack a drone by spoofing the camera (thus affecting the stabilization algorithm) by means of a laser and a projector aimed

at the drone's surface. Again, in [91], there was evidence of the fact that the presence of a magnetic field in the vicinity of a drone, in this case the DJI Phantom, always requires the recalibration of the relative magnetometer before take-off.

4.1.4. Neutralizers Exploiting Protocol-Based Attacks and Replay Attacks

Some cyber-attacks try to exploit the vulnerabilities present in the protocols used in communication networks to perpetrate malicious actions. These attacks include denial-of-service (DoS) attacks, which consist in disabling a machine (or network), making it inaccessible to intended users. Wi-Fi de-authentication, which consists of disconnecting a user from the relative access point (WAP), and flooding, which consists of sending a large amount of traffic to the target in order to make it unable to process legitimate messages, belong to the above family. These attacks can also be aimed at drones. For example, as documented in [91], some commercial drones based on Wi-Fi communications that do not require authentication for network access have proved to be vulnerable to de-authentication and flooding towards the drone network interface controller (NIC). In particular, with de-authentication, it was possible to disconnect the commercial drone from its remote pilot in order to activate a security procedure and take advantage of the disconnection window to take control of it. Another cyber-attack used to disconnect a commercial drone from its controller is the address resolution protocol (ARP) cache poisoning attack, as shown in [94]. Many of these attacks can be prevented using a network access with authentication, but the basic idea can be used to implement a neutralizer to exploit this kind of attack. In other words, as in the spoofing case, it is possible analyze the protocols used by drones to determine some weaknesses, at one or more layers of the communication stack, to be used to carry out neutralization operations. It follows that this kind of neutralizer can be applicable and effective for commercial drones whose protocols are known. They are definitively not a robust solution if the above exploited weaknesses can be patched up by the users, however they could be applicable as a first neutralization technique for commercial drones used improperly but without illegal purpose.

Other techniques useful to implement as neutralizers are replay attacks. According to the classification reported in [91], they can be included within the family of protocol-based attacks. They are based on the interception of a data transmission and its subsequent retransmission with a certain delay and can be used to hijack and disorient a drone. Examples are reported in [95,96]. In the first case, a drone used by the police was hijacked by exploiting a replay of the control commands sent to the drone by the ground control station using the XBee 868LP protocol. In the second case, it was possible to hijack amateur drones using the MAVLink protocol with replay attack. Therefore, even these kinds of attacks can be taken in account, but because they are very simple, eventual countermeasures adopted by the malicious drone(s) should be considered. For instance, the study reported in [97] showed a detection mechanism applicable to replay attacks based on the authentication of the pilot who controls the drone manually. The mechanism uses a classifier capable of recognizing the pilot's distinctive control style by exploiting data from on-board motion sensors.

4.1.5. High-Power Electromagnetics and Lasers

High-power electromagnetics can be used to create beams of electromagnetic energy over a broad spectrum of frequencies, in a narrow- or a wideband way, causing a range of temporary or permanent effects on electronics of targeted drones. According to the classification shown in [9] they can be categorized in two classes: narrowband electromagnetics (also referred as high-power microwaves, HPM), which include high power on a nearly single-tone frequency, and wideband electromagnetics, which have short pulses in the time domain and the energy distributed over a wide band. HMP requires very high power on a single frequency. Consequently, the determination of the effective frequency, which causes malfunctions in the drone to be attacked, is a key factor.

High-power electromagnetics must be directed precisely towards the target to be effective, otherwise lethality is significantly reduced and some devices may still function

after their use. Hence, the assessment of the neutralization effectiveness after a shot is also an issue. An HPM-type device manufactured by Raytheon is illustrated in [98].

Lasers used as mitigators are capable of disabling or destroying an m-drone. As described in [9], an electrolaser ionizes the path to the drone and emits an electric current down the conductive track of the ionized plasma. Lasers can be categorized into low-power or high-power lasers [9]: low-power ones can be used to neutralize some sensitive sensors of the drone (for example, electro-optical sensors); high-power ones (operating at megawatts) can be a real weapon, able to burn part of the drone and destroy it. For both categories, accurate aiming is required, which implies sufficient time to track the target. Laser weaknesses are represented by the need for high technological development for their implementation (for the high-power lasers), sensitivity to weather conditions, accurate pointing and tracking time. A laser-based neutralizer manufactured by Boeing is illustrated in [99].

Both high-power electromagnetics and high-power lasers are a strong interdiction measure, typically used in a military context. In a civil environment, they cannot be a viable option, especially in crowded areas, due the risk of the uncontrolled drone crashing or of triggering the deployment of dangerous payloads. Nor are they suitable for airports and the surrounding space, due to the collateral hazard to aviation operations [5].

Finally, based on limited information available on the market about high-power electromagnetics and high-power lasers, we can easily deduce that they always show large size and weight and require a high power supply. Therefore, they can be mainly integrated into terrestrial platforms (typically they are mounted on tracks) and are not suitable for low-altitude platforms like mini drones.

4.2. Kinetic-Mechanical Neutralizers

Kinetic-mechanical neutralizers are able to physically block or even destroying m-drones. Aiming and/or tracking of malicious drones is required in order to effectively neutralize; in fact, these neutralizers must act as closely as possible to the drone under attack. Let us briefly examine the various types of the available kinetic-mechanical neutralizers, mainly using the data of the survey reported in [9].

For the sake of completeness, note that there is also a simple and economical method of neutralization, classifiable as kinetic-mechanical, not linked to technology and based on appropriately trained birds. This method, used for example by the Scottish and Dutch police (see [9] and relative bibliography), is limited to slow and small drones (with respect to speed and size and of the birds) and is not appropriate to mitigate multiple drones simultaneously [9]. For obvious reasons, we do not consider it as a possible part of a CUS system based on mini drones.

4.2.1. Neutralizers Based on Projectiles

These neutralizers are real weapons using projectiles capable of destroying m-drones. They include machine guns, munitions, guided missiles, artillery, mortars and rockets. Some of them (guided missiles) may require a guidance and tracking system in order to track and hit the drone target, while others can be equipped with an optical sensor for object detection and tracking. They are an expensive solution (the cost per shot is high) and typically used in military contexts. Finally, they are also capable of causing collateral effects, as the hit drone can fall to the ground causing damage to people and/or infrastructures.

4.2.2. Collision UAVs

In this case, a dedicated UAV (drone), equipped with detection and tracking capabilities, follows the malicious drone in order to collide and destroy it. The neutralizer drone requires high speeds to chase the malicious drone and, typically, it is effective for small drones located in protected areas. Collision UAVs can employ detection methods based on computer vision techniques and can carry explosives to maximize damage during impact with the m-drone. They can cause collateral damage, as in the case of projectiles,

and compared to the latter they are characterized by a higher neutralization delay. In conclusion, these neutralizers are disposable systems, acting as a hybrid system halfway between a drone and a missile. An example of a collision UAV is shown in [100].

4.2.3. Nets

Nets are used to trap and immobilize m-drones. They can be projected by a net cannon (an example is shown in [101]) or can be carried by other drones (an example is shown in [102]). Nets are useful for neutralizing small drones, which are difficult to intercept by guns or guided missiles (see bibliography in [9]). They can then be equipped with parachutes to assure a safe descent for the drone/net assembly and to prevent collateral damages to other facilities or for forensic analysis. In any case, the effective neutralization range is short.

4.3. Neutralizers Using Mini Drones

Aerial platforms, like mini drones, show some interesting characteristics, such as high maneuverability, flexibility and deployment speed, but have limitations in terms of SWaP constraints. Therefore, as already stated in the previous paragraphs, it is not feasible to integrate neutralizers like high-power electromagnetics and high-power lasers in these platforms. In addition, neutralizers based on projectiles are not applicable to mini drones, both for SWaP constraints and because they are typically designed to be used with the surface-to-air launcher installed in terrestrial platforms. Small projectiles could be installed on mini drones, but they can be assimilated to nets. All other shown neutralizers, electronic and kinetic-mechanical, can be used with mini drones, even if the use of low-power lasers requires accurate pointing, which could represent a critical issue to solve. In particular, in the case of collision UAVs, the platform is itself a neutralizer.

The use of mini drones can help to maximize the effectiveness or efficiency of some neutralization techniques. An example is RF jamming: by exploiting the mobility of a drone equipped with a jammer, it is possible to approach the m-drone in order to reduce the power necessary to disturb the signal under attack. Let us assume, for example, that in the case of a jammer installed on a ground platform, the minimum distance between jammer and malicious drone is 100 m, and that in the case of a jammer installed on a mini drone, the aforementioned distance is 10 m. The signal produced by the jammer installed on the mini drone consequently undergoes an attenuation lower than 20 dB compared to the signal emitted by the ground platform jammer. This advantage could be partially or totally compensated considering that in the ground platform, a directive antenna can be used to amplify the power transmitted in a certain direction, but, as shown in the work reported in [103], an antenna system capable of offering some directivity can be installed also on mini drones. Furthermore, multiples drones, which simultaneously transmit a jamming signal, could be used in a cooperative way to increase the power of the resulting interfering signal. An example is shown [104], where the authors investigated the problem of simultaneous tracking and jamming of a rogue drone in a 3D space with a team of cooperative drones.

Finally, a drone team can be used directly as a neutralization technique. In the work reported in [16], a drone-based system was proposed for the purpose of intercepting and escorting an m-drone outside a restricted flight zone. The system consists of a defensive swarm, which is capable of self-organizing its defense formation in the event of intruder detection and chasing the malicious drone as a networked swarm. The neutralization approach is as follows: the swarm forms a three-dimensional cluster around the m-drone in such a way that the m-drone has a minimum set of movement possibilities. Assuming that the m-drone is going to avoid collisions with the drones of the swarm to maintain its functioning, by moving the defensive drones in a cooperative way, it is possible to escort the m-done outside the restricted flight zone.

4.4. Comparison of the Neutralizers

A comparison of the neutralizers considered in this paper is shown in Table 6. For each neutralizer, both features and limitations are shown together with the pros and cons of using them as integrated in mini-drone-based platforms.

Table 6. Comparison of the neutralization techniques and their suitability with mini drones.

Neutralizers	Features	Limitations	Pros and Cons with Drones
RF Jamming	• Interfering RF signals are used to lower the SINR (signal to interference plus noise ratio) to the receiver of the malicious drone • Can be used with land platforms (static, mobile, portable) or even aerial platforms (included mini drones) • Can interrupt or lower the quality of the command-and-control link of the receiver drone • Directional antennas can be used to minimize unwanted interference • Allows users to increase the interception capacity of a UAV communication • Can increase the security level of a communication (cooperative jamming) • If the receiver of the malicious drone gets saturated, there are not countermeasures	• Ineffective with autonomous malicious drones (i.e., without command-and-control links) • The range of use depends on the power delivered by the jammer and the distance between the jammer and the malicious drone • Can create unwanted interference, disturbing other communications (even critical ones) • Regulatory restrictions can limit its use • Can cause uncontrolled flights or crashes of the malicious drones with possible collateral damage • Anti-jamming techniques can undermine its effectiveness	• Mini drones can provide limited power for the RF jamming • Needed power for RF jamming can be decreased approaching the defensive drone to the malicious one • A lower jamming power decreases unwanted interference • Needed RF power per drone can be further decreased using more drones simultaneously • A defensive drone can be used as a relay node, transmitting a jamming signal in order to disturb an eavesdropper • Using more drones simultaneously surrounding a malicious drone could allow users to counter some anti-jamming techniques (e.g., those ones based on the angle of arrival)
GNSS Jamming	• Can interrupt the GPS connection of the malicious drone • Makes it more difficult to control the malicious drone • GNSS signals are weak and vulnerable (if not encrypted), therefore this technique can be simple to apply • In some cases, it can prevent the return-to-home function • Can be used with land platforms (static, mobile, portable) or even aerial platforms (including mini drones)	• Ineffective with malicious drones equipped with IMU sensors • Dangerous if used near areas where satellite navigation is required • It can cause uncontrolled flights or crashes of the malicious drones with possible collateral damage • Regulatory restrictions can limit its use • Anti-jamming techniques can undermine its effectiveness	• Same pros and cons as for the RF jamming technique

Table 6. *Cont.*

Neutralizers	Features	Limitations	Pros and Cons with Drones
Spoofing	• Can be used to replace the C2 link or the GNSS service, allowing users to control the malicious drone • Can be applied to on-board sensors to destabilize the malicious drone control system • Can be used with land platforms (static, mobile, portable) or even aerial platforms (included mini drones)	• Information on the systems that are integrated in the malicious drone (sensors, link C2) must be available • An accurate analysis of the communication link or of the sensors to be attacked must be carried out • The technique is often complex and could not be successful (e.g., it is not ineffective for encrypted GPS) • Regulatory restrictions can limit its use • Anti-spoofing techniques can undermine its effectiveness	• No substantial advantages compared to static platforms other than the possibility of exploiting the mobility of drones to increase the operative range • Sensor spoofing could be not suitable with mini drones (e.g., pointing accuracy of the sensor to be spoofed could be an issue)
Protocol-Based and Replay Attacks	• Exploit vulnerabilities in drone communications protocols • Are often easy to implement • Allow to hijack a malicious drone, destabilize its flight or cause return-to-home procedures	• If the vulnerabilities of the communications have been corrected, they are ineffective • Can be mitigated with the help of machine learning (e.g., in the case of replay attacks)	• No substantial advantages compared to static platforms other than the possibility of exploiting the mobility of drones to increase the operative range
High-Power Electromagnetics	• Can damage the electronic systems of the malicious drone • Can be of two different categories: narrowband (high power over a narrow frequency spectrum) and wideband (short pulses in the time domain) • Aggressive countermeasure characterized by an extended range of action	• Accurate pointing towards the malicious drone is required • Lethality for the malicious drone could be low • It is difficult to assess the effectiveness obtained with this mitigation • Can cause uncontrolled flights or crashes of the malicious drones with possible collateral damage	• Not suitable for mini drones because they require large size and weight and a high power supply
Projectiles	• Traditional neutralizer (ammunition, guided missiles, etc.) • Fast response times	• Require accurate pointing • Wind and gravity also need to be considered (depending on the type of the projectiles) • Can cause crashes of the malicious drone with possible collateral damage • High cost per shot in the case of missiles equipped with a tracking and detection system	• Small projectiles could be installed on mini drones, but they can be assimilated to the nets case

Table 6. *Cont.*

Neutralizers	Features	Limitations	Pros and Cons with Drones
Collision UAVs	• Require detection and tracking capabilities of the malicious drone to be impacted • Are a hybrid system between a projectile and a small UAV • Effective for small drones	• Require capabilities of tracking and approach to the malicious drone to be impacted • Low-speed pursuit can result in delays in neutralization • The crash following the impact can cause collateral damage	• The drone itself is a neutralizer
Nets	• Can be projected from cannons or from flying platforms (included mini drones) • Nets equipped with parachutes allow a safe landing of the malicious drone • After the capture of the malicious drone, information can be extracted from its hardware	• Not appropriate at airports as they can cause side effects to other aircrafts • They need small distances from the malicious drone to have an effective neutralization • Accuracy can depend on the surrounding environmental conditions • Variable reaction times depending on the behavior of the malicious drone • Effectiveness also depends on the behavior of the malicious drone	• Small distance from the malicious drone to neutralize can be obtained thanks to the mobility of mini drones • The defensive drone must track and pursue the malicious one • Another approach is based on a team of drones forming a three-dimensional cluster around the malicious drone in order to limit or force its movement possibilities. The team of drones can be seen as a "net".

5. Command and Control Systems

The command-and-control system (C2) is one of the sub-systems of a CUS and it is an essential part for the implementation of the automated decision-making feature, which has been addressed in Section 2. Indeed, it is in charge of (possibly automated) high-level decision-making operations, such as:

- Providing a classification of the attack scenario to assess its threat level, based on the feedbacks coming from the sensing system;
- Granting permission to fly over a specific protected area (for non-malicious drones);
- Selecting the proper mitigation techniques to be used based on the attack scenario and its threat level;
- Planning CUS operations and monitoring their execution.

By means of the previous capabilities, the C2 system may aid the operator in facilitating the automated decision-making for mitigation actions. It can also perform the supervision and the management of the other sub-systems in a CUS. However, it may be convenient to distribute these functions by deploying them in dedicated systems, especially in the case of a cooperative drone-based CUS. In other words, the C2 system may be implemented not as a single centralized decision-making entity, but as a coordinated set of distributed decision-making entities. The rationale behind this assumption is as follows: a single management system could not be feasible in a complex application, such as a CUS with a higher number of platforms, in which some of the operations to be performed require a high degree of autonomy. A single decision-making entity would not be able to provide complete control of all the platforms, but it would have, at most, partial control over the operations performed by the individual platforms, despite having an overview of the threat represented by the malicious drone(s). A centralized decision-making system

would be extremely complex, both for the required computational capacity and for the communication network to be used to connect the various platforms. The latter, in fact, should be able to convey all the raw data collected by the platforms to the C2 system and to spread all the commands given by this latter system to the platforms of the CUS.

Clearly, one of the most critical design aspects of the C2 system is related to its planning capability, which has to guarantee an automated execution and has to affect the defensive team as a whole. Indeed, this capability represents the key enabler for the automated decision-making feature of the system. Generally speaking, planning is the reasoning side of acting and is an abstract and explicit deliberation process that chooses and organizes actions by assessing the current environment's situation (i.e., through automated situational awareness) and by anticipating the expected outcomes of the planned actions. This deliberation aims to achieve some predefined objectives as best as possible. It has to be implemented according to the principles of automated planning, which is an area of artificial intelligence (AI) that studies this deliberation process from a computational point of view [105].

The addressed planning problem includes aspects of different planning cases, such as activity planning (which is concerned with the allocation of activities or targets to a given entity), route planning (which is concerned with the synthesis of routes from a starting position to a set of targets a in a given area of interest), perception planning (which is concerned with the planning around sensing actions for gathering information), communication planning (which is concerned with the planning of communication actions for the cooperation between different entities, both human and artificial), etc. All these planning cases may be combined in the mission planning case, which is related to the planning of actions or tasks by projecting the results of those actions according to a model of the involved entities and by evaluating the desirability of those results. In the specific case of an unmanned system (UMS) and of a network of unmanned systems (NUMS), mission planning is defined as the process for the synthesis of a sequence of tasks in terms of tactical objectives, a route (general or specific), timing and coordination actions [106]. According to these definitions, mission planning mainly refers to a strategic horizon, since it represents a decision-making process to set objectives and tasks and to compute high-level steps (e.g., routes, sensing actions, communication actions, etc.) to satisfy the assigned objectives and tasks. Thus, it usually covers a wide temporal and spatial range with respect to the missions. The outcomes of the mission planning process have to be provided to tactical planners (e.g., the autopilots of the single vehicles), which have to compute short-term and short-range actions (e.g., the real trajectories) to satisfy the assigned tasks.

In the reference CUS, the C2 system has to optimize the operations carried out by the CUS and solve the mission planning process by:

- Computing the set of tasks to be carried out to counter the identified threat;
- Processing the optimal schedule (i.e., assignment and ordering) of the tasks, e.g., the allocation and the sequencing of the target areas to be protected and of the vehicle counter activities (in terms of detection, identification, classification, tracking and neutralization) to be executed;
- Operating over the entire time horizon and space horizon of the threat resolution.

Thus, it is a strategic planning level that sets the general objectives (the threat resolution strategy) and articulates the high-level steps to achieve them. Moreover, the reference mission planning is a dynamic (i.e., online) mission planning to face the dynamic threat scenario of the drone attack. Generally speaking, it is possible to carry out, where necessary or convenient, the following hierarchical decomposition for the C2 system: a module of the system may be explicitly in charge of the coordination of the team by means of a defensive team planning. Such a module is fed by the mission goals and the data of the team and deliberates the defensive tasks for all the vehicles by evaluating their effectiveness from the point of view of the team's mission and by considering the team's relationships and possible conflicts. It could be integrated in all the drones in order to obtain a decentralized architecture, in a single drone (working as team leader) or a in ground platform in the case

of a centralized architecture. Instead, lower-level planners, integrated in all the drones, are in charge of the planning logic for the single vehicle and are fed by the team plan that is deliberated at the higher level. The functional architecture of this planning logic is illustrated in Figure 3.

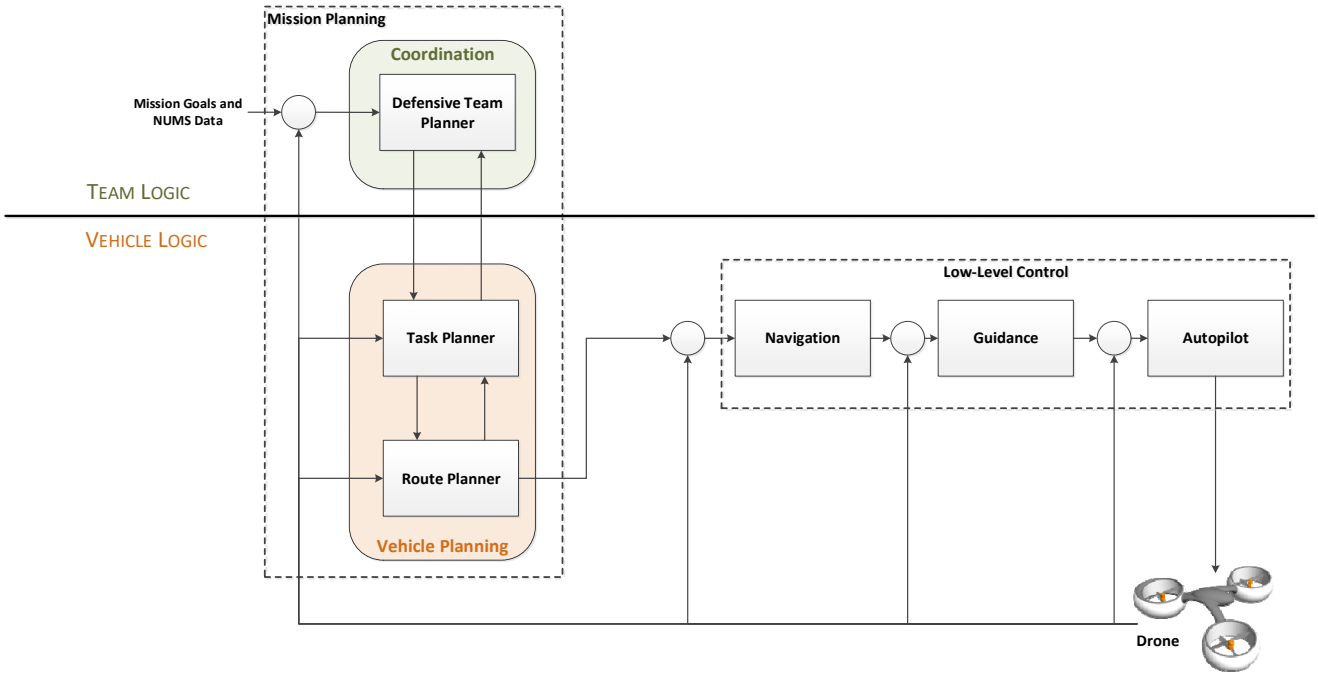

Figure 3. Functional architecture of the planning logic for the C2 system. Such logic is divided into team logic and vehicle logic. The former contributes to the planning of the actions of the overall team. Starting from the team plan, the latter performs the planning and the execution for the single vehicle.

The functional architecture in Figure 3 is compliant with the multilevel optimization principle [107] in order to ensure that the CUS-wide objectives and constraints are respectively optimized and satisfied along the hierarchy. In particular, the global planning problem is broken into simpler problems, which are independently solved. Moreover, the upper levels coordinate the solutions of the decoupled problems of lower levels by means of management functions.

The above hierarchical decomposition can also be used for operations provided by the other systems that comprise the CUS. Detection carried out through the simultaneous use of multiple drones is an example. In this case, based on the number of drones making up the detection system, a model based on "cooperative autonomous systems" can be applied, characterized by a collection of distinct decision-making entities (one per drone) or by a centralized control implemented into a drone hired as the team leader. In both the solutions, similarly to the previous case, the detection activity associated with drones could be subdivided into detection planning (the mission planning), aimed at coordinating the steps to complete the specific detection operation, and trajectory/flight planning (the vehicle planning), consisting of the generation of the trajectories of the individual drones between specific navigation points (scheduled by the detection planning).

Regardless of the shown hierarchical decomposition, it is clear that the use of mini drones could inherently require decentralization of C2 operations in order to simplify the overall CUS architecture.

6. Technological Challenges

A CUS based on mini drones can exploit some peculiarities of these platforms that give added value compared to CUS based on other types of platforms. The fundamental aspect concerns the use of teams, which allows operators to rework some of the techniques of

detection, classification, tracking and mitigation systems in order to maximize performance and effectiveness. However, in order to use drone teams, it is necessary to investigate and develop still-challenging technologies. These technologies are listed below.

6.1. Team Coordination

The coordination mechanism (i.e., the underlying mechanism to achieve a cooperative behavior) may concern: the imposition of an artificial interaction structure as a control or communication structure, aspects of the task specification, interaction dynamics of agent behaviors, etc. This may be seen as the "society design" or "macro design" of a multi-agent system, that is, the synthesis of a logical and physical protocol to ensure that the single agents interact to successfully achieve the global tasks and to avoid pursuing conflicting strategies or plans [108]. Coordination may be also defined as the "process by which an agent reasons about its local actions and the (anticipated) actions of others to try and ensure the community acts in a coherent manner" [109]. These definitions highlight that an effective coordination requires that each agent has to consider the actions of the other agents and that the main achievement is related to coherency, i.e., the goodness of the joint behavior according to the performance of interest for the given problem.

In regard to the design of the coordination mechanism of a team for a given application, one critical point concerns the decision-making architecture, centralized or decentralized. Note that, for the distinction between a centralized and decentralized coordination from an algorithmic perspective, stricter criteria should be adopted, which establish that a coordination of a planning problem is centralized if [110]:

- A single agent solves the overall problem; or
- All the agents solve the same overall problem; or
- The agents employ a wide number of communications (or a wide communication band) to plan their coordinated actions; or
- The agents exchange full plans.

To the contrary, a coordination is decentralized if the agents make their decisions independently and if they employ limited communications (i.e., to exchange positions, maps, etc.). This algorithmic classification introduces a degree of decentralization and influences the theoretical and technical challenges to deal with for the coordination of teams of unmanned vehicles. Indeed, the maximization of the degree of decentralization represents a crucial aspect, looking also at the most recent works. However, such maximization should also consider additional issues, often overlooked in the modelling, including the following realistic scenarios: failures and cyberattacks, sensing noise and modelling uncertainties, intermittent or limited communication, etc.

6.2. Team Communication Network

Considering the mobility characteristics of the drones belonging to a team, the communication network will be a FANET with certain requirements of throughput, latency, transmission robustness, multiple access, flexibility and with constraints of available energy in relation to the mobile nodes (i.e., drones). A review on the communications perspectives of FANETs, with key enabling wireless technologies, applications, challenges and open research topics, is shown in [111]. In particular, the following key elements must be taken care of.

- Routing—the algorithms used must be able to support a routing table capable of rapidly adapting to the continuous topological variations of the network due to the mobility of drones. A survey of routing techniques in FANETs is shown in [112].
- Reliability and security—the network must ensure availability and integrity (and, depending on the application, confidentiality) of the communication between the nodes, characteristics that can be obtained both by operating at a physical level and at some higher levels.

- Scalability—some network drones competing in the execution of a task may need to be replaced for technical reasons or due to the exhaustion of their energy resources, so it is necessary to add other drones to the team to efficiently complete the assigned task.
- Quality of service—different performances must be guaranteed according to the type of information transmitted and the level of criticality.
- Placement—the drones may need to be appropriately arranged in the 3D space in order to maximize the amount of information exchanged and minimize the time required for the exchange, so as to satisfy any energy constraints characterizing the nodes themselves. Clearly, this aspect also falls within the problem of coordination.

6.3. Team Simulation Framework

As previously mentioned, a CUS is a complex system that integrates multiple platforms and different technologies, and the use of a team of drones further emphasizes its complexity. Therefore, having a framework available to simulate the behavior of the CUS and its systems, in particular, those based on teams, would allow users: to carry out a sizing of the aforementioned systems, so that they can be "calibrated" based on the area to be protected and on the possible threat (consisting of one or more m-drones), to simulate scenarios in which teams are used and evaluate the performances by the CUS and to develop and verify the procedures to be adopted for managing the threats.

Simulation can be used in different phases of the CUS development. The functional allocations could be supported by a modelling framework of the systems, where different architectural choices can be modelled, and by simulation and stressing or failure scenarios, through which it is possible to assess the architecture according to different aspects. Accordingly, looking also at the engineering guidelines on architectural assessment, CUS system architecture metrics could be identified and assessed by means of simulation. The architecture can be assessed with respect to its safety (for example to avoid bottle necks, or single points of failures), its efficiency and in terms of the coverage of the extension area or the coverage of different adversarial conditions.

The simulation can be used to build scenarios of attacks to verify the effectiveness of the CUS and also to assure its evolutive behavior. Attack-building can leverage on different techniques. The goal-based strategies aim to maximize the damages induced by the attacking drones to the critical infrastructure. In this way, the assessment from the CUS system of the threat scenarios can be verified and can be improved, assuring its continuous learning. Going deeper in the simulation chain, the attacking drones can be set up by using the generative adversarial networks (GAN), very promising techniques for image synthesis, in order to ensure proper data for the training of the employed artificial intelligence techniques

Finally, simulation can allow for the understanding of the proper human–machine balancing and the level of automation of the CUS system.

7. Discussion

For the purposes of this work, teams of mini drones have been considered as a reference subsystem of the hybrid CUS. This choice was due to several advantages in terms of mobility, coverage expansion, deployment flexibility, team coordination, automated decision-making, neutralization and scalability. The suitability of drone teams for CUS solutions was also confirmed by the analysis of the state-of-the-art research works in the fields of autonomous multi-agent systems and cooperative robotics. Moreover, some current international projects are developing both cooperative drone-based solutions for surveillance and situational awareness applications, as well as cooperative drone-based CUS.

In regard to the sensing phase, this work argues that the proximal sensing capability of a team of mini drones is the main clear advantage over a static ground-based CUS. Drone-based video sensing systems are less affected by the optical occlusion problem, but there is the need for an accurate video stabilization to mitigate the blur effect due to the drone movement. Moreover, drone teams represent an ideal solution to balance the pros

and cons of the different sensing technologies by means of a hybrid configuration of the team and data fusion techniques. The selection of the technologies that best complement each other is a useful activity in order to optimize the level of situational awareness with respect to the complexity and cost of the system, considering the specific requirements (i.e., range, accuracy, etc.) of the application.

In regard to the neutralization phase, the use of mini drones can help in maximizing the effectiveness or efficiency of some neutralization techniques. For example, RF jamming may exploit the mobility of a single drone to reduce the power necessary to disturb the signal under attack, or the mobility of multiples drones, which can be used in a cooperative way to increase the power of the resulting jamming signal. Moreover, a drone team can be used directly as a neutralization technique, or small projectiles could be installed on mini drones, offering a similar solution to the nets case. In any case, for some techniques, it must be taken into account that the target pointing required by the neutralization integrated in the defensive drones can be a challenging issue.

In regard to C2 systems, teams of drones are prone to automated decision-making capabilities according to the multilevel optimization principle. Based on the number of drones, a model based on "cooperative autonomous systems" can be applied, which is usually characterized by a collection of distinct decision-making entities for the decentralization of C2 operations.

In the end, the implementation of a cooperative drone-based CUS raises several technological challenges, in terms of team coordination, team communication network and team simulation framework. All these challenges are also related to the reworking of some of the techniques of detection, classification, tracking and mitigation systems, in order to maximize performance and effectiveness by exploiting the underlying coordination network of the team.

8. Conclusions

This paper focused on the concept of a multiplatform CUS, which consists of a team of mini drones acting as an autonomous and cooperative system. In order to evaluate the feasibility of this concept, the paper provided a systematic review of the main technological pillars: sensing, mitigation and command and control. The analysis has confirmed the effectiveness of the proposed system, while also highlighting the need for decentralization of command-and-control operations. Moreover, the paper discussed some key challenges in terms of team coordination, communication network and simulation framework.

Future work will regard the detailed design, the sizing and configuration of the cooperative drone-based architecture for a specific scenario (e.g., intrusion in critical infrastructures such airports) and preliminary implementation and testing of basic capabilities (coordinated detection of intrusions, cooperative tracking, etc.).

Author Contributions: Conceptualization, V.U.C., A.M., D.P. and G.G.; investigation, V.U.C. and A.M.; writing—original draft preparation, V.U.C. and A.M.; writing—review and editing, D.P. and G.G.; visualization, V.U.C., A.M., D.P. and G.G.; supervision, V.U.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the national project MATIM (Maturazione Tecnologie Innovative Mini e Micro Droni), with grant PRORA (Programma Nazionale di Ricerche Aerospaziali) DM662.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Federal Aviation Administration. Available online: https://www.faa.gov/uas/resources/uas-sightings-report/ (accessed on 10 October 2021).
2. CBNC. Available online: https://www.cnbc.com/2018/12/20/drone-sightings-shut-down-britains-gatwick-airport.html (accessed on 10 October 2021).
3. Hassanalian, M.; Abdelkefi, A. Classifications, applications, and design challenges of drones: A review. *Prog. Aerosp. Sci.* **2017**, *91*, 99–131. [CrossRef]
4. Nato Standardization Office (NSO). NATO Standard AJP-3.3. Allied Joint Doctrine for Air and Space Operations. Edition B Version 1. April 2016. Available online: https://www.japcc.org/wp-content/uploads/AJP-3.3-EDB-V1-E.pdf (accessed on 14 February 2022).
5. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors* **2020**, *20*, 3537. [CrossRef] [PubMed]
6. Lopez, J.; Royo, P.; Barrado, C.; Pastor, E. Modular avionics for seamless reconfigurable UAS missions. In Proceedings of the 2008 IEEE/AIAA 27th Digital Avionics Systems Conference, St. Paul, MN, USA, 26–30 October 2008; pp. 1.A.3-1–1.A.3-10. [CrossRef]
7. Beaudoin, L.; Gademer, A.; Avanthey, L.; Germain, V.; Vittori, V. Potential Threats of UAS Swarms and the Countermeasure's Need. In Proceedings of the European Conference on Information Warfare and Security (ECIW), Tallinn, Estonia, 7–8 July 2011; pp. 24–30.
8. Gigante, G.; Pascarella, D.; Luongo, S.; Di Benedetto, C.; Vozella, A.; Persechino, G. Game-theoretic approach for the optimal configuration computing of an interoperable fleet of unmanned vehicles. *Expert Syst.* **2018**, *35*, e12293. [CrossRef]
9. 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. [CrossRef]
10. Chamola, V.; Kotesh, P.; Agarwal, A.; Gupta, N.; Guizani, M. A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad Hoc Netw.* **2020**, *111*, 102324. [CrossRef] [PubMed]
11. Samaras, S.; Diamantidou, E.; Ataloglou, D.; Sakellariou, N.; Vafeiadis, A.; Magoulianitis, V.; Lalas, A.; Dimou, A.; Zarpalas, D.; Votis, K.; et al. Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review. *Sensors* **2019**, *19*, 4837. [CrossRef]
12. Wang, J.; Liu, Y.; Song, H. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 4–29. [CrossRef]
13. Seongjoon, P.; Hyeong, T.K.; Sanagmin, L.; Hyeontae, J.; Hwangnam, K. Survey on Anti-Drone Systems: Components, Designs, and Challenges. *IEEE Access* **2021**, *9*, 42635–42659.
14. Brust, M.R.; Danoy, G.; Stolfi, D.H.; Bouvry, P. Swarm-Based Counter UAV Defense System. *Discov. Internet Things* **2021**, *1*, 2. [CrossRef]
15. Dressel, L.; Kochenderfer, M.J. Hunting Drones with Other Drones: Tracking a Moving Radio Target. In Proceedings of the 2019 International Conference on Robotics and Automation (ICRA), Montreal, QC, Canada, 20–24 May 2019.
16. Brust, M.R.; Danoy, G.; Bouvry, P.; Gashi, D.; Pathak, H.; Goncalves, M.P. Defending against Intrusion of Malicious UAVs with Networked UAV Defense Swarms. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017.
17. Khan, A.; Rinner, B.; Cavallaro, A. Cooperative robots to observe moving targets. *IEEE Trans. Cybern.* **2016**, *48*, 187–198. [CrossRef]
18. Zhao, Y.; Wang, X.; Wang, C.; Cong, Y.; Shen, L. Systemic design of distributed multi-UAV cooperative decision-making for multi-target tracking. *Auton. Agents Multi-Agent Syst.* **2019**, *33*, 132–158. [CrossRef]
19. Sinha, A.; Tsourdos, A.; White, B. Multi UAV Coordination for Tracking the Dispersion of a Contaminant Cloud in an Urban Region. *Eur. J. Control* **2009**, *15*, 441–448. [CrossRef]
20. ResponDrone, Situational Awareness System for First Responders. Available online: https://respondroneproject.com/ (accessed on 13 February 2022).
21. ROBORDER. Available online: https://roborder.eu/ (accessed on 13 February 2022).
22. Labyrinth, Ensuring Drone Traffic Control and Safety. Available online: https://labyrinth2020.eu/ (accessed on 13 February 2022).
23. 5D-AeroSafe. Available online: https://5d-aerosafe.eu/ (accessed on 13 February 2022).
24. DRONES4SAFETY, Building a Cooperative, Autonomous, Operating Drone System to Enhance Transport Safety. Available online: https://drones4safety.eu/ (accessed on 13 February 2022).
25. RAPID, Risk-Aware Autonomous Port Inspection Drones. Available online: https://rapid2020.eu/ (accessed on 13 February 2022).
26. Pozniak, M.; Ranganathan, P. Counter UAS Solutions through UAV Swarm Environments. In Proceedings of the 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 20–22 May 2019; pp. 351–356. [CrossRef]
27. Pascarella, D.; Gigante, G.; Persechino, G.; Vozella, A. SWADAR (SWarm Advanced Detection and Tracking) Factsheet. 2020. Available online: https://www.edrmagazine.eu/wp-content/uploads/2020/12/EDA2020-Prize_SWADAR.pdf (accessed on 14 February 2022).
28. Keeping a Watchful Eye on Low-Flying Unmanned Aerial Systems in Cities. Available online: https://www.darpa.mil/news-events/2016-09-13 (accessed on 13 February 2022).
29. JEY-CUAS, Joint European System for Countering Unmanned Aerial Systems. Available online: https://ec.europa.eu/defence-industry-space/system/files/2021-06/EDIDP2020_factsheet_CUAS_JEY-CUAS.pdf (accessed on 13 February 2022).

30. Liu, Q.; He, M.; Xu, D.; Ding, N.; Wang, Y. A Mechanism for Recognizing and Suppressing the Emergent Behavior of UAV Swarm. *Math. Probl. Eng.* **2018**, *2018*, 6734923. [CrossRef]
31. Besada, J.A.; Campaña, I.; Carramiñana, D.; Bergesio, L.; de Miguel, G. Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management. *Sensors* **2022**, *22*, 189. [CrossRef]
32. Hoshiba, K.; Washizaki, K.; Wakabayashi, M.; Ishiki, T.; Kumon, M.; Bando, Y.; Gabriel, D.; Nakadai, K.; Okuno, H.G. Design of UAV-Embedded Microphone Array System for Sound Source Localization in Outdoor Environments. *Sensors* **2017**, *17*, 2535. [CrossRef]
33. Salvati, D.; Drioli, C.; Ferrin, G.; Foresti, G.L. Acoustic Source Localization from Multirotor UAVs. *IEEE Trans. Ind. Electron.* **2020**, *67*, 8618–8628. [CrossRef]
34. Guo, J.; Ahmad, I.; Chang, K. Classification, positioning, and tracking of drones by HMM using acoustic circular microphone array beamforming. *J. Wirel. Commun. Netw.* **2020**, *2020*, 9. [CrossRef]
35. Cabrera-Ponce, A.A.; Martinez-Carranza, J.; Rascon, C. Detection of Nearby UAVs Using a Multi-Microphone Array on Board a UAV. *Int. J. Micro Air Veh.* **2020**, *12*, 1756829320925748. [CrossRef]
36. Benyamin, M.; Goldman, G.H. *Acoustic Detection and Tracking of a Class I UAS with a Small Tetrahedral Microphone Array*; US Army Research Laboratory: Adelphi, MD, USA, 2014.
37. Chang, X.; Yang, C.; Wu, J.; Shi, X.; Shi, Z. A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays. In Proceedings of the 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), Sheffield, UK, 8–11 July 2018.
38. Busset, J.; Perrodin, F.; Wellig, P.; Ott, B.; Heutschi, K.; Rühl, T.; Nussbaumer, T. Detection and Tracking of Drones Using Advanced Acoustic Cameras. In *Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications*; SPIE: Bellingham, WA, USA, 2015; Volume 9647.
39. Sedunov, A.; Haddad, D.; Salloum, H.; Sutin, A.; Sedunov, N.; Yakubovskiy, A. Stevens Drone Detection Acoustic System and Experiments in Acoustics UAV Tracking. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019.
40. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques. In Proceedings of the 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2019.
41. Fu, H.; Abeywickrama, S.; Zhang, L.; Yuen, C. Low-Complexity Portable Passive Drone Surveillance via SDR-Based Signal Processing. *IEEE Commun. Mag.* **2018**, *56*, 112–118. [CrossRef]
42. Oliveira, M.T.; Miranda, R.K.; da Costa, J.P.C.L.; de Almeida, A.L.F.; de Sousa, R.T. Low Cost Antenna Array Based Drone Tracking Device for Outdoor Environments. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 5437908. [CrossRef]
43. Mototolea, D.; Stolk, C. Detection and Localization of Small Drones Using Commercial off-the Shelf Fpga Based Software Defined Radio Systems. In Proceedings of the 2018 International Conference on Communications (COMM), Bucharest, Romania, 14–16 June 2018; pp. 465–470.
44. Koohifar, F.; Guvenc, I.; Sichitiu, M.L. Autonomous Tracking of Intermittent RF Source Using a UAV Swarm. *IEEE Access* **2018**, *6*, 15884–15897. [CrossRef]
45. Azari, M.M.; Sallouha, H.; Chiumento, A.; Rajendran, S.; Vinogradov, E.; Pollin, S. Key Technologies and System Trade-Offs for Detection and Localization of Amateur Drones. *IEEE Commun. Mag.* **2018**, *56*, 51–57. [CrossRef]
46. Andraši, P.; Radišić, T.; Muštra, M.; Ivošević, J. Night-Time Detection of UAVs Using Thermal Infrared Camera. *Transp. Res. Procedia* **2017**, *28*, 183–190. [CrossRef]
47. Birch, G.C.; Woo, B.L. *Counter Unmanned Aerial Systems Testing: Evaluation of VIS SWIR MWIR and LWIR Passive Imagers*; Sandia National Lab. (SNL-NM): Albuquerque, NM, USA, 2017.
48. Goecks, V.G.; Woods, G.; Valasek, J. Combining Visible and Infrared Spectrum Imagery Using Machine Learning for Small Unmanned Aerial System Detection. In *Automatic Target Recognition XXX*; Overman, T.L., Hammoud, R.I., Mahalanobis, A., Eds.; SPIE: Bellingham, WA, USA, 2020.
49. Opromolla, R.; Fasano, G.; Accardo, D. A Vision-Based Approach to UAV Detection and Tracking in Cooperative Applications. *Sensors* **2018**, *18*, 3391. [CrossRef]
50. Li, J.; Ye, D.H.; Chung, T.; Kolsch, M.; Wachs, J.; Bouman, C. Multi-Target Detection and Tracking from a Single Camera in Unmanned Aerial Vehicles (UAVs). In Proceedings of the 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Daejeon, Korea, 9–14 October 2016.
51. Saqib, M.; Daud Khan, S.; Sharma, N.; Blumenstein, M. A study on detecting drones using deep convolutional neural networks. In Proceedings of the 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Lecce, Italy, 29 August–1 September 2017; pp. 1–5.
52. Nalamati, M.; Kapoor, A.; Saqib, M.; Sharma, N.; Blumenstein, M. Drone Detection in Long-Range Surveillance Videos. In Proceedings of the 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 18–21 September 2019; pp. 1–6.
53. Aker, C.; Kalkan, S. Using deep networks for drone detection. In Proceedings of the 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Lecce, Italy, 29 August–1 September 2017; pp. 1–6.
54. Kim, B.H.; Khan, D.; Bohak, C.; Choi, W.; Lee, H.J.; Kim, M.Y. V-RBNN Based Small Drone Detection in Augmented Datasets for 3D LADAR System. *Sensors* **2018**, *18*, 3825. [CrossRef]

55. Hammer, M.; Hebel, M.; Borgmann, B.; Laurenzis, M.; Arens, M. Potential of Lidar Sensors for the Detection of UAVs. In *Laser Radar Technology and Applications XXIII*; Turner, M.D., Kamerman, G.W., Eds.; SPIE: Bellingham, WA, USA, 2018.
56. Hammer, M.; Borgmann, B.; Hebel, M.; Arens, M. UAV Detection, Tracking, and Classification by Sensor Fusion of a 360° Lidar System and an Alignable Classification Sensor. In *Laser Radar Technology and Applications XXIV*; Turner, M.D., Kamerman, G.W., Eds.; SPIE: Bellingham, WA, USA, 2019.
57. Wei, P.; Cagle, L.; Reza, T.; Ball, J.; Gafford, J. LiDAR and Camera Detection Fusion in a Real-Time Industrial Multi-Sensor Collision Avoidance System. *Electronics* **2018**, *7*, 84. [CrossRef]
58. Zheng, L.; Zhang, P.; Tan, J.; Li, F. The Obstacle Detection Method of UAV Based on 2D Lidar. *IEEE Access* **2019**, *7*, 163437–163448. [CrossRef]
59. Chen, V.C.; Li, F.; Ho, S.S.; Wechsler, H. Analysis of Micro-Doppler Signatures. *IEE Proc.-Radar Sonar Navigat.* **2003**, *150*, 271–276. [CrossRef]
60. Drozdowicz, J.; Wielgo, M.; Samczynski, P.; Kulpa, K.; Krzonkalla, J.; Mordzonek, M.; Bryl, M.; Jakielaszek, Z. 35 GHz FMCW Drone Detection System. In Proceedings of the 2016 17th International Radar Symposium (IRS), Krakow, Poland, 10–12 May 2016.
61. Caris, M.; Johannes, W.; Stanko, S.; Pohl, N. Millimeter Wave Radar for Perimeter Surveillance and Detection of MAVs (Micro Aerial Vehicles). In Proceedings of the 2015 16th International Radar Symposium (IRS), Dresden, Germany, 24–26 June 2015.
62. Guvenc, I.; Ozdemir, O.; Yapici, Y.; Mehrpouyan, H.; Matolak, D. Detection, Localization, and Tracking of Unauthorized UAS and Jammers. In Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 17–21 September 2017.
63. Lazzari, F.; Buffi, A.; Nepa, P.; Lazzari, S. Numerical Investigation of an UWB Localization Technique for Unmanned Aerial Vehicles in Outdoor Scenarios. *IEEE Sens. J.* **2017**, *17*, 2896–2903. [CrossRef]
64. Oh, B.-S.; Guo, X.; Lin, Z. A UAV Classification System Based on FMCW Radar Micro-Doppler Signature Analysis. *Expert Syst. Appl.* **2019**, *132*, 239–255. [CrossRef]
65. Coluccia, A.; Parisi, G.; Fascista, A. Detection and Classification of Multirotor Drones in Radar Sensor Networks: A Review. *Sensors* **2020**, *20*, 4172. [CrossRef]
66. Molchanov, P.; Egiazarian, K.; Astola, J.; Harmanny, R.I.A.; Wit, J.J.M. Classification of Small UAVs and Birds by Mi-Cro-Doppler Signatures. In Proceedings of the 2013 European Radar Conference, Nuremberg, Germany, 9–11 October 2013; pp. 172–175.
67. Fioranelli, F.; Ritchie, M.; Griffiths, H.; Borrion, H. Classification of Loaded/Unloaded Micro-drones Using Multistatic Radar. *Electron. Lett.* **2015**, *51*, 1813–1815. [CrossRef]
68. Yasin, J.N.; Mohamed, S.A.S.; Haghbayan, M.-H.; Heikkonen, J.; Tenhunen, H.; Plosila, J. Unmanned Aerial Vehicles (UAVs): Collision Avoidance Systems and Approaches. *IEEE Access* **2020**, *8*, 105139–105155. [CrossRef]
69. Shi, X.; Yang, C.; Xie, W.; Liang, C.; Shi, Z.; Chen, J. Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. *IEEE Commun. Mag.* **2018**, *56*, 68–74. [CrossRef]
70. Luo, A. Drones Hijacking—Multi-Dimensional Attack Vectors and Countermeasures. In Proceedings of the DEFCON 24 Conference, Las Vegas, NV, USA, 4–7 August 2016; Available online: https://www.youtube.com/watch?v=R6RZ5KqSVcg (accessed on 28 February 2022).
71. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Cooperative jamming for wireless physical layer security. In Proceedings of the 2009 IEEE/SP 15th Workshop on Statistical Signal Processing, Cardiff, UK, 31 August–3 September 2009.
72. Li, K.; Voicu, R.C.; Kanhere, S.S.; Ni, W.; Tovar, E. Energy efficient legitimate wireless surveillance of UAV communications. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2283–2293. [CrossRef]
73. Lichtman, M.; Poston, J.D.; Amuru, S.; Shahriar, C.; Clancy, T.C.; Buehrer, R.M.; Reed, J.H. A communications jamming taxonomy. *IEEE Secur. Priv.* **2016**, *14*, 47–54. [CrossRef]
74. Junfei, Y.; Jingwen, L.; Bing, S.; Yuming, J. Barrage jamming detection and classification based on convolutional neural network for synthetic aperture radar. In Proceedings of the IGARSS 2018—2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, Spain, 22–27 July 2018; pp. 4583–4586.
75. Parlin, K.; Alam, M.M.; Le Moullec, Y. Jamming of UAV Remote Control Systems Using Software Defined Radio. In Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 22–23 May 2018.
76. Nguyen, D.; Sahin, C.; Shishkin, B.; Kandasamy, N.; Dandekar, K.R. A real-time and protocol-aware reactive jamming framework built on software-defined radios. In Proceedings of the 2014 ACM Workshop on Software Radio Implementation Forum, Chicago, IL, USA, 18 August 2014; pp. 15–22.
77. Karhima, T.; Silvennoinen, A.; Hall, M.; Haggman, S.-G. IEEE 802.11 b/g WLAN tolerance to jamming. In Proceedings of the Military Communications Conference, IEEE MILCOM 2004, Monterey, CA, USA, 31 October–3 November 2004; Volume 3, pp. 1364–1370.
78. DroneShield, DroneGun Tactical. Available online: https://www.droneshield.com/dronegun-tactical (accessed on 4 June 2021).
79. Blighter, AUDS Anti-UAV Defence System. Available online: https://www.blighter.com/products/auds-anti-uav-defence-system/ (accessed on 4 June 2021).
80. MCTECH, MC-HORIZON D360 v3 Battle Proven Reactive Anti-Drone/Quadcopter/Small UAV Jamming System. Available online: https://mctech-jammers.com/products/mc-horizon/mc-horizon-d360.html (accessed on 4 June 2021).

81. Mpitziopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A Survey on Jamming Attacks and Countermeasures in WSNs. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 42–56. [CrossRef]
82. Robinson, M. Knocking My Neighbors Kids Cruddy Drone Offline. DEF CON 23. Available online: https://academic.csuohio.edu/yuc/mobile/GPS-Knocking-My-Neighbors-Kid-Drone-compressed.pdf (accessed on 4 June 2021).
83. Ferreira, R.; Gaspar, J.; Sebstiao, P.; Souto, N. Effective GPS Jamming Techiniques for UAVs using Low Cost SDR Platforms. *Wirel. Pers. Commun.* **2020**, *115*, 2705–2727. [CrossRef]
84. Summers, N. Icarus Machine Can Commandeer a Drone Mid-Flight. October 2016. Available online: https://www.engadget.com/2016-10-28-icarus-hijack-dmsx-drones.html?guccounter=1 (accessed on 4 June 2021).
85. Moskvitch, K. Are Drones the Next Target for Hackers? 2014. Available online: https://www.bbc.com/future/article/20140206-candrones-be-hacked (accessed on 4 June 2021).
86. Noh, J.; Kwon, Y.; Son, Y.; Shin, H.; Kim, D.; Choi, J.; Kim, Y. Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Trans. Priv. Secur.* **2019**, *22*, 12:1–12:26. [CrossRef]
87. He, D.; Qiao, Y.; Chen, S.; Du, X.; Chen, W.; Zhu, S.; Guizani, M. A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles. *IEEE Netw.* **2018**, *33*, 146–151. [CrossRef]
88. Vervisch-Picois, A.; Samama, N.; Taillandier-Loize, T. Influence of GNSS spoofing on drone in automatic flight mode. In Proceedings of the ITSNT 2017: 4th International Symposium of Navigation and Timing, Toulouse, France, 14–17 November 2017; pp. 1–9.
89. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
90. Humphreys, T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1073–1090. [CrossRef]
91. Nassi, B.; Shabtai, A.; Masuoka, R.; Elovici, Y. SoK—Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. *arXiv* **2019**, arXiv:1903.05155.
92. Son, Y.; Shin, H.; Kim, D.; Park, Y.-S.; Noh, J.; Choi, K.; Choi, J.; Kim, Y. Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Security Symposium, Washington, DC, USA, 12–14 August 2015; pp. 881–896.
93. Davidson, D.; Wu, H.; Jellinek, R.; Singh, V.; Ristenpart, T. Controlling UAVs with sensor input spoofing attacks. In Proceedings of the WOOT 10th USENIX Conference on Offensive Technologies, Austin, TX, USA, 8–9 August 2016; pp. 221–231.
94. Hooper, M.; Tian, Y.; Zhou, R.; Cao, B.; Lauf, A.P.; Watkins, L.; Robinson, W.H. Securing commercial WiFi-based UAVs from common security attacks. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016.
95. Rodday, N. Hacking a professional drone. In Proceedings of the Black Hat ASIA 2016, Singapore, 29 March–1 April 2016.
96. Highnam, K.; Angstadt, K.; Leach, K.; Weimer, W.; Paulos, A.; Hurley, P. An uncrewed aerial vehicle attack scenario and trustworthy repair architecture. In Proceedings of the 46th Annual IEEE/IFIP, International Conference on Dependable Systems and Networks Workshop (DSN-W), Toulouse, France, 28 June–1 July 2016; pp. 222–225.
97. Shoufan, A. Continuous authentication of UAV flight command data using behaviometrics. In Proceedings of the 2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Abu Dhabi, United Arab Emirates, 23–25 October 2017; pp. 1–6.
98. Raytheon, Phaser High-Power Microwave System. Available online: https://www.raytheonmissilesanddefense.com/capabilities/products/phaser-high-power-microwave (accessed on 4 June 2021).
99. Boeing, Laser-Focused Battlefield Defense. Available online: https://www.boeing.com/defense/missile-defense/directed-energy/index.page (accessed on 4 June 2021).
100. CDET, RAM UAV Combat Unmanned Aerial System. Available online: https://ramuav.com/ (accessed on 4 June 2021).
101. Drone Defence, NetGun X1—Short Range Drone Protection. Available online: https://www.dronedefence.co.uk/netgun-x1/ (accessed on 4 June 2021).
102. Delft Dynamics, Dronecatcher. Available online: https://dronecatcher.nl/ (accessed on 4 June 2021).
103. Lee, C.U.; Noh, G.; Ahn, B.; Yu, J.; Lee, H.L. Tilted-Beam Switched Array Antenna for UAV Mounted Radar Applications with 360° Coverage. *Electronics* **2019**, *8*, 1240. [CrossRef]
104. Papaioannou, S.; Kolios, P.; Panayiotou, C.G.; Polycarpou, M.M. Cooperative Simultaneous Tracking and Jamming for Disabling a Rogue Drone. In Proceedings of the 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Las Vegas, NV, USA, 24 October–24 January 2021.
105. Ghallab, M.; Nau, D.; Traverso, P. *Automated Planning—Theory and Practice*; Morgan Kaufmann Publishers: San Francisco, CA, USA, 2004.
106. National Institute of Standards and Technology. *Autonomy Levels for Unmanned Systems (ALFUS) Framework*; NIST Special Publication 1011-I-2.0; Terminology Version 2.0; NIST: Gaithersburg, MD, USA, 2008; Volume I.
107. Kolitz, S.E.; Beaton, R.M. Overall System Concepts in Mission Planning. In *New Advances in Mission Planning and Rehearsal Systems*; AGARD Lecture Series; AGARD: Neuilly Sur Seine, France, 1993; Volume 192.
108. Wooldridge, M.J. *An Introduction to MultiAgent Systems*, 2nd ed.; John Wiley & Sons Ltd.: Chichester, UK, 2009.
109. Jennings, N.R. Coordination Techniques for Distributed Artificial Intelligence. In *Foundations of Distributed Artificial Intelligence*; O'Hare, G.M.P., Jennings, N.R., Eds.; John Wiley & Sons Ltd.: New York, NY, USA, 2000; pp. 187–210.

110. Nigam, N. The multiple unmanned air vehicle persistent surveillance problem: A review. *Machines* **2014**, *2*, 13–72. [CrossRef]
111. Noor, F.; Khan, M.A.; Al-Zahrani, A.; Ullah, I.; Al-Dhlan, K.A. A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. *Drones* **2020**, *4*, 65. [CrossRef]
112. Oubbati, O.S.; Atiquzzaman, M.; Lorenz, P.; Tareque, H.; Hossain, S. Routing in Flying Ad Hoc Networks: Survey, Constraints, and Future Challenge Perspectives. *IEEE Access* **2017**, *7*, 81057–81105. [CrossRef]