SoK: Security and Privacy in the Age of Commercial Drones

Ben Nassi[1], Ron Bitton[1], Ryusuke Masuoka[2], Asaf Shabtai[1], Yuval Elovici[1]

{nassib,ronbit}@post.bgu.ac.il, masuoka.ryusuke@jp.fujitsu.com,{shabtaia,elovici}@bgu.ac.il
[1]Software and Information Systems Engineering, Ben-Gurion University of the Negev,
[2]Fujitsu System Integration Laboratories

Abstract

As the number of drones increases and the era in which they begin to fill the skies approaches, an important question needs to be answered: From a security and privacy perspective, are society and drones really prepared to handle the challenges that a large volume of flights will create? In this paper, we investigate security and privacy in the age of commercial drones. First, we focus on the research question: Are drones and their ecosystems protected against attacks performed by malicious entities? We list a drone's targets, present a methodology for reviewing attack and countermeasure methods, perform a comprehensive review, analyze scientific gaps, present conclusions, and discuss future research directions. Then, we focus on the research question: Is society protected against attacks conducted using drones? We list targets within society, profile the adversaries, review threats, present a methodology for reviewing countermeasures, perform a comprehensive review, analyze scientific gaps, present conclusions, and discuss future research directions. Finally, we focus on the primary research question: From the security and privacy perspective, are society and drones prepared to take their relationship one step further? Our analysis reveals that the technological means required to protect drones and society from one another has not yet been developed, and there is a tradeoff between the security and privacy of drones and that of society. That is, the level of security and privacy cannot be optimized concurrently for both entities, because the security and privacy of drones cannot be optimized without decreasing the security and privacy of society, and vice versa.

I. Introduction

Drone technology has advanced significantly in recent years, permitting individuals and businesses to adopt drones for a variety of purposes. Currently, studies are being performed around the world to evaluate the effectiveness of using drones as an alternative means of delivering organs, emergency healthcare, food, and other goods [1–3]. In addition, legislation and regulations are evolving to allow drones to fly in populated areas for commercial use [4]. Although it seems that the day in which drones will fill the skies is about to arrive, a primary research question remains to be answered: From the security and privacy perspective, are society and drones really prepared to take their relationship one step further?

In recent years, the issue of security and privacy of drones and society has received increased attention by various sectors. Within the academic community, in the last five years, drone related research has been presented at top security conferences [5–9]. Drones have been used as weapons in various incidents that received extensive media coverage [10–12], and the volume of such incidents will likely increase significantly with the expected growth in drone shipments in the coming years [13] and the new regulations adopted by many countries which allow drones to fly over populated areas [2]. This new reality has led to increased interest by industry for security mechanisms for both drones and society, a market expected to reach $1.85 billion by 2024 [14]. However, despite all of the efforts that have already been invested in this area, a primary unanswered research question remains: Has the technology that is needed to both support the upcoming age of commercial drones and protect drones and society from one another matured enough to handle the challenges that a large volume of flights will create? Two secondary research questions must be answered in order to answer the primary research question: (1) Are drones and their ecosystems protected against attacks performed by malicious entities? (2) Is society protected against attacks conducted using drones? In order to answer the two secondary questions, a comprehensive analysis that covers the perspectives of each entity is required.

In this paper, we investigate security and privacy in the age of commercial drones. In the first part of the paper (Section II), we address the research question: Are drones and their ecosystems protected against attacks performed by malicious entities? We list a drone's targets, present a methodology for reviewing attack and countermeasure methods, perform a comprehensive review, analyze scientific gaps, present conclusions, and discuss future research directions. In the second part (Section III) of the paper, we address the research question: Is society protected against attacks conducted using drones? We list targets within society, profile the adversaries, review threats, present a methodology for reviewing countermeasures, perform a comprehensive review, analyze scientific gaps, present conclusions, and discuss future research directions. In the third part of the paper (Section IV), we address the primary research question: From the security and privacy perspective, are society and drones prepared to take their relationship one step further? We answer this question based on the analysis performed in the first two parts of the paper.

While other drone related SoKs have been published [15–19], they suffer from two main limitations: (1) Existing SoKs are narrow in scope, focusing on only a specific entity (drones [15] or society [16–19]), or covering just one sector (the scientific [15–17] or industrial [18, 19] sector); and (2) Previously performed SoKs lack a systematic approach for structuring existing knowledge on drones and society [15–19]. As a result, the conclusions made in previous SoKs do not answer the primary research question presented in this paper and do not point out the scientific gaps that should be addressed in order to support the upcoming age of commercial drones and protect drones and society from one another.

In this SoK we address the abovementioned limitations by (1) performing a comprehensive analysis that covers multiple sectors (academia, industry, the media) and explore security and privacy from two perspectives: securing a drone's ecosystem from hostile entities and securing society from attacks conducted using drones; and (2) developing a methodology and defining assessment criteria for reviewing and structuring the existing knowledge with respect to the two secondary research questions. Specifically, for each entity (i.e., drones and society), we list the targets, profile the adversaries, analyze the primary threats/attacks, and explore countermeasure methods. Addressing these limitations allows us to make a holistic observation on security and privacy in the age of drones and point out scientific gaps that must be addressed in order to protect drones and society from one another. We conclude that: (1) the technological means required to protect drones and society from one another has not yet been developed; and (2) there is a tradeoff between the security and privacy of drones and that of society. That is, the level of security and privacy cannot be optimized concurrently for both entities, because the security and privacy of drones cannot be optimized without decreasing the security and privacy of society, and vice versa.

This paper focuses on the new security and privacy challenges that commercial drones (micro, mini, and small drones) have created given their increasing use by individuals, local authorities, law enforcement, the media, and industry and new regulations that allow commercial drones to fly in populated areas (at altitudes lower than 150 meters). Non-commercial drones (small, tactical, and strike drones) are outside the scope of this paper, since they are mainly used by militaries and governments, are not sold to civilians, are not allowed to fly at altitudes below 150 meters, and haven't created any new challenges in the last decade. Furthermore, this paper focuses only on the technological means required to protect drones and society from one another. Non-technological means, such as legislation and regulations, are beyond the scope of this paper.

II. Securing Drones From Society

In this section, we focus on the following research question: Are drones and their ecosystems protected against attacks performed by malicious entities? We start by listing a drone's targets (Section II-A). We present a methodology for reviewing attacks, which is followed by a review (Section II-B); we also present a methodology for reviewing countermeasures, which is followed by a review (Section II-C). Finally, we analyze scientific gaps, present our conclusions, and discuss future research directions (Section II-D).

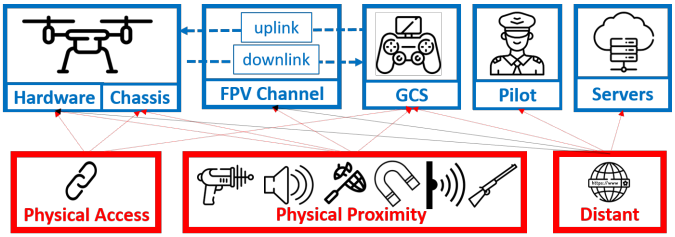

Fig. 1. Red arrows indicate existing attack implementations, black arrows indicate implementations that we expect to see in the future, and the absence of an arrow indicates that attacks cannot be implemented.

A. Target Identification & Adversary Profile

Commercial drones (micro, mini, and small drones) are aerial vehicles that fly remotely, do not carry a human operator, and can carry payload [20]. A drone's ecosystem is comprised of six unique targets (see Fig. 1):

(i) Drone hardware: This target includes a drone's CPU, sensors (e.g., gyroscope, GPS), and firmware.

(ii) Drone chassis and package: This target includes a drone's non-electronic devices (e.g., propellers) and cargo.

(iii) Ground control station (GCS): The GCS is a land-based control system that provides facilities for the pilot to control the drone. Most commercial drones are controlled via a portable GCS, which consists of a dedicated controller and a smartphone. The smartphone is equipped with a dedicated mobile application that provides telemetry (video stream, GPS location, etc.) to the pilot.

(iv) First-person view (FPV) channel: The FPV channel is the radio communication channel between the drone and the GCS. The FPV channel enables the pilot to fly the drone as if he/she was on board and consists of a downlink (used for video streaming) and an uplink (used for controlling the drone via the GCS). Implementation of FPV channels consists of common communication protocols (e.g., Wi-Fi, cellular, and XBee [21]) and proprietary protocols (e.g., OcuSync).

(v) Pilot: This target consists of the person operating the drone and his/her privacy.

(vi) Cloud services: Most drones are not connected directly to the Internet, however the GCS that runs a drone's application is connected to the Internet, and the telemetry of flights is sent to cloud servers for storage and analysis.

In this section, we consider an attacker a civilian with a malicious intention to disrupt the legitimate task of a flying drone (e.g., kidney delivery [1]) in order to cause damage (e.g., compromising a patient's health). The capabilities and weapons that a malicious civilian could possess include any type of equipment that can be legally purchased with a medium-sized budget (i.e., a few thousand dollars) at a store or online, such as: software-defined radio (SDR), a computer, a commercial laser, etc. We consider cannons (laser and radio) and predator birds weapons that the typical civilian cannot obtain, and they are not within the scope of this section.

B. Review of Attack Methods

Here we review attack methods against a drone's ecosystem. We start by describing the criteria used to evaluate attacks

(Section II-B1) and then review and analyze related attacks (Sections II-B2 - II-B6) according to the criteria.

1) Methodology

The following criteria (i-iv) are assessed when reviewing an attack. For some of the evaluated criteria the following marks are used to indicate that a method fully (denoted as ●) or partially (denoted as ◐) satisfies, or does not (denoted as ○) satisfy the criteria.

(i) *Adversary models/operational range (OR1-5)*: We consider three types of adversaries (see Fig. 1) and five operational range (OR1-5) levels that define the distance between the attacker and the target drone. (a) An adversary with direct physical access (OR1): an attacker that has direct physical access to the drone or GCS. This attacker can, for instance, modify the firmware of the GCS or replace the drone's hardware. (b) A physically proximate adversary: an adversary that is within the physical range of the drone or GCS. This includes the acoustic/magnetic range (close proximity - OR2, up to 50 meters), optical range (medium proximity - OR3, up to 500 meters), and radio range (radio proximity - OR4, up to five kilometers with dedicated amplifiers). Such an adversary can send, modify, and replay radio transmissions in order to hijack a drone. In addition, the attacker can disrupt radio transmissions or apply sensor spoofing attacks. (c) A distant adversary (OR5, more than five kilometers): an adversary that resides on the Internet and applies attacks against servers, drones, the GCS, or the FPV channel.

(ii) *Impact (C/I/A)*: We map each attack according to the methodology presented in [22], which explores the impact of an attack on a drone's ecosystem with respect to the three common security principles: *Confidentiality Impact (C)* - any type of attack method that reveals information about the pilot, drone, FPV channel, or telemetry data of the flight. *Integrity Impact (I)* - any type of method that causes the modification of information obtained by the drone, GCS, cloud servers, or pilot. *Availability Impact (A)* - any type of method that causes the pilot to lose control of the drone as a result of a forced landing, crash, or hijacking.

(iii) *High exposure level (●/◐/○)*: This criteria indicates the attack's exposure level, in terms of the amount of drones/users that are affected by the attack. The attack affects: (●) - all drone types; (◐) - a wide range of drones manufactured by different manufacturers (e.g., a vulnerability that is shared by all Wi-Fi FPV drones); or (○) - a specific manufacturer's drones/users (e.g., DJI's drones/users).

(iv) *Low complexity (●/◐/○)*: This criteria concerns the complexity of the attack. The success of the attack: (●) - does not depend on any environmental conditions; (◐) - relies on a preliminary step (e.g., compromising hardware/software); or (○) - depends on environmental conditions that are beyond the attacker's control (e.g., flight altitude, indoor environment).

The attacks are reviewed as follows: they are first categorized by the six targets they compromise (servers and pilots are analyzed together) in Sections II-B2 - II-B6 and are then subcategorized by adversary model (i-iii). For each of the categories, we review related attacks and analyze them according to the abovementioned criteria. The impact criterion is indicated by (A) for availability, (I) for integrity, and (C) for confidentiality. Throughout the review, a criterion is indicated in the text only if the reviewed attack partially satisfies (◐) or fails to satisfy (○) the criterion (otherwise the attack is considered as fully satisfying the criterion). The operational range criterion is analyzed in Table I which summarizes the attacks reviewed.

2) Attacks against drone hardware

(i) Attacks that require direct physical access: *Sasi et al.* [23] identified a vulnerability in the Parrot AR.Drone: No validation of firmware signature. This allowed them demonstrate a supply chain attack against drones by installing compromised firmware that causes the drone to crash by shutting it down during flight (impact - A,I). This attack can be applied to Parrot drones (exposure level - ○) using an infected website or by performing a supply chain attack (low complexity - ◐).

(ii) Attacks that require maintaining physical proximity: Attacks on the stabilizing algorithm via the camera sensor: *Davidson et al.* [24] identified a vulnerability in the stabilizing algorithm of the Parrot AR.Drone 2 which allows an attacker to hijack the drone using a commercial laser (impact - I,A). They directed a laser at the surface of a flying drone, causing the stabilizing algorithm (which is based on detecting movement changes from a downward camera directed at the surface) to follow the laser. This attack can only be applied to Parrot drones (exposure level - ○) that fly a few meters from the ground (low complexity - ○).

Attacks on the gyroscope sensor and compass: A known vulnerability in MEMS gyroscopes (related to the physical characteristics of their structure) is their sensitivity to high amplitude acoustic noise at the resonant frequency, which causes the gyroscope to produce extreme values. *Son et al.* [5] used a directional speaker to exploit this vulnerability by producing an ultrasound signal that forced the drone to land (impact - I,A). This attack can only be applied in indoor environments, since sound deteriorates with distance (low complexity - ○). *Robinson et al.* [25] found that the compass of the DJI Phantom 3 is sensitive to the presence of magnetic fields, a scenario which necessitates its recalibration and prevents takeoff (impact - I,A). This attack can only be applied to DJI drones (exposure level - ○) in outdoor environments (low complexity - ○).

GPS spoofing: These attacks can be applied using an SDR and exploit a known vulnerability in the GPS protocol: Lack of authentication and encryption. *Luo et al.* [26] showed that GPS spoofing of no-flight areas during a manual flight operated by a pilot triggers the drone's safety mechanism, forcing it to land immediately (impact - I,A). *He et al.* [27] showed that GPS spoofing of any coordinate during an autonomous navigation task (e.g., Return to Home) causes the drone to fly to unintended locations (impact - I,A).

GPS jamming: These attacks can be applied using an SDR, and they disrupt radio transmissions used by the GPS protocol by decreasing the SNR. *Farlik et al.* [28] showed that applying GPS jamming to drones prevents any autonomous flight functionality from working (e.g., Return to Home).

(iii) Attacks applied from a distance: Attacks in this cate-

gory target a drone's hardware/firmware and are applied over the Internet. Currently, such attacks cannot be implemented, because drones are connected indirectly to the Internet via the GCS. We expect such attacks in the near future, with the integration of eSIM in the next generation of drones [29].

3) Attacks against the drone chassis

(i) Attacks that require direct physical access: *Belikovetsky et al.* [30] demonstrated a supply chain attack against a drone using a 3D printed propeller that was produced from a compromised computer-aided design (CAD) file. The 3D printed propeller was visually identical to a genuine propeller but caused the drone to crash upon takeoff (impact - A,I). This attack can be applied using an infected website or by performing a supply chain attack (low complexity - ◐).

(ii) Attacks that require maintaining physical proximity:

Nets: Several companies utilize nets to disable and crash drones. Such nets are connected to defensive drones that swoop and swag the hostile drones or fire a shot from the air (using a defensive drone) [31] or the ground (using a gun) [32]. The net stops the propellers from turning and causes the drone to fall and crash to the ground.

Bullets: Guns are also effective and can cause drones flying at low altitudes to crash.

These attacks target drone availability (impact - A). The range between the attacker and the target drone can be extended from low ranges (OR3) to high ranges (OR4) by using a dedicated drone to shoot the nets and a sniper gun (which can be purchased legally in several countries).

(iii) Attacks applied from a distance: Such attacks cannot be implemented against the drone chassis.

4) Attacks against the GCS

(i) Attacks that require direct physical access: *Luo et al.* [26] reversed engineered DJI's official Android application and found a hard-coded authentication token that is used to authenticate the application to the DJI server prior to takeoff. They used the token to authenticate an application that they created to fly a drone (impact - I). This attack can only be applied to DJI drones (exposure level - ○) prior to takeoff (low complexity - ○).

(ii) Attacks that require maintaining physical proximity: While several attacks in this category also affect the GCS, they are primarily directed at other targets, with the GCS being the secondary target affected (e.g., FPV channel jamming targets the FPV channel but affects the GCS as well). These attacks are reviewed according to the primary affected target.

(iii) Attacks applied from a distance: Attacks in this category target the GCS and are applied over the Internet. A GCS that is compromised with malware that is controlled over the Internet can be exploited by attackers to video stream from the GCS to attackers or to remotely control the drone. Surprisingly, although this type of attack can be implemented (because the GCS is connected to the Internet), such attacks has not yet been demonstrated.

5) Attacks against the FPV channel

(i) Attacks that require direct physical access: Such attacks cannot be implemented against the wireless FPV channel.

(ii) Attacks that require maintaining physical proximity: Attacks in this category require the attacker to be within radio range of the attacked drone and are implemented using a radio transducer (e.g., SDR, network interface card).

Attacks on Wi-Fi FPV channels: A fundamental vulnerability exploited in this attack category is the use of open Wi-Fi networks for the FPV channel, which allows an attacker to connect to the local area network (LAN) shared by the drone and its GCS. Several studies [25, 33–35] identified various vulnerabilities that can be exploited if the attacker manages to connect to this LAN. *Robinson et al.* [25] identified a vulnerability in the drone's operating system: Lack of authentication in the FTP folder that stores captured images and videos. This allows an attacker to read files from the FTP folder (impact - C). *Kamkar et al.* [33] exploited the deauthentication frame used in the IEEE 802.11 Wi-Fi protocol to forcefully disconnect the pilot from the network, thus enabling an attacker to hijack the drone (impact - A). *Deligne et al.* [34] exploited the known SYN flood vulnerability and showed how this causes the drone to go out of control and crash (impact - A). *Cabrera et al.* [35] identified two different vulnerabilities in the drone's operating system: (1) The drone's firmware supports the unsecured Telnet protocol; this allows an attacker to kill the drone's main process and crash the drone (impact - A), and (2) There is a lack of authentication of messages sent between the GCS and the drone; this allows an unauthenticated attacker to send protocol messages to take pictures (impact - C), disable the video stream (impact - I,A), and hijack the drone (impact - A).

Nassi et al. [9] demonstrated a side-channel attack on a drone's Wi-Fi network, showing that it is possible to determine whether a specific point of interest (POI) is being video streamed by a drone (impact - C). This attack, which is not limited to open Wi-Fi networks, exploits the variable bitrate mechanism in the H264 video compression algorithm and relies on data extracted from the data link layer (which can be extracted from Wi-Fi communication by any party, using a packet sniffer, even if the party is not connected to the network). This method utilizes a flickering LED installed on a POI to watermark the bitrate of the (uplink) communication; the watermark indicates that the POI is captured by the drone's camera. The abovementioned attacks [9, 25, 33–35] can be applied to Wi-Fi FPV drones (exposure level - ◐).

Attacks on XBee FPV channels: *Rodday et al.* [36] showed that the XBee 868LP protocol, as implemented in professional drones (used by police departments), lacks authentication and encryption. By exploiting these vulnerabilities, they implemented an MITM attack, analyzed the FPV channel's uplink, and demonstrated that they can remotely control a drone by sending protocol messages (impact - C,A). This attack is limited to drones that use the XBee protocol for the FPV channel (exposure level - ◐).

FPV channel jamming: *Multerer et al.* [37] applied radio jamming via SDR against a drone's downlink and showed that the FPV functionality was disabled in the GCS, preventing the pilot from maneuvering the drone and leaving the drone vulnerable to collisions during flight (impact - I,A).

(iii) Attacks applied from a distance: This type of attack

includes interception/blocking of the FPV channel transmitted via cellular cells. Such attacks cannot be implemented at this time, because cellular protocols are not used for the FPV channel in the current drone generation. We expect such attacks in the near future, with the integration of eSIM in the next generation of drones [29].

6) Attacks against pilots & servers

(i) Attacks that require direct physical access or maintaining physical proximity: This type of attack includes disabling the pilot, supply chain attacks against drone servers, etc. This type of attack is outside the scope of this paper due to the nature and novelty of such attacks with respect to drones.

(ii) Attacks applied from a distance: Attacks in this category target data stored in cloud services, which contains private information about the pilots and flights. *Cabrera et al.* [35] identified a vulnerability in Parrot's cloud servers: Lack of authentication in several APIs; this allows an unauthenticated attacker to obtain information regarding flights in a specific area. The authors also showed that this information can be used to deanonymize pilots and locate their home addresses (impact - C). *Check Point Research* [38] identified a stored XSS vulnerability in the DJI Forum, which allows a remote attacker to obtain the credentials of users who logged into the DJI Forum and click a malicious link (low complexity - ◐). By using the credentials, the attacker can access a user's DJI account and obtain flight logs, photos and videos, and profile information (impact - C). Both attacks [35, 38] are the result of poor security implementation by the manufacturer, and they only affect a manufacturer's users (exposure level - ○).

C. Review of Countermeasure Methods

Here we review countermeasure methods used to protect a drone's ecosystem. We start by describing the criteria used to evaluate countermeasures (Section II-C1) and then review and analyze related methods (Sections II-C2 - II-C5) according to the criteria.

1) Methodology

Based on the ontology presented in [49], we defined eight countermeasure method assessment criteria that are related to three categories: (1) robustness and maturity, which evaluates a method's effectiveness, type, and technological readiness level (criteria i-iii); (2) usability, which evaluates the method's ease of use (criteria iv-v); and (3) deployability, which evaluates a method's ease of installation, deployment, and operation (criteria vi-vii). For some of the criteria evaluated the following symbols are used to indicate whether a method fully satisfies (denoted as ●), partially satisfies (denoted as ◐), or does not satisfy (denoted as ○) a criterion.

(i) *Type of Security (P/M/Dt/Re).* We categorize the countermeasures based on the type of protection: *Prevention (P)* - methods used to avoid or prevent the threat; *Mitigation (M)* - methods used to reduce the likelihood of exploiting the vulnerability; *Detection (Dt)* - methods used to identify exploitation of the vulnerability; and *Response (Re)* - methods used to reduce the impact after an incident has occurred.

(ii) *High Effectiveness (●/◐/○).* The attacker: (●) - cannot evade the countermeasure; (◐) - can evade the countermeasure without making improvements to his/her capabilities (e.g., a result of false negatives); (○) - can evade the countermeasure by making improvements to his/her capabilities (e.g., using a stronger radio transmitter).

(iii) *Technological Readiness Level (TRL 1-9).* Based on European Union standards [50], we estimate technological maturity according to a nine-point scale as follows: (1) - basic principles observed; (2) - technological concept formulated; (3) - experimental proof of concept; (4) - technology validated in lab; (5) - technology validated in relevant environment; (6) - technology demonstrated in relevant environment; (7) - system prototype demonstration; (8) - system complete and validated; (9) - actual system proven in operational environment.

(iv) *Negligible Effort by the User/Pilot (●/◐/○).* The countermeasure's operation requires: (●) - no additional effort from the user/pilot; (◐) - additional negligible/one-time effort from the user/pilot (e.g., the use of a strong password to protect the FPV channel); (○) - additional non-negligible/repeated effort from the user/pilot (e.g., a two-factor authentication log in).

(v) *Negligible Impact on the Drone's Usability (●/◐/○).* The countermeasure's operation: (●) - has no impact on the drone's usability; (◐) - has negligible impact on the drone's usability (e.g., a tolerable number of false alerts); (○) - has non-negligible impact on the drone's usability (e.g., a dramatic decrease in the resolution of the FPV channel).

(vi) *Negligible Maintenance Required (●/○).* The countermeasure requires: (●) - no/negligible maintenance (e.g., using digital signatures); (○) - continuous maintenance (e.g., model updating).

(vii) *Negligible Resource Overhead (●/○).* The countermeasure adds: (●) - no/negligible overhead to resources (e.g., uses encryption); (○) - heavy overhead to resources (e.g., a model which continuously runs in the background);

(viii) *Negligible Changes to Infrastructure (●/◐/○).* The countermeasure requires: (●) - simple configuration updates; (◐) - major software updates (e.g., developing new protocol/-software modules); (○) - improved hardware components.

The countermeasures are reviewed as follows: they are first categorized according to the security principles they are aimed at optimizing (authentication, integrity, confidentiality, or recovery) in Sections II-C2 - II-C5, and are then subcategorized by the related methods. We review countermeasure methods and analyze them according to the abovementioned criteria. The security type is indicated by (P) for prevention, (M) for mitigation, (Dt) for detection, and (Re) for response. Throughout this review, a specific criterion is mentioned in the text only if the countermeasure partially satisfies (◐) or fails to satisfy (○) the criterion (otherwise the countermeasure is considered as fully satisfying the criterion). The technological readiness level criterion is analyzed exclusively in Table I which summarizes the countermeasures reviewed.

2) Countermeasures aimed at optimizing authentication:

The identity of users, pilots, and manufacturers must be authenticated by any target in a drone's ecosystem:

(i) Digital signatures: Any file installed/used by a drone's

TABLE I
SECURING DRONES: SUMMARY OF ATTACK AND COUNTERMEASURE METHODS.
FULLY SATISFIES (●), PARTIALLY SATISFIES (◐), DOES NOT (○) SATISFY THE CRITERION. NEG. = NEGLIGIBLE, INFRA. = INFRASTRUCTURE, AUTH. = AUTHENTICATION.

Attacks								Countermeasures								
		Properties			Impact				Robust		Deployment				Usability	
Target Asset	Method	Operational Range	High Exposure Level	Low Complexity	Availability	Integrity	Confidentiality	Method	Security Type	High Effectiveness	TRL	Neg. Maintenance	Neg. Resource Overhead	Neg. Changes to Infra.	Neg. Effort for User	Neg. Impact on Drone
Hardware	Installing Fake Firmware [23]	1	○	◐	✓	✓		Digital Signature	P	●	9	●	●	●	●	●
	Camera Spoofing [24]	3	○	○	✓	✓		Random Sample Consensus [39]	M	◐	4	●	○	◐	●	●
	GPS Spoofing [26, 27]	4	●	●	✓	✓		Verification with Compass [40]	D	◐	3	○	○	◐	○	◐
								Verification with Gyroscope [41]	D	◐	4	○	○	◐	●	◐
								Verification with Nearby Drone [8]	D	●	4	●	○	◐	●	●
								Video-Based Navigation [42]	P	●	2	●	○	◐	●	●
								Multi-Constellation Receiver	M	○	9	●	●	○	●	●
	GPS Jamming [28]	4	●	●	✓	✓		Null Steering	M	◐	9	●	●	○	●	●
	Gyroscope Spoofing [5]	2	●	○	✓	✓		Anomaly Detection [7]	D	◐	6	○	○	◐	●	◐
	Compass Spoofing[25]	2	○	○	✓	✓		Rule-Based Detection [43]	D	◐	3	○	○	◐	●	◐
Chassis	Fake CAD File [30]	1	●	◐	✓	✓		Digital Signature	P	●	9	●	●	●	●	●
	Nets [31, 32]	3/4	●	●	✓			Parachute [44, 45]	Re	●	9	●	●	○	●	●
	Bullets			●	✓											
FPV Channel	Deauthentication [33]	4	◐	●	✓			Encrypted Network Protocol	P	●	9	●	●	●	●	●
	Flooding NIC [34]	4	◐	●	✓											
	Taking & Downloading Videos & Pictures [25, 35]	4	◐	●			✓									
	Killing Main Process [35]	4	◐	●	✓											
	FPV Jamming [37]	4	●	●	✓	✓		Channel Hopping/DSSS [46]	M	◐	9	●	●	○	●	●
	Detecting Captured POI [9]	4	◐	●			✓	Constant Bitrate Video Encoders	P	●	9	●	●	●	●	○
								Proprietary Protocol for FPV	M	◐	9	●	●	◐	●	●
	Remote Control [35, 36]	4	◐	●	✓	✓		Encrypted Network Protocol	P	●	9	●	●	●	●	●
								Continuous Pilot Auth. [47, 48]	D	◐	4	○	○	◐	●	◐
GCS	Reverse Engineering GCS's Application [26]	1	○	○	✓		✓	Obfuscation, Packers	M	◐	9	●	●	●	●	●
Servers	Deanonymizing Pilots [35]	5	○	●			✓	Authorization	P	●	9	●	●	●	●	●
	Extracting Flight History [35, 38]	5	○	●			✓	Two-Factor Auth.	P	●	9	●	●	◐	○	●

ecosystem must be signed by its manufacturer so it can be verified by the ecosystem (type - P); this will prevent attacks that rely on fake files [23, 30].

(ii) Two-factor authentication: Two-factor authentication must be deployed for any sign-in process (e.g., to authenticate users signing into Web servers) (type - P); this requires software changes (negligible changes to infrastructure - ◐) and affects the sign-in process (negligible effort by user - ○). This will prevent attacks that exploit vulnerabilities in the login mechanism of cloud-based services [35, 38].

(iii) Continuous authentication: The identity of a drone's operator must continuously be authenticated by the drone. This can be done with methods that utilize data obtained from motion sensors [47] and maneuvering commands [48], to derive a unique profile for the pilot during flights. This profile is used to continuously authenticate the pilot on board (type - Dt). The main shortcomings of these methods are as follows: false negative and positive errors (high effectiveness - ◐, negligible impact on the drone's usability - ◐) and the need to develop and maintain a dedicated model which continuously runs in the background (negligible changes to infrastructure - ◐, negligible resource overhead - ○, and negligible maintenance - ○). These mechanisms can detect hijacking attempts by malicious pilots [35, 36].

3) Countermeasures aimed at optimizing integrity:

Dedicated countermeasures should be deployed in a drone's ecosystem in order to verify the correctness of the information obtained and decrease the effect of attacks:

(i) Verification: The correctness of the measurements obtained from sensors must be verified in order to detect sensor spoofing attacks. Common ways of verifying the correctness of sensor measurements to detect spoofed values include the use of anomaly detection methods [7] and the application of rule-based approaches [43] (type - Dt). The main shortcomings of these methods are false negative/positive errors (negligible impact on the drone's usability - ◐, high effectiveness - ◐) and the need to develop and maintain a dedicated model which continuously runs in the background (negligible changes to infrastructure - ◐, negligible resource overhead - ○, and negligible maintenance - ○). These methods [7, 43] can be used to detect attacks against the gyroscope [5] and compass [25]. Random sample consensus [39] can be used in cases in which attackers have managed to spoof part of the data/measurements by sampling a random portion of the data

(type - M). This requires the implementation of a software model which continuously runs in the background (negligible changes to infrastructure - ◐, negligible resource overhead - ○). While the success rate of this method can be tuned to mitigate a fixed portion of compromised measurements from the data (up to 50%), attackers can evade this method by compromising a larger part of the data (high effectiveness - ○). This can be used to mitigate attacks that spoof a small portion of a sensor's measurements [24].

GPS measurements can be verified with positions estimated from gyroscope measurements [41] (type - Dt). The main shortcomings of this method are false negative/positive errors (negligible impact on the drone's usability - ◐, high effectiveness - ◐) and the need to develop and maintain a dedicated model which continuously runs in the background (negligible changes to infrastructure - ◐, negligible resource overhead - ○, and negligible maintenance - ○). Another alternative is to compare compass readings obtained in real-time with measurements that were obtained in advance [40] (type - Dt). In addition to the limitations mentioned above, the primary shortcoming of this method is that it cannot be applied on new flight trajectories before modeling them (negligible effort by the pilot - ○). Another approach for verifying the correctness of GPS measurements is collaborative data attestation, i.e., verifying the obtained measurements with nearby drones [8] (type - Dt). This method has major shortcomings: it requires developing drone-to-drone communication which is currently not supported and requires additional hardware (negligible changes to infrastructure - ○). These methods [8, 40, 41] can be used to detect GPS spoofing attacks [26, 27].

(ii) Redundancy: GPS measurements can be obtained simultaneously from multiple global navigation satellite system (GNSS) protocols (e.g., GLONASS, Galileo, and BeiDou) by integrating multi-constellation receivers into the drone (type - M). The main shortcomings of this method are that it requires dedicated hardware (negligible changes to infrastructure - ○) and attackers can overcome it by spoofing all GNSS protocols (high effectiveness - ○). This method can be used to mitigate GPS spoofing attacks [26, 27].

(iii) Robust modulation techniques: FPV channel jamming can be mitigated using direct sequence spread spectrum (DSSS) modulation or channel hopping [46] (type- M), but this requires dedicated radio transmitters (in cases in which they don't exist: negligible changes to infrastructure - ○). These modulation techniques can be used to mitigate FPV channel jamming attacks [37], but attackers can overcome these methods with powerful radio transmitters (high effectiveness - ◐).

(iv) Dedicated techniques: GPS jamming attacks can be mitigated using null steering [51] (type - M). The primary disadvantages of this method are that it requires dedicated hardware (negligible changes to infrastructure - ○) and attackers can evade it by using multiple transmitters (high effectiveness - ◐). This can be used to mitigate the following attack: [28]. Aerial video-based navigation [42] can be deployed as an alternative navigation technique. This technique determines a drone's location by comparing the surroundings captured via the video camera to a satellite imagery database (type - P). The main shortcomings of this approach are that it relies on heavy real-time video processing (negligible resource overhead - ○) and requires dedicated development (negligible changes to infrastructure - ◐). This method can be used to disable the effectiveness of GPS spoofing attacks [26, 27].

4) Countermeasures aimed at optimizing confidentiality:

The information obtained and stored by targets in a drone's ecosystem must be secured against any type of attack that reveals private information.

(i) Encrypted protocols: The encryption-free (open) mode in drones that use Wi-Fi and XBee for the FPV channel must be disabled; only a private (encrypted) mode that requires a password for joining the network should be used (type - P). This will prevent the implementation of attacks that require the attacker to connect to the network shared by the drone and its GCS: [25, 33–36].

(ii) Authorization: The access to information about other pilots in servers must be restricted (type - P). This will prevent attackers from deanonymizing pilots [35, 38].

(iii) Obfuscation: Code obfuscation can be used in official smartphone applications (type - M). This will make the process of reverse engineering the GCS's application more difficult (high effectiveness - ◐) and mitigate the following attack: [26]. FPV channel obfuscation can be applied by using proprietary protocols (e.g., OcuSync) instead of common protocols (e.g., Wi-Fi). This will prevent the extraction of information from the data layer (high effectiveness - ◐) which is necessary for applying attacks (e.g., [9]) by common packet analyzers (type - M). Proprietary protocols require dedicated development (negligible changes to infrastructure - ◐).

(iv) Constant bitrate video encoders: The option to use a constant bitrate video encoder (e.g., by disabling the video compression) must be allowed (type - P). This will decrease the quality (FPS and resolution) of the video obtained (negligible impact on the drone's usability - ○) but will prevent attackers from determining whether a point of interest is video streamed by a drone [9].

5) Countermeasures aimed at providing recovery:

Parachutes for drones (with automated operation) [44, 45] can be used to save parts of the chassis and cargo, and limit the damage in the case of a crash (type - Re). This requires integrating a dedicated component into the drone (negligible impact on infrastructure - ○) and can be operated when the use of bullets and nets [31, 32] has been successful.

D. Scientific Gaps, Insights & Research Directions

Based on the analysis performed in this section and summarized in Table I, we now point out existing scientific gaps, and based on our findings, we provide conclusions and suggest future research directions.

1) Scientific gaps

We consider an attack against drones severe if the attack can be implemented from a range that does not require the attacker to expose him/herself (OR4-5), does not depend on any environmental conditions (low complexity - ●), and affects a broad sector of drones (high exposure level - ●/◐). An analysis of the information presented in Table I reveals that most of

the attacks reviewed in this section are not considered severe, because they require the attacker to expose him/herself due to low operational ranges (OR1-3) [5, 23–26, 30], their success is dependent on environmental conditions that are not under the control of the attacker (low complexity - ◐/○) [5, 23–26, 30], or they are the result of poor security implementation by the manufacturer (exposure level - ○) [23–26, 35, 38]. Only a few of the attacks are considered severe: GPS jamming, spoofing [25, 26], and all of the attacks against the FPV channel [9, 25, 26, 33–36]. Some of the attacks considered severe [25, 33–36] can be prevented by countermeasure methods that effectively prevent the attack (type - P, high effectiveness - ●) with commercial implementation (TRL 9), negligible additional development and maintenance (negligible maintenance - ●, negligible resource overhead - ●, negligible changes to the infrastructure - ●), and negligible impact on usability (negligible effort by pilot/users - ●, negligible impact on the drone's usability - ●).

A scientific gap in the context of securing a drone is a severe attack for which an effective countermeasure (one that meets the abovementioned criteria) has yet to be developed. (1) GPS spoofing [26, 27]: cannot be prevented by any mechanism with a high technological readiness level. (2) Bullets and nets [31, 32]: these attacks threaten drones in countries that allow civilians to purchase this type of equipment. (3) GPS and FPV channel jamming [28, 37]: these attacks have dedicated mitigation methods, however attackers can bypass them by acquiring stronger radio transmitters/jammers. (4) Determining whether a drone is video streaming a point of interest [9]: the only mechanism that prevents this attack (disabling video compression) comes with a cost in terms of usability (low resolution and FPS rate).

2) *Conclusions and research directions*

The analysis presented in this section reveals that drones and their ecosystems are not yet adequately protected. For example, commercial drones that are used to transport organs to hospitals for transplantation are exposed to severe attacks [9, 26–28, 31, 32, 37] that can be performed with inexpensive, easily procured equipment. This is due to the fact that until recently drones were not manufactured with security mechanisms in mind: they were originally designed for hobbyists and have only recently been adopted for commercial use.

Additional research aimed at addressing the abovementioned scientific gaps is required: (1) Developing new means of autonomous navigation, which will serve as alternatives to GPS-based navigation. This can done by increasing the technological readiness level of video-based navigation for long ranges and developing compass-based navigation for short ranges. (2) Investigating methods enabling drones to avoid bullets and nets. For example, developing automatic evasion mechanisms for drones (e.g., the use of an inconsistent/random flight pattern) that will make it difficult for attackers to shoot nets and bullets at a flying drone. (3) Investigating methods that could be used for confidential/secret tasks. One example is to deploy video encoders with a constant bitrate that can provide reasonable quality (rather than full HD/4K) for real-time video streaming and can be operated by pilots for sensitive tasks (e.g., use by police departments) and prevent attackers from learning which object is video streamed. (4) Examining the aspect of remediation of attacks (how to handle a drone and acquire information in cases in which a drone sensor's output has been detected as compromised in order to return it safely to its pilot); for example, this can be done by obtaining measurements from an uncompromised sensor as an alternative to the compromised measurements (e.g., estimate location based on the gyroscope instead of the GPS). (5) Investigating ways of preventing cyber-attacks applied over the Internet; this is particularly important, since the next drone generation will face the Internet [29]). One example is to focus on adapting existing security mechanisms (e.g., firewalls, IPSs) used for cyber-physical systems for use in protecting drones.

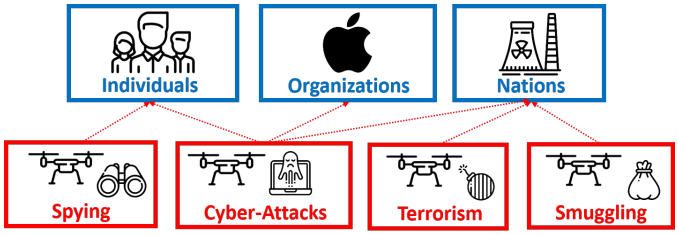

Fig. 2. Security of society – relationship between targets (boxed in blue), threats (boxed in red), and incidents (using red arrows).

III. Securing Society from Drones

In this section, we focus on the following research question: Is society protected against attacks conducted using drones? We start by listing targets within society (Section III-A), discussing adversaries, and reviewing threats (Section III-B). We present a methodology for reviewing countermeasures which is followed by a review of related methods (Section III-C). Finally, we analyze scientific gaps, present our conclusions, and discuss future research directions (Section III-D).

A. Target Identification

In Section II, we examined the security of drones and considered entities within a drone's ecosystem that could be the target of attacks. In this section, societal entities are the targets we aim to secure from attacks conducted by adversaries using drones. We identify three types of targets (see Fig. 2):

(i) Individuals: The security/safety and privacy of civilians.

(ii) Organizations: The security/safety and privacy of companies and organizations.

(iii) Nations: The security/safety of critical infrastructure (e.g., airports), military bases, national facilities, government officials, soldiers, etc.

B. Adversary Profile, & Threat Analysis

We consider an adversary as any pilot who uses a drone in order to violate the security and privacy of individuals, organizations, and nations. The adversary can be an entity acting independently (e.g., a hacker, criminal) or on behalf of a criminal, terrorist, or hacker organization. We identify four primary types of threats that adversaries pose to the three targets (see Fig. 2):

1) Spying: Any type of illegal drone activity which violates the privacy of a target, including video streaming and track-

ing people and organizations. The use of drones to spy on individuals, and more specifically to video stream individuals, is a growing threat to privacy today [52] and an issue that concerns many people [53]. Drones also provide a means of carrying a surveillance device. Several studies have shown that drones equipped with radio transceivers can be used to locate and track people across a city by recognizing the MAC address of their owner's device (e.g., smartphones) [54] and perform an MITM attack on telephony [55] by downgrading 4G to 2G. Drones can also be used to carry traditional spying devices used to eavesdrop on conversations (e.g., directional microphones). The use of drones to spy on organizations is limited to video streaming the organization; therefore it is not considered a dangerous threat. The use of drones to spy on nations in the context of espionage is usually done with non-commercial drones and is not within the scope of this paper.

2) Terrorism: Any type of physical attack performed using a drone that results in the injury/death of individuals and/or the collapse/destruction of an organization or national facility. The use of armed drones for terrorism against nations was demonstrated in an attack against Russian military bases in Syria [12]. Drones also threaten airports, because commercial airplanes are vulnerable to exploding and colliding drone attacks during takeoff and landing [56]. This threat led to the cancellation of hundreds of flights at Gatwick Airport near London [57]. Dozens of near miss incidents involving drones around the world have been reported [58]. Furthermore, drones can cause major disasters, in terms of the number of casualties, by exploding into critical infrastructure (e.g., a nuclear plant) [59]. The use of drones for terrorism against politicians is a growing threat that was recently demonstrated in Venezuela [10], Japan [11], and the US [52]. The use of drones for terrorism against organizations/companies and random individuals/civilians has not yet been demonstrated.

3) Cyber-attacks: Any type of attack against computing devices that requires the adversary to have a line of sight to the device or be within a specified distance of the target device, necessitating the use of a drone. The use of drones equipped with a radio transceiver to perform cyber-attacks against individuals and organizations has been demonstrated in several studies [18, 60–63]. Attackers can use drones to: (1) break into wireless networks [60, 61], (2) steal printed documents [63] (by impersonating a network printer), (3) spread a worm across Philips Hue smart bulbs [62], and (4) hijack a Bluetooth mouse [18]. The use of drones to perform cyber-attacks against organizations and facilities that use air-gapping to secure their networks has also been demonstrated. Two studies [64, 65] used a drone to establish an optical covert channel for data infiltration [65] and exfiltration [64] to/from an air-gapped network. In these studies, the drone was used to carry a laser transmitter [65]) and an optical sensor [64], in order to create a line of sight to a target device in the organization's air-gapped network and establish a communication channel with preinstalled malware.

4) Smuggling: Any type of illegal transfer of goods performed using drones. The use of drones to smuggle goods into facilities and between countries has also been demonstrated. Drones have recently been used by criminals to drop weapons into prison yards [66], and smuggle goods and drugs between countries over borders [67]. Thus far, the use of drones for smuggling has been restricted to incidents targeting nations and national facilities.

C. Review of Countermeasure Methods

Here we review countermeasure methods used to protect a society from attacks conducted using drones. We start by describing the criteria used to evaluate countermeasures (Section III-C1) and then review and analyze related methods (Sections III-C2 - III-C4) according to the criteria.

1) Methodology

We defined seven assessment criteria for countermeasure methods. We note that the definitions for some of the criteria used to analyze countermeasures for securing drones cannot be used to analyze countermeasures for securing society. As a result, we adapted and redefined some of the criteria so they can be used to analyze countermeasures for securing society. We also added additional criteria that should be assessed when analyzing countermeasures for securing society. Definitions of the criteria are provided below:

The first two criteria are (i) operation range (OR1-5), which addresses the operational range of a countermeasure against drones and was defined in Section II-B, and (ii) technical readiness level (TRL 1-9), which was defined in Section II-C. For the criteria listed below, the following symbols are used to indicate whether a method fully satisfies (denoted as ●), partially satisfies (denoted as ◐), or does not satisfy (denoted as ○) a criterion:

(iii) Negligible changes to infrastructure (●/◐/○): deployment requires (●) - no additions/changes to infrastructure; (◐) - negligible changes to infrastructure (e.g., deploying video cameras, antennas); (○) - dedicated facility/areas (e.g., dedicated area for radar).

(iv) Low operation level (●/◐/○): operating the method requires (●) - no special expertise; (◐) - certified manpower (e.g., a guard); (○) - trained professionals (e.g., the use of commercial lasers).

(v) Negligible impact on environment (●/○): (●) - the method can be operated in populated areas; (○) - otherwise.

(vi) Negligible cost (●/◐/○): the cost to deploy this method is (●) - under a thousand dollars (USD); (◐) - up to a few thousand dollars; (○) - otherwise.

(vii) High effectiveness (●/◐/○): the attacker (●) - cannot evade the countermeasure (or must stop the malicious activity and leave the attack scene); (◐) - can evade the countermeasure by making non-negligible improvements to his/her capabilities or under specific environmental conditions (e.g., in darkness); (○) - can evade the countermeasure by making negligible improvements to his/her capabilities (e.g., using a different type of drone).

(viii) High performance (●/◐/○): Attacks are prevented/detected by the countermeasure with (●) - high accuracy; (◐) - medium accuracy (e.g., high false positive rates); (○) - low accuracy (e.g., low true positive rates).

Preventing the implementation of attacks conducted using drones requires a progressive process (rather than a dedicated

method, as is the case when securing a drone from attack) that consists of the following three chronological steps. Step 1: detection, which involves identifying the presence of a suspicious drone in space. Step 2: assessment, which involves determining whether the drone is hostile. Step 3: interdiction, which involves disabling the drone. The countermeasures are reviewed in Sections III-C2 - III-C4 as follows: they are first categorized based on the chronological steps (1-3) and are then categorized by type. We review related countermeasure methods and analyze their use against commercial drones based on the criteria described in the previous subsection. The results of the analysis are summarized in Table II.

2) Detection & tracking

The first step in securing society from hostile drones is to detect and track them. Drone detection refers to recognizing that there is a drone nearby. Drone tracking refers to determining the exact coordinates and altitude of the drone over time (the drone's trajectory). We review scientific and industrial methods used for detection and tracking purposes given the sensors on which they are based (radar, RF scanner, video camera, LiDAR, thermal camera, acoustic, and hybrid sensors). In addition, Table III provides a comparison of the 33 largest drone detection companies [18] that sell commercial devices for drone detection, comparing their products based on the sensors they use and the features they support, according to their specifications. We validated the data in Table III by contacting the companies by mail (33% of them responded).

(a) Radar: Several studies have investigated drone tracking using radar and found that (1) extremely high frequency radar (35 GHz with 1 GHz bandwidth) is required to detect small commercial (mini) drones [68], (2) the non-plastic portions of the drone (e.g., battery pack, carbon fiber frame) dominate its radar signature, as opposed to the plastic portions (e.g., blades) which do not provide a significant return [69], and (3) radar misclassifies birds as drones [70]. Commercial radar has wide operation ranges of 10-50 kilometers (OR5), and it is not influenced by adverse ambient conditions, such as light, darkness, and noise (high effectiveness - ●). However, radar raises false alerts due to the presence of birds (high performance - ◐), and its cost can reach hundreds of thousands of dollars (negligible cost - ○). In addition, radar is not intended to be deployed in urban environments and requires a dedicated area/facility for deployment (negligible changes to infrastructure - ○, negligible impact on environment - ○); it also requires trained professional operators (low operation level - ○). According to the industry analysis that we performed and present in Table III, 13 of the 33 companies analyzed use radar [71–83].

(b) RF scanner: Several studies [6, 9, 84, 85] have suggested the use of RF scanners to detect a drone's presence. *Bisio et al.* [84] and *Nassi et al.* [9] suggested performing network traffic analysis on suspicious intercepted Wi-Fi transmissions in order to classify them as an FPV channel by applying time domain analysis [84] and frequency domain analysis [9] and were able to detect a drone in three seconds. Other studies [6, 85] suggested analyzing the physical layer of the radio signal transmitted from the drone (downlink of the FPV channel). *Birnbach et al.* [6] analyzed the received strength of the downlink of the FPV channel to classify the patterns of drones during approaching, escaping, and spying episodes. *Mototolea et al.* [85] suggested triangulating information from multiple RF scanners located in different locations in order to track a drone. RF scanners have medium detection ranges (OR4), are not influenced by adverse ambient conditions, such as light, darkness, and noise (high effectiveness - ●), can be deployed in urban areas (impact on environment - ●), can be operated with no special expertise (low operation level - ◐), and are inexpensive (low cost - ●). However, they require the deployment of dedicated receivers and antennas (negligible changes to infrastructure - ◐). RF scanners can suffer from low true positive rates, misclassifying an FPV channel as something else (high performance - ○) when a given radio fingerprint of a drone does not exist in a database. According to the industry analysis that we performed and present in Table III, 13 of the 33 companies analyzed use RF scanners [71, 78, 86–96].

(c) Optical methods:

Video cameras: Several studies have suggested methods to detect a drone using a video camera that detects visible frequencies by extracting visual features [97, 98] from the frames of the video stream. *Rozantsev et al.* [99] proposed using six ground cameras to track a drone, accurately reconstructing a drone's flight trajectory within a 100x50 square meter area with an error of up to four meters. Video cameras have an optical detection range (OR3), can be deployed and

TABLE II
SECURING SOCIETY: SUMMARY OF COUNTERMEASURE METHODS FULLY SATISFIES (●), PARTIALLY SATISFIES (◐), DOES NOT (○) SATISFY THE CRITERION. NEG. = NEGLIGIBLE, INFRA. = INFRASTRUCTURE, ENV. = ENVIRONMENT.

	Method	Operation Range	TRL	Neg. Changes to Infra.	Low Operation Level	Neg. Impact on Env.	Neg. Costs	High Effectiveness	High Performance
Detection & Tracking	Radar [68–83]	5	9	○	○	○	○	●	◐
	RF Scanner [6, 9, 71, 78, 84–96]	4	9	◐	◐	●	●	●	○
	Video Camera [71, 74, 76, 89, 97–99] [77–80, 88, 92, 100–102]	3	9	◐	●	●	●	◐	◐
	Infrared Camera [71, 74, 78, 83, 103–105] [79, 92, 100–102]	3	9	◐	●	●	◐	◐	◐
	LiDAR [106–108]	3	9	◐	●	●	○	●	◐
	Acoustics [72, 109–112] [77, 91, 93, 101, 105, 113, 114]	2/3	9	◐	●	●	●	◐	○
	Hybrid (Acoustics & Optics) [101, 105, 115, 116]	3	9	◐	◐	●	◐	●	●
	Hybrid (Radar & Optics) [101, 105, 115, 116]	5	9	○	○	○	○	●	●
Assessment	Data Link Layer-Based Classification [117]	4	5	◐	◐	●	●	○	●
	Physical Layer-Based Classification [118]	4	4	◐	◐	●	●	●	◐
	LED License [119]	3	1	●	●	●	●	○	●
	DSRC-Based Identification [120]	4	9	◐	●	●	●	○	◐
	Camera and IMU Based Identification [121]	3	4	◐	◐	●	●	○	○
	Detecting Capture POI [9]	4	5	◐	◐	●	●	○	●
Interdiction	Bullets & Nets [31, 32]	3/4	9	●	◐	●	●	●	●
	Commercial Jammers [122–125]	4	9	○	○	○	○	●	●
	Predator Birds [126]	3	9	○	◐	●	○	○	●
	Laser Cannons [127, 128]	4	9	○	○	○	○	●	●

used in populated areas (negligible impact on environment - ●), do not require dedicated expertise (low operation level - ●), and are sold for a few hundred dollars (negligible cost - ●). However, as was indicated by *Saqib et al.* [129], video camera-based methods suffer from high false positive rates due to the similarities between the movements of drones and birds (high performance - ◐) and are not effective in darkness (high effectiveness - ◐).

LiDAR & infrared cameras: In order to detect drones in darkness, *Muller et al.* [103] suggested a short wave infrared (SWIR) camera for night detection. However, *Birch et al.* [104] indicated that a long wave infrared (LWIR) camera performs better than a SWIR camera, especially when the background of the drone is the skyline. *Church et al.* [106] analyzed the detection of drones using a LiDAR sensor and found that (1) commercial drone speed does not affect the accuracy of detection, and (2) drones can be detected from a distance of a few hundred meters. Infrared cameras share the same advantages and disadvantages of video cameras, since infrared cameras are less effective in the light (high effectiveness - ◐). However, infrared cameras are more expensive (negligible cost - ◐) than standard video cameras. LiDAR has the same advantages as video cameras. In addition, LiDAR is highly effective in adverse ambient conditions (high effectiveness - ●). However, LiDAR's greatest disadvantage is its high price (negligible cost - ○).

Typically, cameras that capture visible and invisible wavelengths are combined to support detection throughout the day and night. Sixteen of the 33 companies analyzed use at least one optical sensor to detect drones: a video camera [71, 74, 76–80, 88, 89, 92, 100–102], infrared camera [71, 74, 78, 79, 83, 92, 100–102, 105], or LiDAR [107, 108].

(d) Acoustic methods: Several studies [109–111] investigated methods to detect the presence of a drone by analyzing the noise emitted from the drone's rotors and found that the acoustic signature of a drone's rotors can be detected in the frequency domain via a microphone [109], very quickly (in 200 milliseconds) [110], from a range of up to 600 meters, using a microphone array consisting of four microphones [111]. *Chang et al.* [112] evaluated a method for tracking a drone by triangulating sound obtained from two distributed microphone arrays (each consisting of four microphones) and were able to estimate a 100 meter drone trajectory with an error of up to two meters for 80% of the trajectory.

Acoustic methods can be deployed in populated areas (negligible impact on environment - ●), are considered cheap compared to radar and LiDAR (negligible cost - ●), and can be operated with no special expertise (low operation level - ●). However, acoustic methods have a low detection range (OR2-3), require dedicated hardware (negligible changes to infrastructure - ◐), are vulnerable to ambient noise (high effectiveness - ◐), and can suffer from low true positive rates, misclassifying a drone as something else (high performance - ○) when a given acoustic drone fingerprint does not exist in a database. These are likely the reasons that acoustic methods are only used by eight [72, 77, 91, 93, 101, 105, 113, 114] of the 33 companies analyzed.

(e) Hybrid methods: Table II provides a summary of the countermeasures presented in this section, indicating their ability to satisfy the criteria assessed. As can be seen, none of the single sensor-based methods is capable of satisfying the high effectiveness and performance criteria. In order to overcome the limitations that arise from using a single sensor-based method, various approaches that rely on sensor fusion have been suggested. These approaches provide a high level of detection (high effectiveness - ●, high performance - ●).

One approach that was investigated by [115, 116] is combining a set of acoustic and optical sensors in order to improve detection in dark conditions and decrease the false positive rate (resulting from bird misclassification). This approach shares most of the advantages of acoustic/optical methods (negligible changes to infrastructure - ◐, negligible impact on environment - ●). However, combining of a set of video cameras and microphones can be expensive (negligible cost - ◐), require certified manpower (low operational level - ◐,) and may still provide low detection ranges (OR3). These are probably the reasons that only a few companies use this approach [101, 105]. Another approach is to combine radar with at least one optical sensor. The greatest advantage of this approach is that drones and birds can be classified more accurately, so this approach decreases false positive and false negative rates. This approach can be used to detect drones from high detection ranges (OR5) and has been heavily adopted by industry [71, 74, 76, 78–80, 83]. However, this approach is considered very expensive (negligible cost - ○), requires trained professional operators (low operation level - ○), is not intended for deployment in urban environments (negligible impact on environment - ○), and requires a dedicated area/facility for deployment (negligible changes to infrastructure - ○).

Other combinations (see Table III) are less common. Hybrid methods can provide high effectiveness, high performance, and high detection ranges, however their primary disadvantage is their cost. As can be seen from Table III, using multiple sensors for drone detection is the approach taken by more than 54% of the companies we analyzed (18 companies use multiple sensors as a means of detection).

3) Assessment

The second step in securing society from hostile drones is to assess whether the detected drone is hostile; this step is particularly important in areas that allow drone flights, since drones located in the exact same location can be used for both legitimate and illegitimate activities. Determining whether a drone is hostile can be done by classifying a drone's type, remotely identifying a drone, and recognizing its activity:

(a) Classification: Drone classification refers to identifying the manufacturer and model of the drone. Classification can only be used to detect a hostile drone in cases in which the type of drone detected is not among the types that are allowed to fly in a specific area. The following methods: [117, 118] rely on RF scanners. Such methods have several advantages: they can be used in populated areas (negligible impact on environment - ●), are based on inexpensive devices with an additional antenna (negligible cost - ●, negligible changes to infrastructure - ◐), and provide a medium operational range (OR4). However, the main difference between the methods is

TABLE III
COMPARISON OF TOP COMMERCIAL DETECTION DEVICES FOR DRONES.

		Radio		Optical			Acoustic	Features				
Company Name	Product Name	Radar	RF Scanner	Camera	LiDAR	Infrared	Microphone	Effective Range (KM)	Classification	Coverage (°)	Tracking	Mobility
3DEO	Rogue Drone Detection Mitigation [107]				✓			2			✓	
Aaronia	Drone Detection System [71]	✓	✓	✓		✓		50	✓	90/360	✓	✓
Anti-Drone.eu	GROK [72]	✓						4	✓		✓	
	Droneshield [130]						✓	0.5				
Aveillant	Gamekeeper 16U - Holographic Radar [73]	✓						5		90	✓	
Black Sage - BST	UAVX [74]	✓		✓		✓		0.5		90	✓	✓
C speed LLC	LightWave Radar [75]	✓									✓	
CACI	SkyTracker [86]		✓						✓			
CerbAir	Hydra [87]		✓					2	✓	90/360	✓	✓
Chess Dynamics Ltd	AUDS [76]	✓		✓		✓		10		180	✓	✓
DeDrone.com	DroneTracker [88]		✓	✓					✓			✓
DeTect	DroneWatcher [89]		✓					1.6-3.2	✓			✓
	HARRIER DSR [77]	✓		✓			✓	3.2	✓		✓	
Digital Global Systems	SigBASE [90]		✓									✓
DroneShield	FarAlert/WideAlet Sensors [105]					✓	✓	1		30		✓
Gryphon Sensors	Skylight [78]	✓	✓	✓		✓		3-10		360	✓	✓
HGH Infrared Systems	UAV Detection & Tracking [100]			✓		✓				360		
Kelvin Hughes Limited	SharpEve SxV Radar [79]	✓		✓		✓		1.5		360	✓	✓
MAGNA	Drone Detection [101]			✓		✓	✓	0.5-1				
Microflown AVISA	Skysentry AMMS [91]		✓				✓	0.4-1		360	✓	
Mistral Solutions	Drone Detection and Classification System [92]		✓	✓		✓		1	✓			
ORELIA	Drone-Detector [113]						✓	0.1		360		
Quanergy Systems	Q-Guard - LiDar X-Drone [108]				✓			0.1				
Rinicom	SKY PATRIOT [102]			✓		✓		1.5	✓	30		
Rinicom and METIS Aerospace	SKYPERION [93]		✓				✓	4				
ROBIN Radar Systems	ELVIRA [80]	✓		✓							✓	✓
Rohde and Schwarz	RS ARDRONIS-I [94]		✓					1-2	✓			
SAAB Group	Giraffe AMB Radar - ELSS [81]	✓						30-470		360	✓	✓
Sensofusion	AIRFENCE [95]		✓									✓
SpotterRF	A2000 Radar UAVX [82]	✓						0.2-1		45/90	✓	✓
Squarehead Technology	DiscovAir [114]						✓					
TCI International	BlackBird [96]		✓									✓
Thales	SQUIRE [83]	✓				✓		48			✓	✓

their level of effectiveness and performance.

Peacock et al. [117] analyzed the data link layer of the Wi-Fi FPV channel and showed that the SSID (service set identifier) of a network and the MAC address of a connected drone (which can be extracted by packet analyzers) can be used to determine the drone type. This method can accurately classify drones according to the MAC provided by the manufacturer (high performance - ●), but its main disadvantage is that attackers can easily evade classification by changing the drone's MAC address (high effectiveness - ○). *Nguyen et al.* [118] showed that unique characteristics can be extracted from the physical layer of the FPV channel regarding the drone's movement (e.g., shifting, vibration) in order to classify the drone. The unique characteristics are affected by various components (rotors, shape, and propellers) and vary depending on the model so attackers cannot evade classification (high effectiveness - ●). However, the main disadvantage of this approach is its performance which varies between 64 and 89% (high performance - ◐).

(b) Remote drone identification: According to the Federal Aviation Administration (FAA), *"Remote ID is the ability of a drone in flight to provide identification information that can be received by other parties"* [131]. Remote drone authentication and identification in areas that allow drone flights can be performed by authenticating the drone (remote drone identification) and by authenticating the pilot (remote pilot identification). *Yao et al.* [119] suggested a dedicated LED license for drones. The simplicity of this approach is its primary advantage, since it does not require any additional hardware (negligible cost - ●, negligible changes to infrastructure - ●, negligible impact on environment - ●) and can be used by anyone to accurately identify drones (low operation level - ●, high performance - ●). However, identification is limited to optical ranges (OR-3), and attackers can easily duplicate such licenses (high effectiveness - ○).

Another suggestion made by *Yao et al.* [119] is an identification platform for nearby drones which is based on dedicated short-range communications (DSRC). DJI recently

implemented such an identification system for their drones, AeroScope [120], which provides detailed information (e.g., operator's ID, the flight's location and altitude) based on DSRC. AeroScope is intended for consumer use (negligible cost - ●, low operation level - ●), can be deployed in populated areas (negligible impact on environment - ●), and provides a medium operational range (OR4). However, AeroScope has several disadvantages: the pilot can deactivate information sharing and avoid identification (high effectiveness - ○); it can only detect DJI drones, so other drones remain undetected (high performance - ◐); and it requires dedicated hardware (negligible changes to infrastructure - ◐).

Ruiz et al. [121] suggested a method for identifying a drone located among *O(n)* other visually identical drones. They suggested matching the motion detected by the drone's inertial sensors (transmitted by radio signals) and the motion detected by a video camera. This method requires a radio receiver (with an antenna) and a video camera, and it can be used in populated areas (negligible changes to infrastructure - ◐, negligible impact on environment - ●, negligible costs - ●). However, the main disadvantages of this approach are its low operational range (OR3) and the fact that every drone detected by the video camera must be examined, meaning that identifying a single drone among *n* nearby drones requires *O(n)* examinations (high performance - ○). In addition, attackers can imitate the flight behavior of a nearby drone in order to evade identification (high effectiveness - ○).

(c) Activity recognition: Detecting the real activity of a drone in areas that allow drone flights is a very challenging task: given a drone that is passing by a house, how can we determine whether the drone is being used for a legitimate purpose (e.g., delivering a pizza), for spying (e.g., snooping on a neighbor), or to conduct a cyber-attack?

Nassi et al. [9] suggested a method to determine whether a specific POI is being video streamed by a drone. Their method exploits the variable bitrate mechanism in the H264 video compression algorithm and utilizes a flickering LED installed on a POI to watermark the bitrate of the uplink channel. The watermark indicates that the POI is captured by a drone's camera and can be used to determine whether a drone is being used to spy on a POI. The primary advantages of this method are that it relies on a Wi-Fi receiver and a connected antenna (negligible cost - ◐, negligible impact on environment - ◐), provides a medium operational range (OR4), and can detect a spying drone in 2-3 seconds (high performance - ●). However, the main disadvantage of this method is that it is currently only effective for Wi-Fi FPV drones (high effectiveness - ○) and requires the installation of dedicated equipment (for flickering) near a target POI (negligible changes to infrastructure - ◐).

4) Interdiction (disabling drones):

The third step in securing society from attacks conducted using drones is to disable a detected drone whose activity was determined as hostile (e.g., spying on an individual). The review in this section complements the review presented in Section II-B on attack methods used against a drone's ecosystem. Here we focus solely on industrial methods that can be used quickly after a drone's activity has been determined as hostile by individuals, municipal authorities, militaries, and nations. In addition, we focus on legal methods. For example, GPS spoofing might be used by attackers to disable a drone (reviewed in Section II-B), but its application is against the law in countries due to its negative impact on nearby airplanes and devices, so it cannot be used by municipal authorities to disable a hostile drone and thus is not covered in this section.

(a) Nets and bullets: These methods were reviewed in Section II-B and analyzed in Table II; therefore, we do not analyze them again here.

(b) Commercial anti-drone jammers: These jammers are directional RF transmitters in the form of mobile shooting guns [122, 123] or stationary devices [124, 125]. Commercial anti-drone jammers apply jamming to GPS and FPV bands known to be used by drones. FPV channel jamming is effective against manual operations, since it disables video streaming and maneuvering capabilities. The inability to receive commands from the pilot causes the drone to fly in the air where it is exposed to various attacks with a depleting battery. GPS jamming threatens autonomous flights that rely on GPS measurements (high performance - ●, high effectiveness - ●). In addition, the most effective jammer on the market can reach ranges of up to two kilometers (OR4). The main disadvantage of commercial radio jammers is their effect on other nearby devices that utilize radio communication (negligible impact on environment - ○). As a result, their use against drones is restricted in some countries. In addition, stationary commercial jammers are usually deployed in a dedicated facility/area (negligible changes to infrastructure - ◐), can only be operated by trained professional operators (low operation level - ○), and are very expensive (negligible costs - ●).

(c) Predator birds: One company [126] sells eagles and falcons that have been trained to detect, capture, and land drones. However, the operational range that predator birds provide against drones (OR3) is limited compared to jammers. They are very effective against nano and micro commercial drones (high performance - ●), but attackers can use a heavier commercial mini drone in order to avoid being captured by these birds (high effectiveness - ○). In addition, they require a certified operator (low operation level - ◐) and are very expensive (negligible costs - ○).

(d) Laser cannons: Several companies sell laser cannons that irradiate a directed high energy laser beam that causes a drone to burn in the air and crash to the ground [127, 128]. Laser cannons support an operational range of two kilometers (OR4) and are highly effective (because a drone must abandon its malicious task in order to avoid being hit). However, commercial lasers require trained professional operators (low operation level - ○) and a dedicated facility/car for installation (negligible changes to infrastructure - ○).

D. Scientific Gaps, Insights & Research Directions

Based on the analysis performed in this section (summarized in Tables II and III), we now analyze the preparedness of each target to mitigate attacks conducted using drones. Specifically, for each societal target (national facilities, organizations, and individuals) we analyze the related threats, profile the criteria required for an optimal countermeasure method to handle the

threats, point out scientific gaps, and provide our conclusions regarding the research question: Is the target protected against attacks conducted using drones? It should be mentioned that in the analysis we focused on threats that require a dedicated countermeasure against the drone itself (i.e., spying, terrorism, and smuggling) rather than on cyber-attacks (performed via a drone) [18, 60–65] that can be effectively mitigated without considering the drone as a means for the attack. That is, some cyber-attacks (e.g., [64, 65]) can be prevented by an IPS, while other cyber-attacks (e.g., [18, 60–63]) can be prevented by upgrading/patching the protocols used.

1) National facilities

Based on the analysis presented in this section, we define the criteria for optimal countermeasures aimed at protecting national facilities from threats posed by drones. These facilities (e.g., airports, prisons, critical infrastructure) are primarily susceptible to terrorism [12, 57, 59] and smuggling [66, 67]. Because these threats have already been demonstrated in the past [12, 57, 59, 66] and can result in human losses, optimal countermeasures aimed at handling such threats must be resilient to adaptive attacks (high effectiveness - ●) and provide high detection rates with a minimal number of false alarms (high performance - ●). In addition, since early detection of such threats is necessary for immediate response, optimal countermeasures aimed at handling such threats must also have a wide operational range (OR4-5). Satisfying the other criteria (negligible impact on environment, negligible changes to infrastructure, low operation level, and low cost) are less important, since such facilities are often very large, isolated from urban environments, and operated by authorities.

The analysis of countermeasure methods with respect to the criteria specified reveals three interesting observations: First, hybrid methods (such as those that combine optics with radar [77, 101, 105]) are optimal countermeasures for the purpose of detection and tracking. Second, since national facilities are considered no-flight areas (i.e., restricting drone flights near/over them), assessment methods are not required (because any drone that infiltrates their air space is considered hostile). Third, lasers [127, 128] and jammers [122–125]) are optimal countermeasures for the purpose of interdiction. The main insight from these observations is that given that national facilities are isolated and have the budget for purchasing the necessary dedicated mechanisms, they can be secured against hostile drones. Despite that, we identify the existence of asymmetry in terms of the cost required by an attacker to implement an attack on a national facility (the cost of purchasing an inexpensive drone) and the cost of the technology required to prevent such attacks (the cost of expensive technologies such as radar and lasers).

2) Organizations/companies

The main observation from the analysis presented in this section is that organizations are primarily susceptible to cyber-attacks. As we mentioned earlier here, cyber-attacks can be effectively mitigated by either reducing the attack surface or by using traditional IT countermeasures. The main insight from this observation is that organizations/companies are adequately protected against cyber-attacks conducted by drones.

3) Individuals

Based on the analysis presented in this section, we define the criteria for an optimal countermeasure aimed at protecting individuals from threats posed by drones. Since, many areas around the world allow drone flights in populated areas for commercial use, individuals are mainly susceptible to spying performed via drones (e.g., tracking the movement of a person [52]). Spying requires the attacker to maintain a line of sight with a target; hence, an optimal countermeasure method aimed at handling this threat must provide at least a medium operational range (OR3). In addition, since the countermeasure must able to be used by individuals who are not highly skilled and have limited financial resources, an optimal countermeasure must have commercial implementation (TRL 8-9), be reasonably priced (low cost - ●), and be able to be operated with no special expertise (low operation level - ●). Furthermore, because most individuals live in populated areas, an optimal countermeasure must be safe to operate in populated areas (negligible impact on environment - ●) and support deployment in apartments/buildings (negligible changes to infrastructure - ●/◐). In addition, an optimal countermeasure must be resilient to adaptive attacks and provide a high detection rate with a low number of false positives (high effectiveness ●, high performance ●).

The analysis of countermeasure methods with respect to the abovementioned criteria reveals three interesting observations: First, an optimal countermeasure method for the purpose of detection and tracking that is intended for consumer use has yet to be developed, pointing out a major scientific gap. Second, an optimal countermeasure method for the purpose of assessment that is intended for consumer use has also yet to be developed. When considering spying as a primary threat to individuals, determining whether a detected drone is used for spying is extremely important. Hence, the lack of an optimal countermeasure method points out another scientific gap. Third, bullets and nets are optimal countermeasures for the purpose of interdiction (if their use by individuals is allowed). The main insight from these observations is that individuals are not yet adequately protected against drones used for spying (video streaming and tracking). It should be noted that the need for dedicated methods intended for consumer use arose only a few years ago when drones were permitted to fly in populated areas.

4) Research directions

Additional research aimed at addressing the abovementioned scientific gaps and the asymmetry between the cost of a drone and the cost of the technology required to protect society from attacks performed by drones: (1) Developing inexpensive detection and tracking methods that have high levels of effectiveness and performance. For example, replacing a central expensive mechanism (e.g., radar) with a distributed network of inexpensive sensors serving as one strong detection and tracking mechanism (e.g., a system in which laptops that communicate with each other are deployed on different sides of a building to detect and track a passing/approaching

Wi-Fi FPV drone). (2) Developing detection, tracking, and assessment methods intended for consumer use. For example, developing an Internet-based remote drone identification platform that provides information about nearby drones (e.g., a drone's stated activity, pilot). The integration of eSIM in the next generation of drones opens up new opportunities for building such a platform without the need to develop dedicated protocol for remote drone identification (e.g., utilizing existing knowledge on tracking users via the cellular cells that their smartphones are connected to). (3) Investigating methods for recognizing illegal activity performed by a drone with a proprietary FPV channel. For example, detecting illegal drone activity by analyzing a drone's flight trajectory/pattern.

Additional research is also required for detecting and tracking new types of drones that are currently being developed: (1) Drones that are disguised as birds (with wings instead of propellers) are not yet sold commercially, however such drones represent an emerging research trend [20]. The acoustic and visual signatures of their flight differ from the current drone generation, so improved optical and acoustic methods are required to detect such drones; and (2) Fully autonomous drones that operate without any pilot control might appear in the future and require improved/new detection methods which are not based on utilizing the FPV channel.

IV. Concluding Remarks & Discussion

In this section, we focus on the following research question: Has the technology that is needed to protect drones and society from one another matured enough to handle the challenges that a large volume of flights will create? The analysis presented in this paper reveals the following: First, the technology required to secure drones and society from one another has not yet been developed for the safe and responsible deployment of drones. The abovementioned scientific gaps (for both entities) must be addressed, and the level of security and privacy must be optimized beyond its current level. These findings raise concerns regarding the preparedness of each side and their ability to safely handle the upcoming challenges of the age of drones. Commercial drones that are currently used to transport organs to hospitals for transplantation [1] are exposed to severe attacks [9, 26–28, 31, 32, 37] that can be performed with easily procured equipment. On the other hand, society is not protected against attacks conducted using drones, especially in areas that allow drone flights.

Second, while both entities should strive to achieve a perfect level of security and privacy, an interesting question arises: In theory, can both entities (drones and society) reach a perfect level of security and privacy in parallel? The analysis performed in this paper reveals an interesting tradeoff between drones and society in that the security and privacy of drones cannot be optimized without decreasing the security and privacy of society, and vice versa. For example, deploying a method that prevents GPS spoofing will make it more difficult to disable a drone used to perform a terrorist attack. Similar to cryptography (where there is a tradeoff between public safety and preserving data confidentiality), there is a need to find a responsible balance between the level of security and privacy of drones and society. Examining whether this balance has been achieved can serve as the basis of criteria for the safe and responsible deployment of drones.

References

[1] DroneDJ, "Dji matrice 600 pro successfully deliver kidney in maryland," https://dronedj.com/2018/11/21/dji-matrice-600-pro-deliver-kidney/.

[2] Wikipedia, "Delivery drone," https://en.wikipedia.org/wiki/Delivery_drone.

[3] B. Insider, "Amazon and ups are betting big on drone delivery," http://www.businessinsider.com/amazon-and-ups-are-betting-big-on-drone-delivery-2018-3.

[4] Wired, "President trump moves to fill america's skies with drones," https://www.wired.com/story/faa-trump-drones-regulations/, 2017.

[5] Y. Son, H. Shin, D. Kim, Y.-S. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors." in *USENIX Security Symposium*, 2015, pp. 881–896.

[6] S. Birnbach, R. Baker, and I. Martinovic, "Wi-fly?: Detecting privacy invasion attacks by consumer drones," *NDSS*, 2017.

[7] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Xinyan, "Detecting attacks against robotic vehicles: A control invariant approach," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 801–816.

[8] T. Abera, R. Bahmani, F. Brasser, A. Ibrahim, A.-R. Sadeghi, and M. Schunter, "Diat: Data integrity attestation for resilient collaboration of autonomous systems," *NDSS*, 2019.

[9] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici, "Drones' cryptanalysis - smashing cryptography with a flicker," in *2019 2019 IEEE Symposium on Security and Privacy (SP)*, vol. 00, 2019, pp. 833–850.

[10] N. Y. Times, "Venezuelan president targeted by drone attack, officials say," https://www.nytimes.com/2018/08/04/world/americas/venezuelan-president-targeted-in-attack-attempt-minister-says.html.

[11] Spiegel, "Man arrested for landing 'radioactive' drone on japanese prime minister's roof," https://www.independent.co.uk/news/world/asia/man-arrested-for-landing-radioactive-drone-on-japanese-prime-ministers-roof-10203517.html.

[12] T. Drive, "Russia offers new details about syrian mass drone attack, now implies ukrainian connection," http://www.thedrive.com/the-war-zone/17595/russia-offers-new-details-about-syrian-mass-drone-attack-now-implies-ukrainian-connection.

[13] B. Insider, "Drone market shows positive outlook with strong industry growth and trends," http://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts-2017-7, 2017.

[14] "The global anti-drone market size is anticipated to reach usd 1.85 billion by 2024," https://www.prnewswire.com/news-releases/the-global-

anti-drone-market-size-is-anticipated-to-reach-usd-1-85-billion-by-2024--300673188.html, 2018.

[15] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, p. 7, 2017.

[16] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, 2018.

[17] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, 2018.

[18] D. L. Fran Brown, "Game of drones," *DefCon 25*, 2017.

[19] A. H. Michel, *Counter-drone systems*. Center for the Study of the Drone at Bard College, 2018.

[20] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progress in Aerospace Sciences*, vol. 91, pp. 99–131, 2017.

[21] R. D. Arena, "Wifi fpv vs 5.8ghz fpv vs 2.4ghz fpv: Ultimate guide," http://www.rcdronearena.com/2016/03/15/wifi-fpv-vs-5-8ghz-fpv-vs-2-4ghz-fpv-explained/.

[22] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012, pp. 585–590.

[23] R. Sasi, "Drone attacks: How i hijacked a drone," https://nullcon.net/website/archives/goa-2015.php, 2015.

[24] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling uavs with sensor input spoofing attacks." in *WOOT*, 2016.

[25] M. Robinson, "Knocking my neighbors kids cruddy drone offline," *DefCon 23*, 2016.

[26] A. Luo, "Drones hijacking - multi-dimensional attack vectors and countermeasures," *DefCon 24*, 2017.

[27] D. He, Y. Qiao, S. Chen, X. Du, W. Chen, S. Zhu, and M. Guizani, "A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles," *IEEE Network*, 2018.

[28] J. Farlik, M. Kratky, and J. Casar, "Detectability and jamming of small uavs by commercially available low-cost means," in *2016 International Conference on Communications (COMM)*. IEEE, 2016, pp. 327–330.

[29] Counterpoint, "Cellular connected drones will be the 'iphone moment' for drone industry," https://www.counterpointresearch.com/cellular-connected-drones-will-iphone-moment-drone-industry/.

[30] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "dr0wned – cyber-physical attack with additive manufacturing," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. Vancouver, BC: USENIX Association, 2017.

[31] A. S. Inc, "Delft dynamics," https://www.delftdynamics.nl/.

[32] D. D. UK, "Net gun x1," https://www.dronedefence.co.uk/products/netgun-x1/.

[33] S. Kamkar, "Skyjack," 2015.

[34] E. Deligne, "Ardrone corruption," *Journal in Computer Virology*, vol. 8, no. 1, pp. 15–27, May 2012.

[35] P. Cabrera, "Parrot drones hijacking," 2018.

[36] N. Rodday, "Hacking a professional drone," *Black Hat Asia*, 2016.

[37] T. Multerer, A. Ganis, U. Prechtel, E. Miralles, A. Meusling, J. Mietzner, M. Vossiek, M. Loghi, and V. Ziegler, "Low-cost jamming system against small drones using a 3d mimo radar based tracking," in *2017 European Radar Conference (EURAD)*. IEEE, 2017, pp. 299–302.

[38] CheckPoint, "Dji drone vulnerability," https://research.checkpoint.com/dji-drone-vulnerability/.

[39] M. A. Fischler and R. C. Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381–395, 1981.

[40] K. Highnam, K. Angstadt, K. Leach, W. Weimer, A. Paulos, and P. Hurley, "An uncrewed aerial vehicle attack scenario and trustworthy repair architecture," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*. IEEE, 2016, pp. 222–225.

[41] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An efficient uav hijacking detection method using onboard inertial measurement unit," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 17, no. 6, p. 96, 2018.

[42] W. G. Aguilar, V. S. Salcedo, D. S. Sandoval, and B. Cobeña, "Developing of a video-based model for uav autonomous navigation," in *Latin American Workshop on Computational Neuroscience*. Springer, 2017, pp. 94–105.

[43] R. Mitchell and R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 5, pp. 593–604, 2014.

[44] ParaZero, "Safeairtm m-200," https://parazero.com/solutions/safeair-for-dji-matrice-200/.

[45] M. Parachutes, "Mars parachutes," https://www.marsparachutes.com/.

[46] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[47] A. Shoufan, "Continuous authentication of uav flight command data using behaviometrics," in *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2017, pp. 1–6.

[48] A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh, and E. Damiani, "Drone pilot identification by classifying radio-control signals," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2439–

2447, 2018.

[49] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn, "Sok: Everyone hates robocalls: A survey of techniques against telephone spam," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 320–338.

[50] E. TEC-SHS, "Technology readiness levels handbook for space applications," 2008.

[51] "Infini dome," https://www.infinidome.com/drone-protection.

[52] C. for the Study of the Drone at Bard College, "Drones at home: Drone incidents: A survey of legal cases," https://dronecenter.bard.edu/files/2017/04/CSD-Drone-Incidents.pdf.

[53] Y. Wang, H. Xia, Y. Yao, and Y. Huang, "Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the us," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 3, pp. 172–190, 2016.

[54] G. Wilkinson, "The machines that betrayed their masters," *Black Hat Asia*, 2014.

[55] E. Group, "Milipol 2017: Eca group unveils its signal intelligence solution for mounting embedded on its aerial," https://www.ecagroup.com/en/business/milipol-2017-eca-group-unveils-its-signal-intelligence-solution-mounting-embedded-its.

[56] Wired, "A drone-flinging cannon proves uavs can mangle planes," https://www.wired.com/story/drone-plane-collision-damage-study/.

[57] Wikipedia, "Gatwick airport drone incident," https://en.wikipedia.org/wiki/Gatwick_Airport_drone_incident.

[58] ——, "List of uav-related incidents," https://en.wikipedia.org/wiki/List_of_UAV-related_incidents.

[59] Reuters, "Greenpeace crashes superman-shaped drone into french nuclear plant," https://www.reuters.com/article/us-france-nuclear-greenpeace/greenpeace-crashes-superman-shaped-drone-into-french-nuclear-plant-idUSKBN1JT1JM.

[60] R. P. Mike Tassey, "Wireless aerial surveillance platform," *DefCon 19*, 2011.

[61] T. Reed, J. Geis, and S. Dietrich, "Skynet: A 3g-enabled mobile attack drone and stealth botmaster." in *WOOT*, 2011, pp. 28–36.

[62] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 2017, pp. 195–212.

[63] J. Toh, M. Hatib, O. Porzecanski, and Y. Elovici, "Cyber security patrol: detecting fake and vulnerable wifi-enabled printers," in *Proceedings of the Symposium on Applied Computing*. ACM, 2017, pp. 535–542.

[64] M. Guri, B. Zadov, and Y. Elovici, "Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2017, pp. 161–184.

[65] B. Nassi, A. Shamir, and Y. Elovici, "Xerox day vulnerability," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 415–430, 2019.

[66] BBC, "Big rise in drone jail smuggling incidents," http://www.bbc.com/news/uk-35641453.

[67] L. A. Times, "Two plead guilty in border drug smuggling by drone," http://www.latimes.com/local/california/la-me-drone-drugs-20150813-story.html.

[68] J. Drozdowicz, M. Wielgo, P. Samczynski, K. Kulpa, J. Krzonkalla, M. Mordzonek, M. Bryl, and Z. Jakielaszek, "35 ghz fmcw drone detection system," in *Radar Symposium (IRS), 2016 17th International*. IEEE, 2016, pp. 1–4.

[69] C. J. Li and H. Ling, "An investigation on the radar signatures of small consumer drones," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 649–652, 2016.

[70] P. Molchanov, R. I. Harmanny, J. J. de Wit, K. Egiazarian, and J. Astola, "Classification of small uavs and birds by micro-doppler signatures," *International Journal of Microwave and Wireless Technologies*, vol. 6, no. 3-4, pp. 435–444, 2014.

[71] Aaronia, "Drone detection system," https://www.aaronia.com/.

[72] Anti-Drone.eu, "Grok," https://anti-drone.eu/.

[73] Aveillant, "Gamekeeper 16u - holographic radar," http://www.aveillant.com/.

[74] B. S. BST, "Uavx," https://www.blacksagetech.com/.

[75] C. speed LLC, "Lightwave radar," http://cspeed.com/.

[76] C. D. Ltd, "Auds," www.chess-dynamics.com/.

[77] DeTect, "Harrier dsr," https://detect-inc.com/.

[78] G. Sensors, "Skylight," https://www.srcinc.com/.

[79] K. H. Limited, "Sharpeve sxv radar," https://www.kelvinhughes.com/.

[80] R. R. Systems, "Elvira," https://www.robinradar.com/.

[81] S. Group, "Giraffe amb radar - elss," https://saabgroup.com/.

[82] SpotterRF, "A2000 radar uavx," https://spotterrf.com/.

[83] Thales, "Squire," www.thalesgroup.com/en.

[84] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, "Improving wifi statistical fingerprint-based detection techniques against uav stealth attacks," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[85] D. Mototolea and C. Stolk, "Detection and localization of small drones using commercial off-the-shelf fpga based software defined radio systems," in *2018 International Conference on Communications (COMM)*. IEEE, 2018, pp. 465–470.

[86] CACI, "Skytracker," http://www.caci.com/.

[87] CerbAir, "Dronewatch," https://www.cerbair.com/.

[88] DeDrone.com, "Dronetracker," https://www.dedrone.com/.

[89] DeTect, "Dronewatcher," https://detect-inc.com.

[90] D. G. Systems, "Sigbase," https://www.digitalglobalsystems.com/.

[91] M. AVISA, "Skysentry amms," microflown-avisa.com/.

[92] M. Solutions, "Drone detection and classification system," https://www.mistralsolutions.com/.

[93] Rinicom and M. Aerospace, "Skyperion," http://

metisaerospace.com/skyperion-counter-uav/.
[94] R. . Schwarz, "R&s ardronis-i," https://www.rohde-schwarz.com.
[95] Sensofusion, "Airfence," https://www.sensofusion.com/.
[96] T. International, "Blackbird," https://www.tcibr.com/.
[97] A. Rozantsev, V. Lepetit, and P. Fua, "Flying objects detection from a single moving camera," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 4128–4136.
[98] S. Hu, G. H. Goldman, and C. C. Borel-Donohue, "Detection of unmanned aerial vehicles using a visible camera system," *Applied optics*, vol. 56, no. 3, pp. B214–B221, 2017.
[99] A. Rozantsev, S. N. Sinha, D. Dey, and P. Fua, "Flight dynamics-based recovery of a uav trajectory using ground cameras," in *Conf. Comp. Vision and Pattern Recognition*, 2017.
[100] H. infrared systems, "Uav detection and tracking," https://www.hgh-infrared.com/.
[101] MAGNA, "Drone detection," https://magnabsp.com.
[102] Rinicom, "Sky patriot," www.rinicom.com/.
[103] T. Müller, "Robust drone detection for day/night counter-uav with static vis and swir cameras," in *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*, vol. 10190. International Society for Optics and Photonics, 2017, p. 1019018.
[104] G. C. Birch and B. L. Woo, "Counter unmanned aerial systems testing: Evaluation of vis swir mwir and lwir passive imagers," 2017.
[105] DroneShield, "Faralert/widealet sensors," https://www.droneshield.com/.
[106] P. Church, C. Grebe, J. Matheson, and B. Owens, "Aerial and surface security applications using lidar," in *Laser Radar Technology and Applications XXIII*, vol. 10636. International Society for Optics and Photonics, 2018, p. 1063604.
[107] 3DEO, "Rogue drone detection and mitigation," https://3deo.biz/applications/drone-detection-and-mitigation.
[108] Q. Systems, "Q-guard - lidar x-drone," https://quanergy.com/.
[109] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher, "Real-time uav sound detection and analysis system," in *Sensors Applications Symposium (SAS), 2017 IEEE*. IEEE, 2017, pp. 1–5.
[110] J. Mezei and A. Molnár, "Drone sound detection by correlation," in *Applied Computational Intelligence and Informatics (SACI), 2016 IEEE 11th International Symposium on*. IEEE, 2016, pp. 509–518.
[111] M. Benyamin and G. H. Goldman, "Acoustic detection and tracking of a class i uas with a small tetrahedral microphone array," ARMY RESEARCH LAB ADELPHI MD, Tech. Rep., 2014.
[112] X. Chang, C. Yang, J. Wu, X. Shi, and Z. Shi, "A surveillance system for drone localization and tracking using acoustic arrays," in *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*. IEEE, 2018, pp. 573–577.
[113] ORELIA, "Drone-detector," http://www.drone-detector.com/en/.
[114] S. Technology, "Discovair," www.sqhead.com/.
[115] H. Liu, Z. Wei, Y. Chen, J. Pan, L. Lin, and Y. Ren, "Drone detection based on an audio-assisted camera array," in *Multimedia Big Data (BigMM), 2017 IEEE Third International Conference on*. IEEE, 2017, pp. 402–406.
[116] J. Busset, F. Perrodin, P. Wellig, B. Ott, K. Heutschi, T. Rühl, and T. Nussbaumer, "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*, vol. 9647. International Society for Optics and Photonics, 2015, p. 96470F.
[117] M. Peacock and M. N. Johnstone, "Towards detection and control of civilian unmanned aerial vehicles," 2013.
[118] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu, "Matthan: Drone presence detection by identifying physical signatures in the drone's rf communication," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2017, pp. 211–224.
[119] Y. Yao, H. Xia, Y. Huang, and Y. Wang, "Privacy mechanisms for drones: Perceptions of drone controllers and bystanders," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 6777–6788.
[120] "Dji aeroscope," https://www.dji.com/aeroscope.
[121] C. Ruiz, S. Pan, A. Bannis, X. Chen, C. Joe-Wong, H. Y. Noh, and P. Zhang, "Idrone: Robust drone identification through motion actuation feedback," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 2, pp. 80:1–80:22, Jul. 2018.
[122] DroneShield, "Dronegun," https://www.droneshield.com/dronegun-tactical/.
[123] R. Hill, "Block 3 dronebuster and dronebuster-le," http://flexforce.us/counter-uas/dronebuster/.
[124] Bilghter, "Auds," http://www.blighter.com/products/auds-anti-uav-defence-system.html.
[125] MCTECH, "Mc-horizon," http://mctech-jammers.com/products/mc-horizon.html.
[126] G. F. Above, "Drone hunting eagles," www.guardfromabove.com.
[127] Raytheon, "Beam on," https://www.raytheon.com/news/feature/beam-on.
[128] MBDA, "Laser effector," https://www.mbda-systems.com/innovation/preparing-future-products-3/high-energy-laser-weapon-systems/.
[129] M. Saqib, S. D. Khan, N. Sharma, and M. Blumenstein, "A study on detecting drones using deep convolutional neural networks," in *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 2017, pp. 1–5.
[130] Anti-Drone.eu, "droneshield," https://anti-drone.eu/.
[131] FAA, "Uas remote identification," https://www.faa.gov/uas/research_development/remote_id/.