

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2020.DOI

# Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems

HONGGU KANG<sup>1</sup>, (Student Member, IEEE), JINGON JOUNG<sup>2</sup>, (Senior Member, IEEE), JINYOUNG KIM<sup>3</sup>, (Member, IEEE), JOONHYUK KANG<sup>1</sup>, (Member, IEEE), and YONG SOO CHO<sup>2</sup>, (Member, IEEE)

<sup>1</sup>Department of Electrical Engineering, KAIST, Daejeon 34141, South Korea

<sup>2</sup>School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, South Korea

<sup>3</sup>Korea University Business School, Seoul 02841, South Korea.

Corresponding author: J. JounG (e-mail: jgjounG@cau.ac.kr).

Manuscript received Month 00, 2020; revised Month 00, 2020; accepted Month 00, 2020. This research was supported in part by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIT) (2018R1A4A1023826) and in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-0-01787) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation)

**ABSTRACT** Recognizing the various and broad range of applications of unmanned aerial vehicles (UAVs) and unmanned aircraft systems (UAS) for personal, public and military applications, recent un-intentional malfunctions of uncontrollable UAVs or intentional attacks on them divert our attention and motivate us to devise a protection system, referred to as a counter UAV system (CUS). The CUS, also known as a counter-drone system, protects personal, commercial, public, and military facilities and areas from uncontrollable and belligerent UAVs by neutralizing or destroying them. This paper provides a comprehensive survey of the CUS to describe the key technologies of the CUS and provide sufficient information with which to comprehend this system. The first part starts with an introduction of general UAVs and the concept of the CUS. In the second part, we provide an extensive survey of the CUS through a top-down approach: i) the *platform* of CUS including ground and sky platforms and related networks; ii) the *architecture* of the CUS consisting of sensing systems, command-and-control (C2) systems, and mitigation systems; and iii) the *devices and functions* with the sensors for detection-and-identification and localization-and-tracking actions and mitigators for neutralization. The last part is devoted to a survey of the CUS *market* with relevant challenges and future visions. From the CUS market survey, potential readers can identify the major players in a CUS industry and obtain information with which to develop the CUS industry. A broad understanding gained from the survey overall will assist with the design of a holistic CUS and inspire cross-domain research across physical layer designs in wireless communications, CUS network designs, control theory, mechanics, and computer science, to enhance counter UAV techniques further.

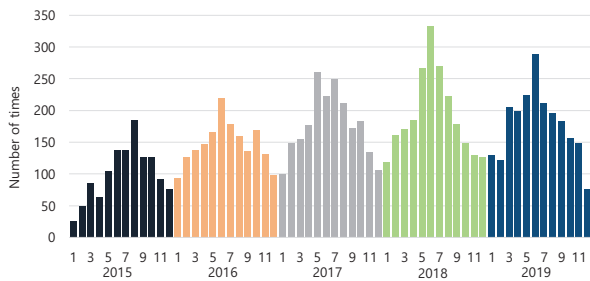
**INDEX TERMS** Unmanned aerial vehicle (UAV), unmanned aircraft system (UAS), counter UAV system (CUS), counter drone systems, public safety, defense.

## I. INTRODUCTION

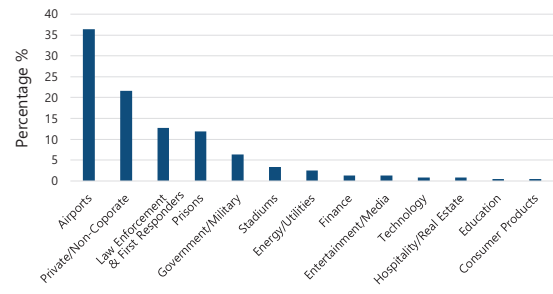
Given the various practical and potential applications and purposes behind the use of unmanned aerial vehicles (UAVs) and unmanned aircraft systems (UAS) from non-public hobbies to military purposes, UAVs and UASs have been rigorously studied and developed over the last 30 years. Currently, in real life, we can readily observe various public and non-public use cases of UAVs, also widely known as drones. In this paper, UAV is used as a general term for unmanned aircraft, including remotely

piloted aircraft controlled by an operator on the ground and drones that can fly autonomously [1]. Though the word 'drone' can be used to describe a wide variety of vehicles, including even seafaring submarines and land-based autonomously vehicles, UAVs (or UASs) and drones are used interchangeably throughout the paper. Moreover, the UAS, which consists of a UAV and the controllers, is also used interchangeably with UAV.

## A. MOTIVATIONS



**FIGURE 1.** Number of incidents caused by UAVs in the United States from January of 2015 to December of 2019, as reported to the FAA in the US [12]



**FIGURE 2.** Industries affected by UAV incidents across the globe, as reported in online news articles between December of 2018 to March of 2020 and collected in earlier work [39]

### 1) Rapid Growth of UAVs and Their Applications

Applications of UAVs range from recreation to commercial and military applications, including enjoyment, hobbies, and games with drones, the filming of movies for recreation [2]–[4], and the operation of UAVs for military purposes [5]–[11]. As reported by the federal aviation administration (FAA) in the United States (US), there are 1,692,700 registered drones (approximately, 29% for commercial and 71% for recreation) in the US as of September 2020 [12]. The commercial UAV industry, whose dynamics has been dubbed a modern-day gold rush by multiple industry players [13], has grown rapidly in tandem with expanding market needs, such as disaster management, emergency services, agricultural applications, cargo inspection, or recreational purposes, to name a few. Clearly, UAVs are considered as an essential enabler to enlarge commercial markets and are used in various industries, such as in i) the agricultural industry for seeding, cross-pollination, and crop-dusting [14], [15]; ii) the distribution industry for the delivery and/or collection of packages [16]–[19]; iii) the construction industry for building and measuring [20], [21]; and, iv) the information technology (IT) industry for enlarging service coverage areas and establishing emergency networks [22]–[27]. Furthermore, UAVs are used to provide effective public services, such as environmental (e.g., traffic and air pollution) monitoring [28]–[30] and firefighting and rescue operations [31].

### 2) Rapid Growth of Accidents and Crimes Involved in UAVs

With the various and vigorous promising applications of UAVs, now is a suitable time to consider UAVs from a different angle considering the possibility that they may threaten our safety. At a 2013 campaign rally in Dresden, Germany, a quadcopter drone hovered within a few feet of Angela Merkel, the Chancellor of Germany, and Thomas Maiziere, the German Defense Minister, eventually crashing in front of Merkel [32]. This harmless stunt was found to have been orchestrated by the Pirate Party in the form of a protest against drone observation

and government surveillance in Germany. The White House has not remained exempt from threats of rogue drones either; a DJI quadcopter for recreational purposes accidentally crash-landed on the south lawn of the White House in 2015 [33]. The benign nature in these cases, however, was not replicated in subsequent incidents. About a year and a half later, a Japanese protester against the use of nuclear power managed to land a drone, marked with an odious radioactive sign, on the roof of the Japanese prime minister’s office [34]. The drone was carrying a container filled with radioactive sand from Fukushima. Multiple major news outlets have started to voice serious concerns over hostile drones (e.g., [35], [36]). Recently, hostility by malignant drones became apparent to the general public when Nicolas Maduro, the President of Venezuela, was attacked by two commercial drones, each of which contained one kilogram of C-4 explosive, in Caracas, Venezuela, in August of 2018 [37]. This series of drone attacks on a head of state captured only a fraction of the negative externalities of the booming UAV industry. Rogue drones hovering over airports or private compounds pose diverse ranges of threats from security to privacy. Stealth drones deliver contraband by dropping packages onto prison grounds. Concerns over potential threats by UAVs have materialized quickly.

Furthermore, according to a survey of online news articles, there were more than 200 incidents (100 in North America, 77 in Europe, 38 in Asia/Pacific, 17 in the Middle East, and 6 in Latin America) in 2019 [38]. As also shown in Fig. 1, the number of incidents that are caused by UAVs, as reported to the FAA in the US [12], generally increases every year. Compared to the total number of incidents in 2015, i.e., 1,213, this number increased by 76% to 2,142 in 2019.

On the other hand, because UAVs have multidirectional purposes, their negative effects are also extensive. For example, UAVs disturb current aviation operations, invade personal privacy, and threaten public and national safety. Based on data, collected from online news articles between December of 2018 and March of 2020 [39],

the industries affected by the UAV-related incidents were determined. These are categorized in Fig. 2. As verified in the analysis, UAVs affect various industries; in particular, the majority of incidents occur at airports, at a rate of approximately 35%. An accident at an airport can cause serious disasters and even fatalities, posing therefore a threat to both human life and property.

### 3) Lack of Studies and Surveys on Counter UAV Systems

To mitigate such alarming effects caused by UAVs, governments regulate UAV operations via civil aeronautics laws irrespective of the *operators* and *operation* [40]–[44]. For the operators, a legal license, insurance, and registration are required. For example, 171,744 licenses have been issued as of March of 2020 in the US [12]. With regard to operational regulations, an authorized private/public office controls and restricts UAV operations by setting limits on the maximum operation speed and height, locations, behaviors, and communication frequency bands. However, because the current regulation passively controls UAV operations, it does not guarantee privacy and safety from uncontrollable UAVs, e.g., those with unintentional malfunctions owing to a connection loss by the operator and the UAVs of the illegal intruders who attempt to attack public and military facilities. In keeping with the rapid development of UAV technologies, the resultant threat from uncontrollable UAVs is inevitable. Therefore, to secure personal privacy, commercial, public, and military facilities and areas from uncontrollable and belligerent UAVs, i.e., malicious UAVs (mUAVs)<sup>1</sup>, a protection system, referred to here as a *counter UAV system (CUS)*, also known as (a.k.a.) a counter-drone system [38], is desired.

Compared to the regular aircrafts, the UAVs, in general, have unique characteristics. For example, UAVs are unmanned, inexpensive/affordable, fly at low altitudes with slow speed, and have limited payload. Therefore, the UAVs can reasonably (re)modeled to mUAVs, and the mitigators against mUAVs are required to be studied separately from the existing studies for the defense of the regular airplanes. The in-depth and large-scale surveys of CUS, however, are lack and the current surveys have been performed covering only a part of CUS as summarized in Table 1 [45]–[52]. On the other hand, in this survey, we provide a comprehensive survey for designing holistic CUS that includes platform, architecture, devices, and their functions for CUS. The CUS platforms will be categorized according to the mobility and operating area. The CUS architecture including various sensing, command and control (C2), and mitigation systems will be surveyed with the specific functions and devices. Furthermore, the challenges and vision of the related market will be provided. To the best of our knowledge, this study is the

<sup>1</sup>Throughout the paper, uncontrollable and belligerent UAVs, including intrusion UAVs and hostile UAVs, are referred to as mUAVs.

**TABLE 1. Relevant Surveys and Studies on CUS**

Ref.	Focus
[45]	Performance evaluation of visible, short-, mid-, and long-wave infrared sensors for UAV detection
[46]	UAV detection, identification, and countermeasures
[47]	UAV detection and classification utilizing radar, electro-optical/infrared and acoustic sensors
[48]	Surveillance technologies and commercial anti-drone systems
[49]	Cyber/physical threats from/to UAVs and a few technologies for detection, tracking, and interdiction
[50]	Proposal of a drone surveillance framework and a few enabling technologies for the framework
[51]	Cyber and physical threats against civilian UAVs
[52]	UAV detection for airport protection
This survey	Comprehensive survey for designing holistic CUS: Platforms, architectures, devices and functions, and market overview

first work that comprehensively surveys on the CUS as summarized in the following subsection.

### B. ORGANIZATION AND CONTRIBUTIONS OF THIS SURVEY

The acronyms frequently used in the paper and the taxonomy of our survey on the CUS are shown in Tables 2 and 3, respectively. Table 3 contains five columns for the survey topics, subtopics, category, examples/descriptions with pros and cons, and references. The main survey consists of three parts from Section II to Section VI with the following five topics: i) UAV applications and regulations; ii) platforms and networks of the CUS; iii) the CUS architecture; iv) devices and functions of the CUS; and v) markets, challenges, and the future vision of the CUS.

- The first part, i.e., Section II, is an introductory part that briefly introduces the various UAV applications and regulations for operators and operations. Moreover, the necessity of the CUS is justified by introducing the concept of the CUS.
- In the second part, the CUS is rigorously surveyed throughout Sections III, IV, and V through a top-down approach from the platform to the architecture of the CUS followed by the devices and functions of the CUS. In Section III, the CUS platform is introduced and categorized into three parts based on the operation methodologies as follows: i) the ground platform, i.e., the main platform accounting for approximately 90% of CUS platforms and operated on the ground in static, mobile, and handheld manners; ii) the sky platform, approximately 10% of all platforms and operated at low or high altitudes; and iii) the CUS networks that link multiple platforms. In Section IV, the CUS architecture is surveyed with related topics, specifically, sensing systems, command-and-control (C2) systems, and mitigation systems. The sensing systems gather

TABLE 2. Acronyms / Abbreviations Used in This Paper (Alphabetic order)

Acronym	Full name	Acronym	Full name	Acronym	Full name
A2A	Air-to-air	GNSS	Global navigation satellite systems	pUAV	Pursuer UAV
A2G	Air-to-ground	GPS	Global positioning system	RCS	Radar cross-section
AoA	Angle of signal arrival	H2A	Hard to access	RF	Radio frequency
BS	Base station	IMU	Inertial measurement unit	RTH	Return to home
BVLoS	Beyond visual line of sight	IoT	Internet-of-things	RTof	Round-trip ToF
C2	Command and control	IR	Infrared	SDN	Software-defined networking
CAGR	Compound annual growth rate	IT	Information technology	SME	Small- and medium-sized enterprise
CNN	Convolutional neural network	JDL	Joint directors of laboratories	SVM	Support vector machine
CUS	Counter UAV system	LiDAR	Light detection and ranging	SWAP	Size, weight, and power
CW	Continuous wave	LoS	Line-of-sight	TDoA	Time difference of arrival
DFIG	Data fusion information group	MAC	Media access control	ToF/ToA	Time of flight/arrival
DoD	Department of defense	MANET	Mobile ad hoc network	UAS	Unmanned aircraft system
EM	Electromagnetic	MDS	Micro-Doppler signature	UAV	Unmanned aerial vehicle
EMP	Electromagnetic pulse	mUAV	Malicious/malignant/misapplied UAV	UWB	Ultra wideband
EO	Electro-optical	NFV	Network function virtualization	UCAV	Unmanned combat aerial vehicles
FAA	Federal aviation authority	NLoS	Non-line-of-sight	VANET	Vehicle ad hoc network
FANET	Flying ad hoc network	PE	Pursuit-evasion	VLoS	Visual line of sight

TABLE 3. Overview of the Survey

Topic	Subtopic	Category	Examples/Description with Pros (o) & Cons (x)	References
UAV Applications & Regulations (Sec. II)	Applications of Commercial UAVs (Sec. II-A)	1) Military applications 2) Civilian-noncommercial 3) Civilian-commercial	• Reconnaissance, surveillance, target acquisition, mine countermeasures, relay • Monitoring, relief activities • Agriculture, construction, delivery, entertainments, IT services, science	Tab. 4
	Regulations (Sec. II-B)	1) Regulation on operators 2) Regulation on operation 3) Regulation violation	• License, insurance, training • Maximum height and speed, regional restriction, frequency band • Accidents, non-violent crimes, violent crimes	Tab. 5
Platforms & Networks of CUSs (Sec. III)	Ground Platform (Sec. III-A)	1) Static 2) Mobile 3) Human-packable	• (o) Precise, (x) vulnerable to unexpected threats • (o) On-demand & flexible deployment, (x) Insufficient developed • (o) Portable, lightweight (x) Limited performance	Fig. 3
	Sky Platform (Sec. III-B)	1) Low altitude 2) High altitude	• Cost-effective system below a few km, (o) rapid deployment • Costly system below tens of km, (o) wide coverage	Fig. 4 Fig. 5
	CUS Network (Sec. III-C)	1) Centralized networks 2) Decentralized networks	• High-performance central platform supporting low-performance platforms • Homogeneous platforms and heterogeneous platforms	
Architecture of CUSs (Sec. IV)	Sensing systems (Sec. IV-A)	1) Sensing systems 2) Data fusion	• Sound wave data, radio wave data, light wave data • Source information, data types, JDL levels, and centralization levels	
	C2 systems (Sec. IV-B)	1) Orchestration 2) Computing	• Procedure of integrated CUS • Centralized/decentralized computing	Fig. 6
	Mitigation systems (Sec. IV-C)	Neutralizing methods: Disruption, disabling, destroying, control, providing the alternate flight instructions		
Devices & Functions of CUSs (Sec. V)	Sensors (Sec. V-A)	1) Sound waves 2) Radio waves 3) Light waves	• (Sonar) sensors, acoustic sensors, ultrasonic sensors • RF sensors, Radar • EO/IR, LiDAR	Fig. 7 Tab. 6
	Mitigators (Sec. V-B)	1) Non-Physical mitigators 2) Physical mitigators	• RF/GNSS jamming, high-power electromagnetics, spoofing, laser • projectile, collision UAVs, nets, eagles	Tab. 7
CUS Market (Sec. VI)	Market dynamics (Sec. VI-A)	Dancing landscape of the global CUS market: What does it look like and how is it changing? Market size and growth, geographic composition, market growth drivers/inhibitors, market fragmentation		Fig. 8 Tab. 8
	Incumbents (Sec. VI-B)	Game of drones: Who are the current major players in the civilian CUS market? Global established corporations, regional SME, SME partnerships and acquisition		Tab. 9 Fig. 9
	Challenges & Future Direction (Sec. VII)	CUS Networks (Sec. VII-A)	Integrated CUS network and its optimization are required. Software-defined networking (SDN) and network function virtualization (NFV) technologies can be used	
Assessment Criteria (Sec. VII-B)	Various assessment criteria are proposed: mUAV neutralization probability (mUNP), expected loss of profit (ELP), covering space per cost (CSC), mitigation completion time (MCT), mitigation completion power (MCP) capacity of mitigation (COM), mitigation cycle of CUS (MCC), and operating duration of CUS (ODC)			
	Technol. Challenges (Sec. VII-C)	Technological challenges and strategies to overcome challenges: i) fundamental framework and prototype, ii) dynamic & flexible CUS networks, iii) data fusion, iv) automation & fast computation, v) tracking, and vi) price reduction		
Market vision (Sec. VII-D)	Yin and Yang of the CUS industry: What are the lessons for adjacent market players? Asymmetric interdependence between the UAV and CUS industries, temporal precedence of UAVs, and potential CUS saturation			Tab. 10

data from the environments. The C2 systems perform computing tasks, such as detection, identification, tracking, and localization, and determine false alarms, establishing whitelists/blacklists, and setting neutralizing methods according to the threat level. The mitigation systems neutralize mUAVs. Section V introduces the sensors and mitigators with their functions performed by the architecture topics of CUSs at the device level. Here, various sensors, such as radar, radio frequency (RF) sensors, light detection and ranging (LiDAR), electro-optical (EO)/infrared (IR) sensors, sound navigation ranging (sonar), and acoustic/ultrasonic sensors, and mitigation devices (including lasers, projectiles, collision UAVs, jammers, electromagnetic pulses (EMPs), spoofing/hacking devices, and nets) are briefly surveyed and their limitations and requirements for the CUS are discussed.

- In the last section, the current trends and distinctive characteristics of the CUS market are identified to help readers understand the industrial and geographical distributions of the current CUS market, both the drivers and inhibitors of the CUS market growth, and the major players and their competitive yet cooperative dynamics in the CUS market. Also, highly distinctive characteristics of the CUS market are identified as the asymmetric interdependence between the UAV and CUS industries, the temporal precedence of the UAV industry, and the complete dependence of the CUS market demise on both regulatory changes and the growth rate of the UAV industry.

The broad understanding gained from this survey will help design a holistic CUS to neutralize/destroy mUAVs and mitigate this threat by aspiring cross-domain research across physical layer designs in wireless communications, UAV network designs, control theory, mechanics, and computer science.

## II. UAV APPLICATIONS AND REGULATIONS

Recently, the commercial UAV market has grown gradually and applications of UAVs have broadened from their typical military purpose to various purposes as the cost of UAV systems decreases. With the explosive growth of UAVs, injuries and manual physical labor in the military and in industry have been reduced, and various leisure activities have newly appeared given the mobility and flexible operations of UAVs. On the other hand, the increased number of UAV applications has also caused concern about potential accidents and crimes. To prevent the misuse of UAV systems and illegal operations, regulations pertaining to UAVs have been established in many countries. However, such regulations have a fundamental limit in that they cannot actively control accidents and illegal operations, and the potential threat of mUAVs remains. Therefore, an active defense system,

i.e., the aforementioned CUS, is desired. In this section, applications of UAVs and pertinent regulations are briefly introduced to clarify the motivation of this CUS survey, followed by the concept of the CUS. A comprehensive survey of the CUS will be provided after this section.

### A. UAV APPLICATIONS

The main applications are categorized into military applications, civilian-noncommercial (i.e., public) applications, and civilian-commercial applications, including industry and personal applications, as summarized in Table 4. Various applications in each category are introduced below.

#### 1) Military Applications

UAVs have been deployed in various military missions/operations, such as intelligence, surveillance, target acquisition, reconnaissance (ISTAR), combat, and communications [5]–[11], [53]–[56]. UAVs equipped with multiple sensors, e.g., EO/IR and acoustic sensors, can complete important reconnaissance and surveillance missions. Exploiting multiple sensors on UAVs, useful information can be collected during surveillance, target acquisition, and reconnaissance, and can then be processed to make the better battle plans, with one example being ISTAR. Using advanced communication technology, multiple drones can cooperate to complete a military mission, such as video reconnaissance [56]. Exploiting the relatively small form factor of mini UAVs compared to a human-scale aircraft enables concealable countermeasures such as radar and communication jammers [10]. In addition, a mid-size unmanned combat aerial vehicle (UCAV) or a combat drone can carry aircraft ordnance, such as missiles and/or bombs, and can be used for drone strikes [53]. For an effective attack, the sufficient accuracy of detection and identification of the target location, i.e., target acquisition, are required. The small UAV can also be used to detect and eliminate land mines. Additionally, a UAV that operates as a base station (BS) or relay station can enlarge the communication coverage area on a battlefield, where a BS is unavailable, such that emergent and short-time communications become possible [5], [54]–[56].

#### 2) Civilian-Noncommercial Applications

The civilian-noncommercial applications of a UAV cover a wide area, from public services to scientific research [28]–[31], [57]–[60], [81]–[83].

- **Monitoring:** A UAV can fly and hover around hard-to-access (H2A) or dangerous places, where monitoring is necessary for safety, comfort, and scientific purposes. For example, government facilities and public infrastructure elements covering a wide area are challenging for a person to monitor completely using a fixed camera or a simple patrol strategy.

TABLE 4. Applications and Functions of UAVs

Applications	Categories	Description & Examples	References
Military	ISTAR	Intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) via UAVs	[6]–[9]
	Combat	Unmanned combat aerial vehicles (UCAV) or combat drone with aircraft ordnance, such as missiles, bombs, or jamming devices, collision drones, and mine countermeasures	[10], [11], [53]
	Communications	UAVs that operate as a base station and relay station to enlarge the coverage area	[5], [54]–[56]
Civilian-Noncommercial	Monitoring	Low-cost real-time monitoring, wide-area monitoring at a glance, and remote research at H2A places, such as contaminated sky areas and active volcanoes	[28]–[30], [57], [58]
	Relief activities	Quick investigation of the scene of a fire using a small-size UAV, prompt reporting at the location of accident, and fumigation using UAVs	[31], [59], [60]
Civilian-Commercial	Agriculture	Soil and field analyses, seeding, planting, monitoring crop growth, cross-pollination, irrigation, and health assessment and crop-dusting	[14], [15], [61], [62]
	Construction	Land surveys, safety monitoring, protection of construction sites, inspections to prevent numerous dangers and safety hazards through 3D mapping, and video footage	[20], [21]
	Delivery Services	Transferring medicines and vaccines, packages, food, and other small goods into out of remote or H2A regions	[16]–[19], [63]–[65]
	Recreation	Film creation, photography, racing, and commercial advertisements, and DIY HW/SW	[2]–[4], [66]
	IT services	UAVs as BSs, relays, and data correctors for enhancing the quality of IT services using, e.g., broadband communication systems, IoT systems, and cellular systems	[22]–[27], [43], [67]–[80]

UAVs, however, can monitor a complete area at a glance from the sky or a specific spot while flying at that spot, meaning that they can cover a target area without blind and/or occluded spots. UAVs can patrol to monitor and detect instances of spontaneous combustion at a relatively low cost. They can also be applied to the real-time monitoring of vehicle density levels to collect traffic information [29], [81]. Note that conventional fixed surveillance cameras can monitor only a part of the road. Though helicopters with cameras can obtain footage of roadways much more freely, the operation cost is extremely high. UAVs can resolve such mobility and operation cost issues and collect useful information, such as detour routes, so that drivers can avoid traffic jams or accidents. In addition, UAV monitoring can also be used for scientific purposes, e.g., for air pollution measuring [30] and for monitoring the status of active volcanos [28].

- **Relief activities:** Other important public applications of UAVs are relief activities. Bulky pieces of equipment, such as helicopters and fire trucks, cannot easily reach a building/house fire in urban areas due to various obstacles and traffic. Moreover, firefighters may not even be allowed to enter the building/house due to the possibility of a fatal collapse. Under such an emergent situation, a UAV can be serve as a lifesaver owing to its small size and mobility, which enables it to readily enter such buildings, quickly investigate the situation, and report the circumstances inside. A UAV equipped with the ability to spray water can also extinguish fires at critical spots, such as at gas tanks and ignition points, immediately without direct human control [31]. A UAV can also conduct

rescue missions by probing H2A places, reporting the locations of accidents, and comforting victims after spotting them [59]. A fumigator UAV to fight pandemics and epidemics is another important relief activity of a UAV. For instance, fumigator drones were deployed to prevent the spread of diseases, i.e., such as the coronavirus (COVID-19) in South Korea early 2020 [60]. Fumigator drones spray disinfectants over a vast area in a short time, requiring the least amount of manpower. Moreover, disinfectants sprayed via a UAV can easily fumigate blind spots that are normally difficult to reach by human hands. Note that using fumigator drones for the prevention of epidemics is controversial because the effectiveness of this strategy depends on the type of virus and whether the contagion can spread aurally, yet fumigator drones will be further developed and widely used owing to their potential benefits in this area.

### 3) Civilian-Commercial Applications

Various industries from large companies to small start-up companies exploit the benefits of UAV to increase their profit. Although the commercial/industrial use of UAVs is relatively new compared to military uses, there are a wide variety of civilian-commercial applications [82], [83].

- **Agriculture:** To increase crop yields, UAVs can assist in farming industries or can help farmers complete various tasks, such as soil and field analyses, seeding, planting, monitoring crop growth, cross-pollination, irrigation, health assessments, and crop-dusting [14], [15], [61], [62]. Here, an essential technology enabling many of the agricultural tasks of UAVs is the sensing capability of UAVs. By detecting and

tracking topographical and geographical variations using EO/IR sensors and LiDAR, UAVs can avoid collisions and create efficient schedules of flight routes. Moreover, various sensors, such as hyperspectral, multispectral, or thermal sensors, are required to monitor humidity levels and temperatures.

- **Construction:** UAVs have already begun to be used in the construction industry, reducing much human effort as well as errors associated with traditional constructing tasks [20], [21]. For example, UAVs can survey land from the perspective of drones, monitor the safety of the laborers, protect construction sites from theft or vandalism, inspect numerous dangers and safety hazards through three-dimensional (3D) mapping, and provide video footage to facilitate communications and surveillance. In such cases, along with the sensing capability, which is the essential technology of agricultural UAVs, the communication capability should be emphasized as an essential technology as well, enabling the advantages of UAVs at construction sites. Very low-latency communication is essential for construction UAVs to prevent accidents at construction sites. To this end, 5G/beyond 5G (B5G) technology can be applied to these UAVs. The 3GPP Working Groups ensure that the 5G system will meet the connectivity needs of UASs [84]. Considering the UAVs as an invaluable tool in construction, UAVs will take on even more integral and complex tasks associated with large projects in the future.
- **Delivery service:** UAVs can be used to transport lightweight medicines and vaccines, packages, food, and other small goods into or out of remote or otherwise inaccessible regions (i.e., an H2A region). For example, UAVs can transport medicines and vaccines into H2A regions [63], [64]. They can also retrieve medical samples from an H2A region. Many postal companies from the US, Australia, Switzerland, Germany, Singapore, and Ukraine have tested the feasibility and profitability of courier services using UAVs [65]. Food delivery UAVs, specifically rotary-wing types, have also been demonstrated by many companies involved in the foodservice industry. Because UAVs are a power-limited system, to complete their delivery services given their limited battery power or fuel (e.g., Amazon 'Prime Air' carrying a package up to approximately 2 kg with a 13-min flight time to the destination [85]), delivery path optimization and UAV status monitoring methods have been studied [16]–[19]. Before the expected widespread usage of UAVs as couriers in the future, appropriate regulations should be established to overcome safety and legal hurdles and prevent their potential illegal use, as reported in Section I.
- **Recreation:** Diverse UAVs ranging from low-cost toys to expensive high-end products for civilian applica-

tions such as filmmaking, photography, racing, and commercial advertisements, are easy to find in society at present. Depending on the application type, many key technologies are involved. Controlling the 1,218 UAVs performing the light show at opening ceremony of the Olympic Winter Games PyeongChang, South Korea, in 2018 required seamless control technology and communications technology to provide the massive number of connections between the UAVs and a control center to keep them all airborne simultaneously [86]. Taking video and photos using UAVs requires stabilizer technology to obtain a clear shot from the UAVs [2]. In addition, customizing the software and hardware of UAVs, as is done with what are termed do-it-yourself (DIY) UAVs, and flying and controlling UAVs during races have become a type of e-sport recently. For example, in the global drone racing league MultiGP, which started in 2015 [66], a pilot controls the UAV by observing footage from a camera mounted on the UAV with the signal sent to goggles or a monitor worn by the pilot, i.e., a first-person view (FPV) or 'video flying'. Here, efficient image processing and communication technologies are required for seamless and high-quality video streaming (typically a frequency of 2.4 GHz or 5.8 GHz). Like a traditional robot maze competition, a UAV race can serve to evaluate and validate a learning algorithm to determine optimal paths in the sky [3], [4]. For personal recreation purposes, the pilots of UAVs should recognize and follow the regulations and practice basic courtesy to ensure public safety and privacy.

- **IT services:** As one of the most promising applications of commercial UAVs is to provide IT services, where the UAV operates as, for example, a BS, relay, and/or data corrector from sensors, to enhance the quality of IT services. Especially in relation to wireless communications, there have been many comprehensive surveys of how wireless communications can be enhanced by UAVs (e.g., [25], [43], [67]–[71], [73]–[77], [80] for communication applications aided by UAVs and the references therein.). Examples include broadband communications [67], internet-of-things (IoT) applications [70], [72], communication platforms depending on the altitude of UAVs [74], wireless channel models involved in UAV communications [75], [76], cellular systems supported by UAVs [43], [77], and data links [80]. To enhance the many wireless communication applications, rigorous and various, technical and theoretical studies have been conducted to find the optimal designs of the parameters involved in UAV communications, such as the trajectory and placement of UAVs [22]–[24], [26], [27], [78], [79], resource usage (e.g., power and time) [27], [87]–[89], and proper topologies [90], [91].

**TABLE 5. Regulations on Commercial UAVs in 20 countries and Violation Consequences [40]–[44]**

Class	Various Contents of Regulations & Violation Consequences
Regulation on Operators	<ul style="list-style-type: none"> <li>• Pilot license and insurance are mandatory for operators if the weight of the UAV exceeds a certain standard or if UAVs are operated in populated areas</li> <li>• Training is required for BVLoS operation</li> <li>• Re-evaluation of pilot competency is required regularly</li> </ul>
Regulation on Operation	<ul style="list-style-type: none"> <li>• Conditions on security of sight: daytime, good weather, VLoS, BVLoS with a collision-avoidance function</li> <li>• Limits of functions/operations: maximum weight, height, and speed of UAVs, maximum distance between the UAV and pilot</li> <li>• Restrictions on region: minimum distance from certain objects, such as airspace, aircrafts, vehicles and people, and certain areas, such as national properties, military bases, airports, and populated areas</li> <li>• UAV data communications should be conducted within certain a frequency band</li> <li>• Interfering and disturbing law enforcement are restricted</li> <li>• Loading, carrying, or dropping any cargo or hazardous items by a UAV is restricted</li> </ul>
Regulation Violation	<ul style="list-style-type: none"> <li>• Accidents that are unintentionally caused by an unskilled pilot and unexpected changes of weather phenomena</li> <li>• Non-violent crimes caused by a misapplied UAV, such as a privacy intrusion, data robbery, and illegal delivery</li> <li>• Violent crime is closely related to political and military issues, such as terrorism</li> </ul>

## B. REGULATION PERTAINING TO UAV OPERATIONS

As introduced in the previous subsection, numerous applications of UAVs have been introduced or will eventually be introduced, with enormous benefits. Various incidents, however, accompanied by the increase in UAV-aided services and technologies will also increase, as stated in Section I. To prevent unwanted incidents caused by UAVs, regulations on commercial UAVs have been established in many countries [40]–[43], [80], [92]. The details of these regulations vary from country to country. For example, a pilot license is mandatory for operation in some countries, e.g., the US, China, and the United Kingdom (UK), though not all. In South Korea and Australia, a pilot license is required only if the weight of the drone exceeds a specified standard. The aviation authorities of 132 countries all across the globe have also created regulations [44]. Although regulations vary widely among countries, their common purpose is to prevent unwanted incidents stemming from UAV operations, and they can be categorized into regulations pertaining to *operators* and those affecting *operations*, as shown in Table 5.

### 1) Regulations on Operators

UAV operators in many countries are regulated by laws in their countries. Specifically, a pilot license and insurance are required under specific environments or in all cases in some countries, such as Australia, where a pilot license is required if the weight of the UAV exceeds two kilograms. Likewise, in the US, the pilot license is required (mandatory for commercial purposes) and a re-evaluation of pilot competency should be conducted every two years. Moreover, pilot training is required for beyond-visual-line-of-sight (BVLoS) operations in some countries.

### 2) Regulations on Operation

UAV regulations specify certain operational constraints, such as maximum speeds, maximum heights, minimum distances regarding certain areas or objects, approved flight areas and behaviors, and set operating frequency bands. Most countries regulate the maximum height and speed of UAVs. The minimum distances to people, vehicles, or certain areas such as military bases is also specified. In some countries, only a visual-line-of-sight (VLoS) between the UAV and the operator is allowed during UAV operation; i.e., the UAV operation under the BVLoS is not allowed, as unclear sight may cause an incident with high probability while operating UAVs. However, some countries allow BVLoS operation if a collision-avoidance function is employed by the UAV. UAV registration is required in some countries. During UAV communications, a data link should be established within a predetermined frequency band according to certain regulations.

Regulations also define basic ethical courtesies carrying no legal binding force to protect privacy and safety, e.g., no flying over private property, no carrying of hazardous materials, and no dropping of any item.

### 3) Regulation Violations

Though regulations of UAV systems have been established to prevent incidents, they passively control the potential misuse of UAVs and can be violated intentionally or unintentionally. Thus, violating a regulation and the consequent effects should be clearly understood and examined to develop appropriate countermeasures so that the remaining threats to private privacy and public safety can be reduced further. To this end, violations of regulations and the accompanying results are categorized into three different cases, with possible countermeasures and technologies.

- **Accidents:** The regulations on maximum heights or speeds can be violated unintentionally owing to a lack of caution or unexpected disturbances such as wind. If a UAV flies too far away under a BVLoS environment, the strength of the communication signals becomes insufficient and the pilot may lose control. In these cases, the UAV can intrude upon private property or any restricted area and can result in casualties and/or property damage. There is a high probability that such accidents occur when the pilot is unqualified. Unless the pilot has a license or the UAV is registered with appropriate insurance, tracking a suspect is also difficult, and this causes a delay of the recovery process. Note that approximately 70% of the incidents shown in Fig. 2 were caused by such an intrusion.
- **Non-violent crimes:** Violating regulations, a UAV could be misapplied and used for non-violent crimes, such as privacy intrusions, data robberies, and illegal deliveries. Specifically, an offender could attempt to gather private or secret information from civilians, officers or servicepersons by taking photographs and eavesdropping on them. Conveying illegal objects such as unauthorized firearms, explosives, and drugs could also be conducted using an unauthorized UAV. For example, as shown in Fig. 2, there were several crimes accounting for more than 10% among incidents to smuggle contraband into prisons.
- **Violent crimes:** violent crimes, i.e., attacks, directly threaten our safety with possibly fatal outcomes. Violent crimes are closely related to political and military issues, such as terrorism, and are relatively rare compared to accidental and non-violent crimes. However, as UAVs become more easily accessible to the public, there is growing apprehension that violent crimes involving them will increase.

To prevent possible damage from accidents, non-violent crimes, and violent crimes with mUAVs, further clear and concrete regulations are required. Hence, both regional and international regulations pertaining to UAVs continue to be established. Furthermore, for safety and to protect our property from mUAV misapplications and to enjoy the enormous benefits from various UAV applications, further active countermeasures that effectively detect and mitigate mUAVs are necessary. Henceforth, a comprehensive survey of defense systems is provided.

### III. PLATFORMS AND NETWORKS OF CUS'S

As stated in the previous section, a defense system is required for the active protection our safety, property, and prosperous future life. Defense systems to prevent unwanted incidents, crime, and attacks from the misapplication of UAVs, i.e., mUAVs, are referred to as CUSs. A CUS detects, recognizes, tracks, and mitigates mUAVs. Moreover, a CUS can localize the pilot of an mUAV. In

this section, the details of CUSs will be surveyed based on their platforms and networks.

We categorize the platforms of CUSs into the two classes of ground and sky platforms, as illustrated in Fig. 3. Ground and sky platforms consist of CUSs that operate on the ground and in the sky, respectively. Ground platforms can further be classified into static ground, mobile ground, and human-packable (i.e., handheld and wearable) platforms according to their mobility and portability levels. Based on the operating altitude, sky platforms can also be further classified into two platforms: low-altitude platforms (LAPs) and high-altitude platforms (HAPs). Integrated platforms consisting of ground and sky platforms that operate both on the ground and sky are called hybrid platforms.

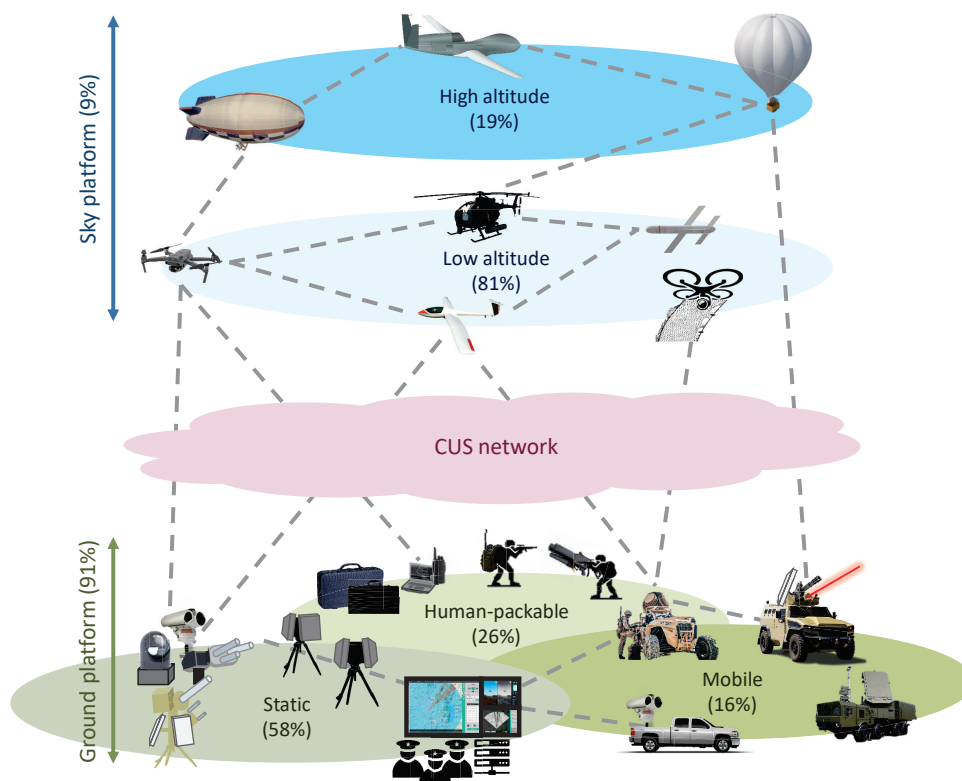
Each platform can be appropriately employed in a CUS considering their advantages and disadvantages and depending on the specific requirements of each application. Furthermore, multiple platforms can be deployed simultaneously and can cooperate through a network, i.e., a *CUS network*. The network should be inter-operable and compatible so that it can coordinate multiple platforms. For example, a static ground platform equipped with radar, two LAPs equipped with an EO sensor, and a mobile ground platform providing RF jamming can be cooperatively operated as a unified CUS network<sup>2</sup>. The CUS network can maximize the effectiveness of defense by complementing the limitations of each platform. In addition, the CUS network can incorporate any types of platforms, e.g., a hybrid platform that is a specific implementation of the CUS network.

In this section, data-driven insights are discussed for each platform obtained from the current CUSs, consisting of approximately five hundred products, a partial dataset of which is available in the literature [38]. Note that there can be a dedicated ground platform for C2 systems (i.e., a C2 station with a human), while this would be difficult for sky platforms. Instead, sky platforms, especially HAPs, can equip C2 systems without humans or systems to support C2 systems. The products of CUSs do not include a dedicated system, and C2 systems are partially distributed to each platform. The details of C2 systems are discussed in Section IV.

#### A. GROUND PLATFORM

Ground platforms are classified as the static ground, mobile ground, and human-packable platforms according to the operation method. Static ground platforms are typically heavy and thus are deployed and operated at a fixed location. On the other hand, mobile ground platforms are typically vehicle-mounted that can be operated *on the move* or at a fixed location. Human-packable (handheld/wearable) platforms are compact and portable

<sup>2</sup>Throughout the survey in this paper, EO sensors and RF jamming are considered as different devices from IR sensors and global navigation satellite system (GNSS) jamming, respectively.



**FIGURE 3.** Platforms of CUS. These platforms are classified into two classes: ground platforms and sky platforms. Ground platforms are categorized into static, mobile and, human-packable platforms, while the sky platforms are categorized into low-altitude platforms and high-altitude platforms

so as to be carried and operated by a human. The details of each platform are surveyed below.

It is worth noting that, following characteristics of the CUS platforms, a game-theoretic problem can be formulated between mUAVs and CUS. The CUS tries to restrict and deter mUAVs, whereas the mUAVs attempt to complete their missions (e.g., reaching destination to perform harmful behavior). The mUAVs may try to find a path that is not the shortest, but most appropriate to complete the malicious missions, predicting the response of CUS. On the other hand, the CUS can also anticipate the malicious behaviors of mUAVs and establish the effective strategies to defend. In [93], interactive time-critical situations were studied based on the cumulative prospect and game theories. Here, an mUAV tries to minimize the malicious mission completion time, whereas a CUS platform confronts mUAV to try to maximize the malicious mission completion time of the mUAV. In this game, the defense strategies should be carefully designed considering the mobility constraint.

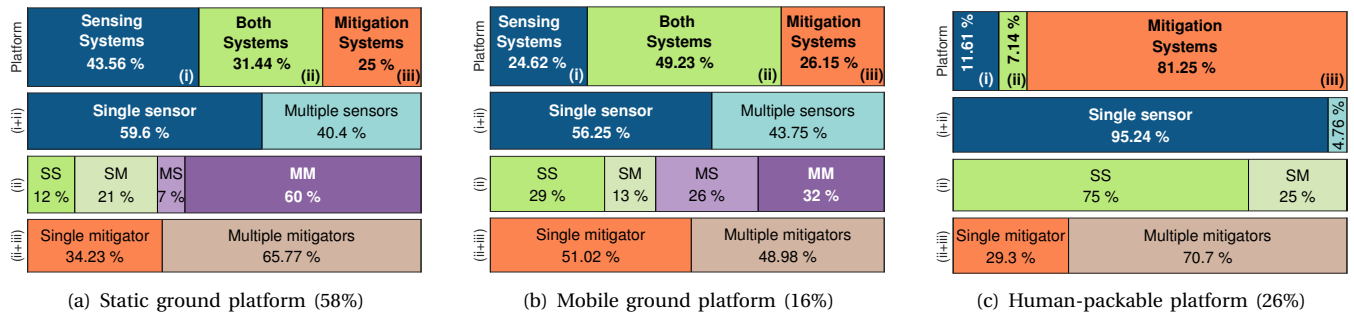
#### 1) Static Ground Platform

The static ground platforms of CUSs constitute the majority of all platforms (approximately, 54% [38]) and are designed to be deployed on stationary ground facilities, e.g.,

airports, airfields, nuclear power stations, oil refineries, government facilities, and households. These platforms are associated with fewer constraints on their size, weight, and power (SWAP). Therefore, static ground platforms are elaborate and efficient and can be optimized for specific tasks to defend against mUAVs. However, static ground platforms are less flexibly able to cope with unpredictable threats from mUAVs.

A static ground platform can be equipped with only a sensing system (approximately, 43%) or a mitigation system (approx. 25%), or both (approx. 31%), as depicted at the top of Fig. 4(a), where the area represents the percentage. Approximately 60% of sensing systems have a single sensor, and 40% of them are equipped with multiple types of sensors, e.g., radar, RF sensors, EO, and IR sensors [94]–[99], as shown in Fig. 4(a)-(i+ii). On the other hand, approximately 34% of mitigation systems have a single mitigator, and 66% of them are equipped with multiple mitigators, such as RF and GNSS jammers [94]–[98], [100], as shown in Fig. 4(a)-(ii+iii).

It is important to note that integrated platforms equipped with both sensing and mitigation systems require reliable connectivity and high-level orchestration among the systems. Thus, static ground platforms are relevant to integrated platforms as SWAP constraints



**FIGURE 4.** Portfolios of the types of ground platforms of CUSs. A partial data set is available in the literature [38]: a) static ground platform, accounting for approximately 58% of CUSs, b) mobile ground platform, at approximately 16% of CUSs, and c) human-packable platform, accounting for approximately 26% of CUSs. SS, SM, MS, and MM denote single-sensor and single-mitigator, single-sensor and single-mitigator, multiple-sensor and single-mitigator, and multiple-sensor and multiple-mitigator, respectively

are in general absent compared to mobile and human-packable platforms. Hence, as shown in Fig. 4(a)-(ii), the platform with multiple-sensors and multiple-mitigators (MM) accounts for approximately 60% of static ground platforms that have both sensing and mitigation systems. Here, single-sensor and single-mitigator (SS) platforms, single-sensor and single-mitigator (SM) platforms, and multiple-sensor and single-mitigator (MS) platforms account for approximately 12%, 21%, and 7%, respectively. The details of these sensors and mitigators are surveyed in Section V.

## 2) Mobile Ground Platform

The mobile ground platforms of CUSs, representing approximately 14% of CUSs [38], are mounted on ground vehicles, and they can be agilely deployed to the target location using the mobility of the vehicles on the ground [101]. Mobile ground platforms are suitable for battlefields and dynamically and rapidly changing environments. However, compared to static ground platforms, mobile ground platforms have SWAP constraints; thus, the available levels and types of sensing and mitigation systems can be limited on this platform. Moreover, the utilization of the mobile ground platform is affected by the capability of the vehicles.

As shown at the top of Fig. 4(b), among all mobile ground platforms, approximately 49% of them have both sensing and mitigation systems [102]–[104], approximately 25% employ only a sensing system [105], and remaining 25% have only a mitigation system [106]. Compared to static ground platforms for which 31% have both sensing and mitigation systems, we can infer that an individual mobile ground platform performs as a total solution of an integrated CUS for successful countermeasures, whereas there is a room for a static ground platform to be interoperated with other static ground platforms without significant SWAP constraints.

For the platform with a sensing system, as shown in Fig. 4(b)-(i+ii), approximately 56% of sensing systems have a single sensor, while 44% of them are equipped

with multiple types of sensors, comparable to the static ground platform. However, as shown in Fig. 4(b)-(ii+iii), nearly half of the mitigation systems have a single mitigator, while for the remaining half, the mitigation systems are equipped with multiple types of mitigators [102], [104]–[106]. The ratio of the mobile ground platform with multiple types of the mitigators is less than that of the static ground platforms, standing at approximately 66%, as the deployment of multiple devices may not be allowed for mobile ground platforms owing to the limited area of the associated vehicles. Furthermore, for the same reason, compared to the portion of MM on the static ground platform, i.e., 60%, the MM portion of the mobile ground platform accounts for approximately 32%, as shown in Fig. 4(b)-(ii).

## 3) Human-Packable Platform

The human-packable platforms for CUSs, accounting for approximately 22% of CUSs [38], are designed to be operated by an individual by hand. Most human-packable platforms with the sensing systems resemble a backpack or briefcase, whereas those with mitigation systems resemble rifles. Human-packable platforms are lightweight and can be carried by a person, meaning that they are portable. However, the performance of the human-packable platforms is limited considering SWAP constraints; e.g., they are associated with inaccurate detection, tracking, and targeting capabilities, and also depends on the skill of the operator. Furthermore, due to the stringent SWAP constraints, most human-packable platforms only employ mitigation systems (approximately 81%) without a sensing system, as shown at the top of Fig. 4(c). In these cases, mitigation systems are equipped with multiple mitigators (approximately 70%, as shown in Fig. 4(c)-(ii+iii)), and the typical mitigators used are RF and GNSS jammers [107]–[109], while the sensing systems are replaced by the eyes of the operators. If a sensing system is employed (approximately 19%), it mainly consists of RF sensors [110], [111]. Only approximately 7% of human-packable platforms employ both sensing and mitigation

systems [112], [113].

The human-packable platforms equipping multiple sensors [114] take approximately 5% as shown in Fig. 4(c)-(i+ii), and no MS and MM are employed for the human-packable platforms that have both sensing and mitigation systems as shown in Fig. 4(c)-(ii). Therefore, the human-packable platforms are relevant as a supplement with other platforms or for a limited personal purpose.

## B. SKY PLATFORM

Sky platforms are systems mounted on certain UAVs, e.g., airships, balloons, fixed-wing aircrafts, and rotary-wing air copters. Due to their maneuverability in air, flexible on-demand placement is possible. Sky platforms are even more flexible and more expeditious than mobile ground platforms.

It is important to note that benefiting from its flexibility, the sky platform can be employed as a multiple-pursuer UAV (pUAV) that tracks and chases mUAVs. In differential game theory, there have been studies on frameworks to examine pursuit-evasion (PE) problems [115]. By solving the PE problem, a control scheme can be designed for pursuers to pursue evaders under position and velocity constraints. To address PE problems, a linear-quadratic differential game was introduced in classic work [116], [117]. Multiple players have also been studied [118], where a high-speed pursuer attempts to capture a couple of slow-moving evaders. In other work [119]–[121], reach and avoid differential games were proposed for applications of aircraft control, motion planning, and collision avoidance. Environments in the presence of obstacles were also studied [122], while other authors [123] considered a multiple-pursuer and single-evader problem in which the multiple cooperative pursuers (i.e., pUAVs) capture a single evader (i.e., mUAV). A single-pursuer and multiple-evader problem was also studied [124], [125]. In further [126], [127], a scenario in the presence of a defender that protects an evader against a pursuer was considered. A distributed algorithm for managing multiple cooperative pUAVs was proposed to mitigate multiple mUAVs [128]. However, the PE problem is not completely applicable to the design of a CUS. Instead, PE problems can be applied in the case of pursuers who protect a protective area from evaders [129].

Sky platforms are not restricted to traditional missions, e.g., reconnaissance and attacks, and they recently have been rigorously studied for various objectives, such as tracking and jamming [130]–[133]. Moreover, recent studies have investigated diverse roles of UAVs, for example, as a UAV relay that supports communications between two nodes [25], a UAV BS that supports users considering secrecy [78], and a UAV-based edge node that performs computing tasks offloaded by nearby users [134].

On the other hand, sky platforms have critical limitations compared to ground platforms. Sky platforms have

limited payloads and battery power such that they can carry only lightweight and low-powered sensing systems and/or mitigation systems. Furthermore, sky platforms may generally require wireless air-to-ground communication links and systems, where the communication architecture can be either an ad-hoc network without infrastructure or a centralized network with a central network node. These requirements and the load-and-battery limitations make sky platforms more challenging compared to ground platforms.

### 1) Low-Altitude Platform

LAPs can fly and hover to cope effectively with mUAVs at low altitudes up to a few kilometers [92], [135]. LAPs are more affordable, and their deployments are quicker and more flexible than HAPs. Due to the extremely high maneuverability and cost-effective mission achievement capability of LAPs, they can play an important role as a part of an integrated CUS. LAPs are typically lightweight compared to HAPs, and their payloads and fuel/battery power are thus limited. To overcome these limitation, energy-efficient designs of UAVs has been vigorously studied [131], [133], [136], [137]. Moreover, the limited energy/power issue has been tackled through various methods, e.g., the rotation of multiple UAVs, rapid replacement of the batteries, wireless power transmission [138], and a tethered UAV whose power can be supplied through a cable [139]. This type of tethered UAV can also have a wired communication link for further reliable and secure communications [140].

Most LAPs that engage mUAVs are equipped with only a mitigation system only. The typical mitigation method of a LAP is to use either a net or a collision UAV [141], [142]. On the other hand, a small percentage of LAPs have a sensing system with most likely a single sensor, i.e., an EO and/or IR sensor [140], [143], [144]. Despite the fact that LAPs can be equipped with both sensing and mitigation systems, their performance is still restricted unless they cooperate with other types of platforms owing to their limited sensing and mitigation capabilities [142], [145].

### 2) High-Altitude Platform

HAPs fly and hover at high altitudes of up to tens of kilometers [67], [92]. Because HAPs have less stringent SWAP conditions, they can be equipped with more systems, such as the communication systems and battery/fuel systems. Compared to LAPs, HAPs can fly longer and higher and have a wider communication range and the field of vision owing to their high-altitude operability and the high probability of line-of-sight (LoS) environments in communications. Therefore, HAPs can effectively counteract mUAVs intruding from high altitudes and can also support other platforms.

However, HAPs are costly and much more difficult to operate compared to LAPs. Moreover, the deployment of

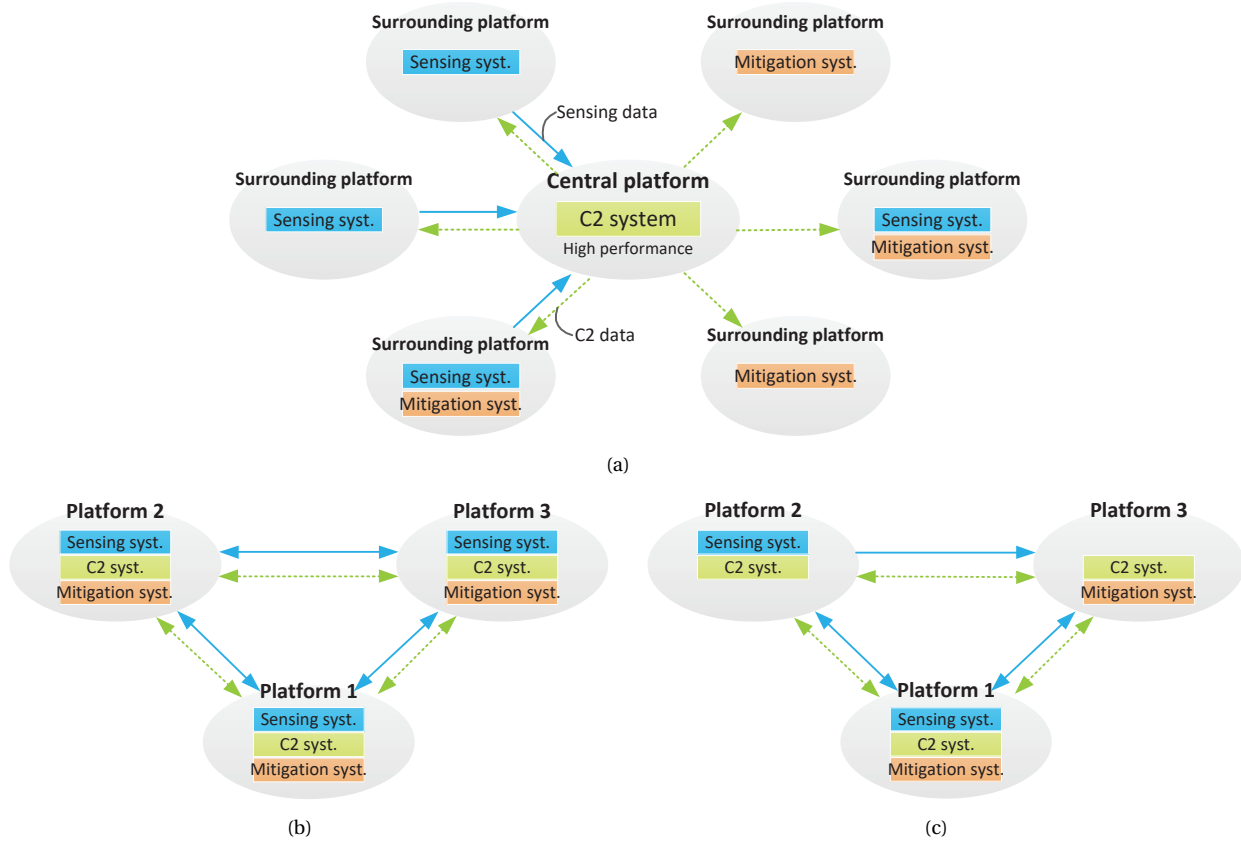


FIGURE 5. Examples of CUS networks: (a) centralized network, (b) decentralized homogeneous network, and (c) decentralized heterogeneous network

HAPs requires more time compared to the time needed to deploy LAPs. Note that traditional aircraft or unmanned combat air vehicles developed for reconnaissance and defense/mitigation during military operations can be interpreted as high-end HAPs for CUSs [146]–[150].

Typical HAPs are equipped with both sensing systems and mitigation systems, where the sensing systems have multiple types of sensors, such as EO, IO, and radar types, and the widely used mitigator types are projectiles. Surveillance HAPs are equipped with only sensing systems. HAPs have been vigorously studied and developed to support other platforms [151]. In such cases, satellite communications can be considered to link multiple platforms beyond HAPs [67].

### C. CUS NETWORKS

As surveyed above, each platform has unique benefits; e.g., ground platforms are less constrained by SWAP constraints and sky platforms can provide highly flexible on-demand deployment and wide operation coverage. On the other hand, each platform also has certain limitations; e.g., ground platforms can support only limited coverage and sky platforms have stringent SWAP constraints. Therefore, a hybrid platform that consists of ground and sky systems can be considered to offset the shortcomings

and enjoy the benefits of each system. Furthermore, by leveraging the advantages of ground and sky systems and providing a spatial diversity gain, hybrid platforms can significantly enhance the performance of CUSs. Hybrid platforms usually have both sensing and mitigation systems and consist of various types of sensors as well as mitigators [144], [152]–[154].

An integrated CUS which encompasses hybrid platforms can consist of multiple platforms, such as multiple ground platforms, sky platforms, hybrid platforms, and combinations of these in a network [154], [155]. The capability of an integrated CUS is determined by not only the performance of an individual platform but also the properties of the entire system of networks. The network can enhance the cooperation among the platforms and thus maximize the effectiveness of the CUS. Integrated networks are categorized into centralized and decentralized networks, as shown in Fig. 5. Decentralized networks can be further classified according to the homogeneity of the platform [156]. We henceforth introduce two classified network models and then discuss the appropriate amalgamation of these models.

### 1) Centralized Network

As shown in Fig. 5(a), a centralized network consists of a single high-performance central platform and a cluster of low-performance surrounding platforms. Any type of platform, i.e., ground and sky platforms, can be operated as either the central platform or the surrounding platforms. To perform as a centralized C2 system which is a specific implementation of a centralized network, the high-performance central platform makes decisions and directs the surrounding platforms to neutralize UAVs effectively. Here, the fully centralized network operates effectively when it can obtain access to all required information, operate the necessary facilities for making decisions, and disseminate the instructions to the surrounding platforms.

The centralized network, however, is vulnerable. A breakdown or failure of the central platform would affect all surrounding platforms, resulting in inefficient CUS operation. Furthermore, exchanging information among the platforms can cause a long latency because the information must pass through the central platform. Therefore, robust and independently dedicated networks are desired to circumvent this general concern of centralized network. If there are multiple high-performance platforms, the centralized process can be partially distributed.

### 2) Decentralized Network

In a decentralized network, C2 systems are distributed to multiple platforms, as shown in Figs. 5(b) and (c), such that each platform in the network cooperatively computes and makes decisions. A decentralized network can be categorized into two models, i.e., a decentralized homogeneous network model and a decentralized heterogeneous network model.

- **Decentralized homogeneous network:** The decentralized homogeneous network consists of multiple platforms that have identical performance and functions, i.e., homogeneous platforms, as shown in Fig. 5(b). Thus, unlike the platforms in a decentralized heterogeneous network, each platform in the decentralized homogeneous network has its own sensing and mitigation systems. When any of the platforms do not operate, the CUS can still operate with slight performance degradation. The merit of the decentralized homogeneous network is robustness against malfunctions of the platforms. However, each function of the homogenous platform provides relatively low-quality performance compared to that of heterogeneous platforms. Therefore, the platforms may partially cooperate for sensing, computing, decision making, and neutralizing mUAVs to maximize the effectiveness of the CUS.
- **Decentralized heterogeneous network:** The heterogeneous decentralized network consists of multiple types of platforms, i.e., heterogeneous platforms, as shown in Fig. 5(c), where each platform performs

only a few specific tasks, e.g., sensing, computing, decision making, and neutralization. In this case, each platform should have the capability to execute sufficient performance for its assigned mission such that any platform can request that another platform perform a task that it cannot perform. If any platform that undertakes a unique function fails to complete its role, this partial malfunction may cause a bottleneck and failure of the entire CUS operation, as the central platform breakdown in a centralized network. However, the well-designed networks as shown in Fig. 5(c) can resolve this issue. As shown in Fig. 5(c), if any platform does not operate, the other two platforms can cooperate to complete the mission. The decentralized heterogeneous network would be a good solution to achieve a tradeoff between robustness and performance.

## IV. ARCHITECTURE

In this section, the architecture of the integrated CUS is introduced. Integrated CUS architectures can be categorized into three types based on their roles, as follows (refer to Fig. 6): *Sensing systems* that gather data from the environment and transmit the observed data to C2 systems; *C2 systems* that perform computing tasks (e.g., detection/identification and tracking/localization algorithms) and make decisions based on the received data, such as the detection/identification declaration, localization/tracking declaration, and time and method of the neutralization of mUAVs; and *mitigation systems* that perform mUAV neutralization based on the decisions of the C2 systems.

Each sensing system, the C2 system, and the mitigation system can be equipped in either single or multiple platforms. On the other hand, each platform can employ multiple systems, i.e., an integrated architecture. However, only a few platform products utilize the integrated type of architecture because it requires a considerable level of the autonomy to operate the CUS effectively, which could be a burden and has remained underdeveloped with regard to maximizing the performance of CUSs. Hence, most platforms have only either a sensing or mitigation system and their limitations are compensated by the network among the platforms, as stated in Section III. At this point, the details of each part of the CUS architecture are introduced.

### A. SENSING SYSTEMS

The survey on sensing systems is focused on the information collected by sensing systems i.e., the gathering of data, and how the sensing systems operate.

#### 1) Gathering Data

The sensing systems can collect data such as sound wave data, radio wave data, and light wave data. Wave data can be obtained through various devices, such as sonars,

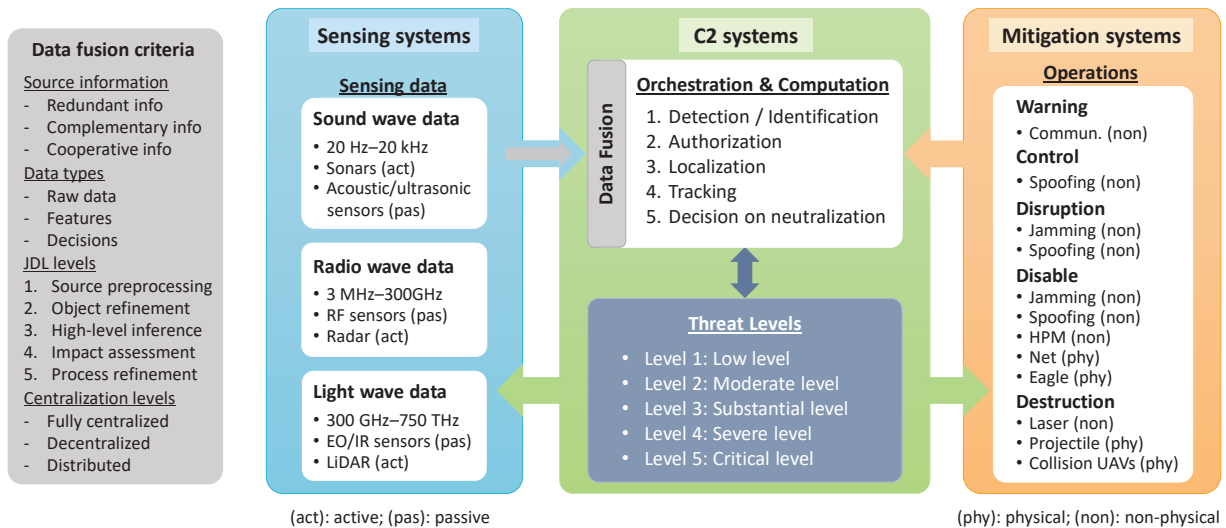


FIGURE 6. Diagram of CUS architecture that consists of sensing systems, C2 systems, and mitigation systems

acoustic/ultrasonic sensors, radar, RF sensors, LiDAR and, EO/IR sensors. As the details of each sensor are presented in Section V, wave data is discussed here.

- **Sound wave data:** Sound waves are the mechanical waves that include infrasound (up to 20 Hz), acoustic (between 20 Hz and 20 kHz), and ultrasound (above 20 kHz, up to several gigahertz) waves. Sound waves have lower velocities than electromagnetic waves such as radio waves and light, and are longitudinal and not polarizable. Sound waves require a medium (e.g., air and water) through which to propagate. Sound wave data can make sensing systems more reliable by providing additional data with electromagnetic (EM) wave data. To capture sound data, sonar operates actively, i.e., active sensors, whereas acoustic/ultrasonic sensors operate passively, i.e., passive sensors. However, sonar typically is used for underwater applications to navigate and communicate and is rarely used for UAV detection owing to the poor propagation characteristics of sonar waves in air. From this survey, it is revealed that sonar has limited applications, UAV mapping and collision-avoidance functions [157]–[160]. On the other hand, acoustic/ultrasonic sensors are widely used for UAV detection; this is discussed further in Section V-A(1).
- **Radio wave data:** Radio waves consist of waves in the electromagnetic spectrum, typically in the frequency range from 3 MHz to 300 GHz, and radio wave information has been widely used as UAV detection data. In this case, the wireless channel state information is critical to capture radio wave information. For example, the path loss is a key metric to determine the presence of mUAVs. For detecting UAVs in the sky, it is important to under-

stand air-to-ground (A2G) and air-to-air (A2A) radio channels. A2G and A2A channel models are different from those of traditional terrestrial channels [75], [76]. Analytic A2G channels can be characterized by their LoS and non-LoS (NLoS) components. A2G channels are then analyzed according to the LoS probability depending on the environment model [78], [161]. A2A channels tend to have a lower path loss exponent than A2G and terrestrial channels [75]. Therefore, exploiting the LoS in A2A channels, sky platforms equipped with synthetic aperture radar or RF sensors can reliably collect radio wave information. To capture radio wave information, radar transmits signals and gathers the radio data from reflected echo signals, i.e., active sensors. On the other hand, an RF sensor collects the ambient RF signals emitted from mUAVs, i.e., passive sensors, as discussed further in Section V-A(2).

- **Light wave data:** Compared to radio waves, the light waves have higher frequencies and shorter wavelengths with different characteristics. In more detail, light waves include the infrared light (300 GHz–430 THz) and visual light (430 THz–750 THz) spectrums. Light waves have a shorter range than radio waves yet a better resolution owing to the shorter wavelength with a higher frequency compared to radio waves. However, light waves are affected by weather phenomena, such as clouds, fog, rain, falling snow, sleet, and direct sunlight, due to their short wavelength and have high degree of straightness. Hence, the LoS requirements of light waves are more stringent than those of radio waves. Light wave information in the visual spectrum is intuitive and can be analyzed by humans, yet the information

collected at dark times, e.g., at night and on cloudy days, is insufficient to provide high-quality visual images. Meanwhile, infrared radiation is emitted by objects according to the black body radiation law. This makes infrared sensors capable of collecting data such as temperatures irrespective of the degree of visible illumination. However, because infrared images are detected based on heat energy, these images are influenced by the emissivity and reflection of sunlight. As active and passive sensors, LiDAR and EO/IR sensors are widely used to collect light information, as discussed further in Section V-A(3).

## 2) Data Fusion

The majority of sensing systems have a single type of sensor. The data collected by a single sensor or identical types of sensors, however, could be insufficient for accurate and precise detection/identification and localization/tracking. To offset the limitations of single types of sensors, multiple types can be employed by high-end systems considering the requirements and usage environments. Furthermore, instead of simply obtaining results from each sensor type, comprehensive *data fusion* (i.e., the fusion of sensing information) can be implemented [47]. Note that data fusion considers not only multiple sensor types but also multiple identical sensors and can be implemented in sensing systems and C2 systems.

Data fusion is multidisciplinary in that a clear classification is not established. We introduce four classification criteria to provide a clear understanding of data fusion. Data fusion can be categorized according to the source information [162], the data type, the abstraction level [163], joint directors of laboratories (JDL), or data fusion information group (DFIG) models<sup>3</sup>, and by the locations at which fusion is performed [166]. The source information can be classified as (i) redundant information pertaining to the same target for greater reliability, (ii) complementary information provided by sources about different parts of the target, and (iii) cooperative information that is combined into new information (e.g., multimodal data fusion). The types of data for the input and/or output of fusion can be raw data (analog/digital signals), features, or decisions. Here, the data type (i.e., data amount or compression level) which affects the performance should be carefully designed by considering the tradeoff between performance and cost, such as the communication bandwidth and power consumption of the sensors. Furthermore, the processes of data fusion are classified based on the JDL and DFIG models into five levels: (i) source preprocessing, (ii) object refinements:

<sup>3</sup>The process of data fusion, including the *data*, *sensor*, and *information* fusion steps, is categorized into levels 1 to 4 based on JDL or levels 0 to 5 based on DFIG, where the levels are as follows. Level 0: source preprocessing or subject assessment; Level 1: object assessment; Level 2: situation assessment; Level 3: impact assessment (or threat refinement); Level 4: process refinement; and Level 5: user refinement (or cognitive refinement) [164], [165]

mUAV classification, identification, and tracking; (iii) high-level inference; (iv) impact assessments: evaluations of threats and predictions; and (v) process refinement: resource and sensor management. Fusion can be performed in a fully centralized architecture, a decentralized architecture, or a distributed architecture according to the process and fusion capabilities. Note that the majority of the computation for fusion is performed at a C2 system, which can also be centralized, decentralized, and/or distributed. Details will be introduced in the next subsection.

Some researchers [167] employed a support vector machine (SVM) with multiple features of sensing data to detect UAVs. The fusion of radar and audio sensors was studied to identify clearly whether a detected object is an mUAV or possibly a harmless entity, such as a bird [168]. Other authors [169] studied mUAV detection with radar, IR, and EO, as well as acoustic sensors. Multimodal deep learning was recently studied [170], where data fusion was implemented by extracting multiple features.

## B. C2 SYSTEMS

As mentioned in Section III, the majority of platforms have only either a sensing or a mitigation system. A central platform can perform many roles of a C2 system yet is technically discriminated from a C2 system. Some of the hardware and software of a C2 system can be included in multiple platforms. In other words, C2 system architecture types can be distributed over multiple platforms, and each platform can compute and make partial decisions separately. However, a dedicated C2 system is a core processing unit that can orchestrate multiple platforms for high-end performance of the CUS and can have high computing power. C2 systems make decisions about which tasks are required, i.e., *orchestration*, and the *threat levels* of mUAVs, and perform *computation* for orchestration and decisions. According to i) the distance between the mUAV and the protection area, ii) the speed and direction of the mUAV, iii) the payload carried by the mUAV (e.g., explosives), iv) the size and type of UAV, and v) the attributes of the protective area, the threat level can be determined, as follows:

- Level.1 (Low): a threat is unlikely.
- Level.2 (Moderate): a threat is possible, but not likely.
- Level.3 (Substantial): a threat is a strong possibility.
- Level.4 (Severe): a threat is highly likely.
- Level.5 (Critical): a threat is expected imminently.

C2 systems make decisions autonomously or by well-timed human intervention. Here, human intervention can be a bottleneck to cope with fast-moving UAVs. Therefore, fully autonomous with the least human intervention possible will enhance the performance of CUSs.

### 1) Orchestration

The orchestration procedure of C2 systems in an integrated CUS can be divided into five steps, as follows [49],

[50]. Note that the threat level can be updated during every step, and step (v) can be directly executed while omitting the other steps depending on the threat level.

- (i) **Detection/identification:** To detect any suspicious object, C2 systems initially gather data from the sensing systems. C2 systems may then perform data fusion by dividing the tasks of extracting features and making decisions (i.e., identification) with sensors as to whether the detected object is a UAV or another small object, e.g., a bird, kite, or balloon. The decision can be made from raw data, feature data, or local decision data. Furthermore, C2 systems can classify the payload carried by the UAV to determine the threat level [171], [172].
- (ii) **Authorization:** When C2 systems conclude that a detected object is a UAV, they can then verify whether the detected UAV is authorized or unauthorized. According to the decision with regard to verification of authorization, C2 systems update the level of the UAV threat.
- (iii) **Localization:** If the threat level exceeds a predefined level (e.g., level 2), C2 systems identify where the detected UAV is located and/or whether it is heading toward a sensitive protecting area, i.e., mUAV localization. Localization for the operators of mUAVs can be performed to investigate and prevent future threats, i.e., operator localization. Generally, operator localization can be performed only when veiled operators communicate with UAVs by RF signals, whereas mUAV localization can be achieved not only by RF signals but also by other data sources. Here, the threat level is updated according to the localization results.

Localization for mUAVs should be implemented without GNSS because the GNSS information of mUAVs is unavailable for CUSs. Localization without GNSS (i.e., indoor localization) has been widely studied [173]–[175]. Indoor localization techniques can be classified into geometric positioning (e.g., triangulation), fingerprinting, proximity analysis, and vision analysis. The applicable localization techniques for CUSs are geometric positioning and vision analysis. Geometric positioning requires angle and distance information. The angle-of-arrival (AoA), received signal strength index, time of flight/arrival (ToF/ToA), time difference of arrival (TDoA) [176]–[178], and round-trip ToF (RToF) [179] can be estimated from sound, radio, and light data, and the estimated information provides source information for geometric positioning. Estimation by ToF/ToA and TDoA-based methods may be infeasible for the localization of uncooperative UAVs, as they require a common clock and synchronization. In one study [180], radio-based UAV detection and AoA estimation algorithms were investigated. In another study

[181], AoA estimation techniques using a directional antenna array were proposed to localize UAVs. A visual analysis can also be employed for localization. The visual analysis is implemented based on light information (i.e., captured images). The obtained information is discriminated with irrelevant background (e.g., buildings and static objects) to estimate the positions of mUAVs [173], [182]–[184]. However, a depth camera is needed to estimate the distance between an mUAV and a sensor. The distance can also be estimated with prior knowledge of the mUAV without a depth camera [185].

- (iv) **Tracking:** According to the updated threat level, the C2 systems determine whether to track the detected mUAV. A sky platform is an effective tool capable of physically tracking an mUAV, i.e., chasing it. On the other hand, tracking can be interpreted as the algorithmic tracking of the target UAV by C2 systems and sensing systems. Tracking can also be implemented by data fusions such as localization. For algorithmic tracking, an extended Kalman filter, a particle filter, and template matching are widely employed for general tracking from ground sensors [130], [183], [186]. Note that authorized UAVs can actually be camouflaged or stolen/spoofed/hacked by malicious operators, and UAVs can veil their intentions and pretend to be authorized until the moment they present the harmful threat. Authorized UAVs can operate in a malicious manner abruptly. Thus, C2 systems must continue to observe/track even authorized UAVs. While tracking an mUAV, the threat level must be updated according to the tracking result.
- (v) **Decision on Neutralization:** C2 systems can make decisions to neutralize UAVs from the updated threat level. Neutralization methods include controlling, warning, disrupting, disabling, and destroying [187]. Following the regulations of the authorities and according to the neutralization strategy, the neutralization method is determined by the C2 system. To increase the effectiveness, multiple mitigation systems with various neutralization methods can be operated simultaneously.

## 2) Computation

Throughout the integrated CUS procedures, high computing power is required to improve the accuracy and effectiveness of detection/identification, localization, tracking, and neutralization. Outstanding computing performance is required to implement state-of-the-art data fusion schemes, detection-localization-tracking algorithms, and for orchestral multi mitigation system operation. The computing complexity can increase exponentially for integrated CUSs that require the capability to cope with multiple UAVs and state-of-the-art algorithms. To this end, C2 systems must provide high computing power.

Meanwhile, centralized computing can be a bottleneck in CUSs. A breakdown or/and failure of centralized computing can limit the system's ability to protect the skies. Decentralized or distributed computing can provide a robust network without system bottlenecks, while a single C2 system on a global platform can lead to a vulnerable network. Decentralized/distributed computing can be implemented on platforms with computing capabilities cooperatively sharing computing tasks.

Recently, *cloud computing*, where a cloud with powerful computing capabilities performs highly complex tasks, has emerged. The cloud can provide high computing power and network management given its benefits of vast resources. However, cloud computing is centralized and has the drawback of latency. *Fog computing* or *edge computing* has also emerged to deal with this problem. Fog computing can cope with latency-sensitive applications using network edge nodes. Network edge servers (or *cloudlets*) with a distance closer than the cloud compute tasks and therefore decrease the propagation delay. On the other hand, the cloud can be reached by passing several networks on which network managing operations (e.g., routing, medium access control) are needed. However, the computing latency of fog computing is greater than that in cloud computing. Therefore, *task offloading* must be rigorously designed based on this tradeoff. Note that employing the sky platform (not only the ground platform) as a cloudlet has also been vigorously studied [134], [188]. Readers can refer to one earlier study [189] and the references therein for more details.

### C. MITIGATION SYSTEMS

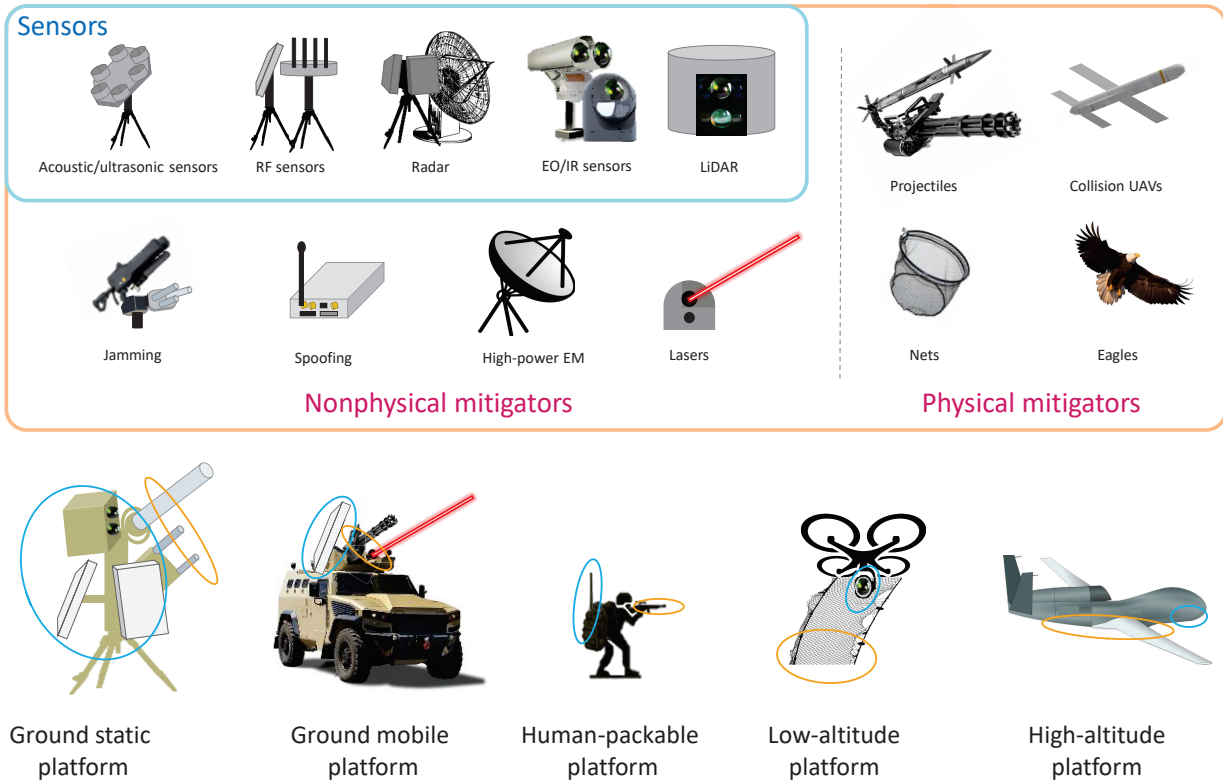
According to the threat level as determined by the C2 system and following the regulations of relevant authorities, several mitigation systems can be simultaneously activated and cooperate to mitigate mUAVs effectively. Based on the strength of the threat level and countermeasures against mUAVs, mitigation systems can *warn*, *control*, *disrupt*, *disable*, and *destroy* by utilizing various mitigators, such as RF/GNSS jamming, spoofing, high-power microwaves (HPMs), lasers, nets, eagles, projectiles, and collision UAVs [187].

- (i) **Warning:** With knowledge of the utilized communication system of the mUAV, mitigation systems can warn and neutralize the mUAV by communicating with the operator of the mUAV on restrained terms when the threat level is Level 2(Moderate). Because the pilot of the mUAV can sabotage the UAV, which could be a danger for civilians if the mUAV is flying or hovering over habitations, the warning would be the first neutralization<sup>4</sup> strategy before other mitigation methods are used. To the end, mitigation systems should include a communication system

and the capability to provide the direction of the flight such that the mUAV can deviate from the unauthorized route to avoid an intrusion.

- (ii) **Control:** Instead of warning the mUAV operator, direct control of the mUAV can be implemented via spoofing. This requires more sophisticated and high-end techniques and devices when the threat level is higher than or equal to Level 3(Substantial). By taking control of the mUAV, mitigation systems can land the mUAVs safely and immediately on the ground. If there is a return to home (RTH) mode in the mUAV, the RTH mode can be activated [190]. However, owing to the lack of standards, protocols, and regulations, it is difficult to implement control methods practically.
- (iii) **Disruption:** Disruption refers to interrupting the operation of an mUAV. Mitigation systems can disrupt potential mUAVs that can threaten a protected area when the threat level is higher than or equal to Level 4(Severe). Typical disruption methods are cyber attacks, such as jamming and spoofing. By using jamming and spoofing methods, mitigation systems disrupt the mUAV so that it cannot be operated with full maneuverability. Once the mUAV is disconnected from the operator by disruption, the RTH mode can be activated [190].
- (iv) **Disabling:** Compared to disruption, which causes UAVs to malfunction, disabling UAVs is harsher when the threat level is higher than or equal to Level 4(Severe). Stronger RF/GNSS jamming, spoofing, and HPMs can disable mUAV operation in a non-physical manner. In addition, a net catcher or eagles, which are the kinetic mitigation systems, can disable UAVs physically.
- (v) **Destruction:** Destroying mUAV is the harshest means of physically neutralizing an mUAV by using weapons such as lasers, projectiles, and collision UAVs [191]. These system can be activated when the detected mUAV is too close to a secure-sensitive area, such as an airport, airfield, nuclear power station, oil refinery, public infrastructure, government facility, or military facility and related areas, and/or then they are too fast to verify the threat or to use other more moderate neutralization methods. In urgent situations, i.e., threat Level 5(Critical), the multiple destroying systems can be activated and cooperate to improve the protection capability. The destruction of an mUAV may have a knock-on effect from the debris of the mUAV and the explosion. Thus, in urban environments where many people can be injured, mitigation systems need to determine the destruction time. The destruction can also be deferred to locate and capture the operators of mUAVs. Note that the physical destruction can be a last resort for mitigating mUAVs.

<sup>4</sup>Neutralization and mitigation are interchangeably used throughout the paper.



**FIGURE 7.** Sensors and mitigators. Note that radar, RF sensor, jamming, spoofing, and high-power EM employ antennas and their functions can be implemented with the same hardware; therefore, their appearances are similar to one another. The platforms show sensing and mitigation systems equipped in ground static platforms, ground mobile platforms, human-packable platforms, LAP, and HAP

To overcome the limitation of single mitigator/UAV of CUSs, the operation of the multiple UAVs is desired. To this end, the newest wireless communication technologies capable of supporting/controlling numerous devices and with ultra-reliable and low-latency communications, e.g., 5G and B5G, are recommended for CUSs.

## V. CUS DEVICES AND FUNCTIONS

Sensors and mitigators are essential components that compose the sensing and mitigation systems, respectively, as introduced in Section III and as shown in Fig. 6. Each sensor and mitigator has unique characteristics, limitations, and shapes, as shown in Fig. 7. Additionally, multiple sensors and mitigators can be deployed on a single platform, as shown in Fig. 7. In this section, we introduce the details of sensors and mitigators and their functions.

### A. SENSORS

A sensor is generally a device, module, machine, or subsystem that detects and reports events or changes of a monitored surrounding environment. Herein, the sensors of sensing systems for CUSs are intended to detect and report UAVs and can be classified as active

or passive sensors. Active sensors, such as radar and LiDAR, transmit waves and receive reflected waves to collect data. On the other hand, passive sensors such as the acoustic/ultrasonic sensors, RF sensors, and EO/IR sensors, receive ambient waves which are emitted from UAVs. Sensors can be also categorized according to the frequency of the transmitting and/or receiving waves. Herein, sensors are surveyed based on the wave frequencies, from low to high, as shown in Fig. 6. They are also categorized in Table 6.

#### 1) Acoustic/Ultrasonic Sensors

Microphones are pressure transducers that convert sound waves into electrical signals and are thus widely used as the acoustic/ultrasonic sensors that detect the spectral range of audible (between 20 Hz and 20 kHz) and ultrasound (above 20 kHz, up to several gigahertz) waves. Most UAVs generate sound from the engines/motors and/or rotors. Mini-UAVs generate buzzing and hissing sounds in the frequency range of 400 Hz to 8 kHz [192], which can be detected by the acoustic sensors. The gathered sound data can be compared to libraries of acoustic signatures to discriminate UAVs from other, similar objects [192]. For example, DroneShield built a database

**TABLE 6. Characteristics and Limitations of Sensors**

Sources	Sensors	Act/Pas	Characteristics & Strength	Limitations & Weakness	References
Sound Waves	Acoustic/ultrasonic sensors	Passive	<ul style="list-style-type: none"> <li>• 20 Hz–20 kHz, Microphones</li> <li>• Acoustic signature library</li> <li>• Supporting other type of sensors</li> </ul>	<ul style="list-style-type: none"> <li>• Range is limited</li> <li>• Vulnerable to ambient noise</li> <li>• Capacity limits and updating of libraries</li> </ul>	[192]–[200]
	RF sensors	Passive	<ul style="list-style-type: none"> <li>• Communication spectrum. Capturing commun. signals between mUAVs and operators</li> <li>• Low complexity and easy to implement</li> </ul>	<ul style="list-style-type: none"> <li>• Knowledge of mUAV communication specifications, such as modulation protocols and MAC addresses, is desired</li> <li>• Poor target detection reliability</li> </ul>	[48], [201]–[205]
Radio Waves	Radar	Active	<ul style="list-style-type: none"> <li>• 3 MHz–300 G Hz (Operate in cloudy weather)</li> <li>• (FM)CW radar, UWB radar, mmWave radar</li> <li>• Micro Doppler signatures (MDS)</li> <li>• Longer range than LiDAR, Velocity info.</li> </ul>	<ul style="list-style-type: none"> <li>• Large radar cross-section (RCS) is desired</li> <li>• Limited performance for low altitudes and speeds</li> <li>• Interference from other small objects</li> <li>• LoS is highly desired</li> </ul>	[206]–[230]
	EO/IR	Passive	<ul style="list-style-type: none"> <li>• 300 GHz–430 THz (visible spectrum)</li> <li>• EO: visual images, IR: thermal images</li> <li>• EO: day light, IR: w/o day light</li> <li>• Assisted by computer-vision technologies</li> </ul>	<ul style="list-style-type: none"> <li>• Provides 2D images</li> <li>• Limited by weather cond. &amp; background temp.</li> <li>• Susceptible to positions of objects (horizon)</li> <li>• LoS is required</li> </ul>	[45], [130], [231]–[240]
Light Waves	LiDAR	Active	<ul style="list-style-type: none"> <li>• 300 THz–500 THz (light pulse)</li> <li>• Providing 3D representation</li> <li>• Detecting an object in a complex background, i.e., high-resolution detection is possible</li> </ul>	<ul style="list-style-type: none"> <li>• LoS is required and the detection range is short</li> <li>• Limited usage in nighttime/cloudy weather</li> <li>• Operating altitude: 500–2,000 m</li> <li>• Expensive technology</li> </ul>	[101], [241], [242]

of the acoustic signatures of various UAV models to prevent false alarms due to ambient noise [193]. Also, the detection system employs acoustic sensors to detect the rotating propellers of UAVs and compare the detected data with the acoustic signatures in a database [194]. However, the libraries of acoustic signatures do not cover all types of proliferating UAVs over various fields. Furthermore, acoustic sensors cover a limited range, and acoustic/ultrasonic data is vulnerable to wind and surrounding ambient noise sources. Though the LoS environment can enhance the detection performance, it is not required for acoustic/ultrasonic sensing. To overcome the limitations of acoustic/ultrasonic sensing and to bolster the performance capabilities of other types of sensors, various techniques and algorithms have been studied using acoustic/ultrasonic data.

A microphone can be used to detect a UAV [195]. To increase the detection range, the arrays of microphones can be used [196]. Localization and tracking of UAVs were studied with an acoustic array using calibration and beamforming [197]. In another study [198], a classifier with two layers was proposed, where the first layer determined the existence of a UAV and the second layer determined the UAV type, e.g., fixed-wing or rotary-wing. Machine learning-based algorithms such as the SVM and k-nearest neighbor (k-NN) algorithms, as well as neural networks were studied to classify the time- or frequency-domain acoustic/ultrasonic signals generated from UAVs [199], [200].

## 2) RF Sensors

RF sensors capture ambient EM signals emitted from mUAVs or remote operators to detect mUAVs. The majority of commercial UAVs are remotely controlled by their operators. For example, UAVs and operators communicate telecommand and telemetry information, such as altitude, position, battery life, and video data. Hence, RF

sensors can detect mUAVs unless the mUAV is preprogrammed and autonomous. Because RF sensors are easy to implement and have low computational complexity, they have been studied for various systems. In one such study [201], the average signal strength measured by several RF sensor nodes was used to detect UAVs. Using Wi-Fi receivers and software-defined radio boards, RF sensors eavesdrop on the link between the mUAV and the controller and capture the vibrating patterns of the UAV body for UAV detection [202], [203]. The detection and classification of micro UAVs from the RF signals were also studied based on machine learning approaches [204].

RF sensors are widely applied to various systems owing to their simplicity, yet they have several limitations. RF sensors have poor target detection reliability and high false alarm probability rates. Because the RF sensor is passive, it does not provide the range information of the mUAV. Knowledge of the spectrum band in use is required for detection. Furthermore, knowledge of modulation protocols, e.g., the frequency hopping spread spectrum, the direct sequence spread spectrum, and orthogonal frequency division multiplexing, and/or the identification of media access control (MAC) addresses is required to improve the fidelity of the detection performance [48]. Here, spectrum sensing can be employed to acquire information [205]. Signals sharing the same frequency band as UAVs, i.e., electromagnetic interference, make RF-based UAV detection more challenging. Furthermore, identifying MAC addresses is only possible for disclosed-to-the-public MAC addresses.

## 3) Radar

To determine the range, angle, or velocity of an mUAV, radar is widely used as an active sensor in sensing systems in a CUS. A radar system consists of a transmitter, a receiver, and a processor [211]. The transmitter radiates EM signals whose frequency ranges typically between

3 MHz and 300 GHz depending on the application. The EM signals are reflected by the mUAV and return to the radar. The returning EM signals reflected from the mUAV provide essential information with which to obtain the mUAVs' location and speed. Thus, the amount of the received signal power is critical to determine the detection performance of the radar. However, because the reflected radar signals captured by the receiving antenna are very weak, they need to be amplified at the processor. The reflected radar signals captured by the receiving antenna are inversely proportional to the frequency, whereas they are proportional to the radar cross-section (RCS), a measure of how detectable an object is that depends on the material, size, and location (i.e., the distance and incident and reflected angles) of the mUAV. From the reflected radar signals, the processor can calculate the round-trip time (i.e., ToA) and the frequency shift due to the Doppler effect to estimate the distance and velocity information of the mUAV.

However, traditional radar systems are designed to detect legacy (manned) aircraft with high velocities and a large RCS, and they are inappropriate to detect slow-moving and low-flying mUAVs with a small RCS [206], [224], [226], [227]. To circumvent this issue, the micro-motions of vibrating (by engines or motors) and rotating (by propellers) structures of UAVs [218]–[220], which cause a unique micro-Doppler signature (MDS), have recently been used for radar detection. Research has shown that quadcopters, hexacopters, and octocopters have different MDS characteristics [222], [223]. Radar can detect mUAVs by analyzing the MDSs of mUAVs [206], [215]–[217]. The joint time-frequency analysis method, e.g., short-time Fourier transform, can also be utilized to analyze the radar MDSs of UAVs [221].

Various types of radar to detect objects with small RCSs have been studied. An unmodulated continuous wave (CW) Doppler radar system with a long dwell time can capture rich information to deal with small UAVs with a small RCS [207]–[210], though it cannot obtain the target range [211]. A frequency-modulated CW radar system can estimate the ranges as well as velocities of multiple targets simultaneously [46], [212]–[214]. On the other hand, ultra-wideband (UWB) radar generates an extremely narrow pulse, resulting in wideband utilization. UWB radar can be employed for high-resolution ranging resulting in an accurate ToA. Experimental results show that MDSs induced by mini-UAVs and birds are significantly different, and it was found that mini-UAVs and birds can be distinguished based on features caused by the flapping wings of the birds and the unique MDS [206], [228]–[230], [243]. It was also found that millimeter-wave radar can provide high-fidelity micro-Doppler echoes from a mini-UAV from the very rapidly rotating propellers [224], [243].

#### 4) EO/IR Sensors

EO sensors detect EM waves that range from the infrared (300 GHz–30 THz) up to the ultraviolet (larger than 790 THz) frequencies. Typically, EO sensors capture visible wavelengths (300 GHz–430 THz) reflected from mUAVs to detect them under daylight conditions. On the other hand, IR sensors, i.e., thermal cameras, detect the infrared spectrum to capture the heat signature (resolutions as low as 0.01°C) radiated from mUAVs and thus can detect targets even without sufficient light, e.g., during the night and cloudy and/or dark days. The spectrum should be determined based on the expected temperature of the target object. An IR sensor can detect heat emitted from the motors and engines of mUAVs [45], [231], [232], where IR cameras with shorter wavelength provide better performance to capture fast-moving bright and small targets than long-wavelength IR cameras [45].

Passive EO/IR sensors provide only two-dimensional (2D) images. Accordingly, to enhance the detection performance, various machine learning- and deep learning-based approaches have recently been employed. Machine learning-based approaches, e.g., SVM and k-NN, classify objects based on predetermined features, whereas deep learning-based approaches are typically convolutional neural networks (CNN) without specified features. For example, the use of neural networks has been rigorously investigated and developed for EO/IR sensors [130], [233]–[239]. In [233], a regression-based approach was studied for its ability to classify and detect UAVs. In that case, the training dataset was also provided. The training data set can be artificially generated for the CNN [240]. Various neural networks, such as that by Zeiler and Fergus of the Visual Geometry Group and another entitled 'You Only Look Once', have also been assessed for UAV detection [234], [240]. Robust algorithms for static/moving cameras were designed to propose candidate regions and classify UAVs with birds [238], and the onboard UAV system was devised to detect and chase other UAVs using a lightweight camera and a low-power algorithm without a GNSS service [237]. A pUAV detecting a target mUAV based on template-matching algorithms with a morphological filter was also considered [130]. In another study [239], an onboard UAV-Net detector was proposed to detect small objects. Algorithms based on CNNs and spatio-temporal filtering have also been proposed to detect and track mUAVs and discriminate mUAVs from birds [235]. In other work [236], a super-resolution object-detection method for detecting UAVs was designed.

Though EO/IR sensors have been widely studied and utilized for object detection, they have several limitations. The detection performance capabilities of EO/IR sensors are highly degraded under NLoS environments. Further, good focusing capability and multiple cameras are required for EO/IR sensors to perform multi-direction detection. EO/IR sensors are susceptible to

TABLE 7. Characteristics and Limitations of Mitigators

Category	Subcategory	Characteristics & Strength	Limitations & Weakness	References
Nonphysical	RF/GNSS Jamming	<ul style="list-style-type: none"> <li>Interfering with mUAVs to degrade the received SNR</li> <li>GNSS signals of mUAVs are weak and vulnerable</li> <li>Increase the possibility of eavesdropping on mUAVs, which is useful when spoofing them</li> </ul>	<ul style="list-style-type: none"> <li>Ineffective for autonomous mUAVs</li> <li>Ineffective for GNSS-robust mUAVs with IMU sensors</li> <li>Ineffective for encrypted GPS in mUAVs</li> <li>Short distances are desired</li> </ul>	[132], [133], [244]–[247]
	Spoofing	<ul style="list-style-type: none"> <li>Controlling mUAVs and GNSS spoofing are possible</li> <li>Exploiting the vulnerabilities of various systems in mUAVs</li> </ul>	<ul style="list-style-type: none"> <li>Comm. information regarding mUAVs is required</li> <li>Solid analysis on mUAVs is required</li> </ul>	[247]–[252]
	High-power EM	<ul style="list-style-type: none"> <li>Impairing electronic systems via high-power EM waves</li> <li>Narrowband EM waves: high power on a single frequency</li> <li>Wideband EM waves: short pulses in the time domain</li> </ul>	<ul style="list-style-type: none"> <li>Accurate direction of EM wave is required</li> <li>Kill assessment may not be possible</li> <li>There is a chance of a low lethality rate</li> </ul>	[253]–[255]
	Lasers	<ul style="list-style-type: none"> <li>Low power lasers: dazzlers</li> <li>High-power lasers: burn and destroy mUAVs</li> <li>Tracking of the target is required</li> </ul>	<ul style="list-style-type: none"> <li>Sensitive to adverse weather conditions</li> <li>Accurate direction/aiming is required</li> <li>Lower cost per shot than physical projectiles</li> </ul>	[255]–[263]
Physical	Projectiles	<ul style="list-style-type: none"> <li>Machine guns, munitions, guided missiles, mortars</li> <li>Traditional mitigator to neutralize enemies</li> <li>Quick reaction capability is possible</li> </ul>	<ul style="list-style-type: none"> <li>Precise aiming is required considering gravity/wind</li> <li>High cost per shot</li> <li>Crashed mUAVs may cause the collateral damages</li> </ul>	[264], [265]
	Collision UAVs	<ul style="list-style-type: none"> <li>Collision drones with detecting and tracking capabilities</li> <li>Hybrid of projectiles and small UAVs</li> <li>Effective for contiguous small mUAVs</li> </ul>	<ul style="list-style-type: none"> <li>Approaching and tracking mUAVs are required</li> <li>Chasing with low velocity causes mitigation delays</li> <li>Crashed mUAVs may cause collateral damage</li> </ul>	[191], [266]–[271]
	Nets	<ul style="list-style-type: none"> <li>Net cannons and sky platforms carrying nets are possible</li> <li>Nets equipped with parachutes cause mUAVs to descend safely</li> <li>Possible to extract info. from an mUAV after capturing it</li> </ul>	<ul style="list-style-type: none"> <li>Need to approach mUAVs closely</li> <li>Effective range for mitigation is short</li> <li>Accuracy highly depends on environment</li> </ul>	[272]–[284]
	Eagles	<ul style="list-style-type: none"> <li>Using trained eagles for hunting as mitigators of mUAVs</li> <li>High technology may not be required</li> <li>Fewer human resources are required than in other schemes</li> </ul>	<ul style="list-style-type: none"> <li>Applicable to slower mUAVs and those that are smaller than eagles</li> <li>Injuries to eagles, ineffective for multiple mUAVs</li> </ul>	[49], [285]

adverse weather conditions and may fail to detect objects near the horizon. A mUAV with temperature comparable to background objects may be challenging for IR sensors to detect [45].

### 5) LiDAR

Similar to radar, LiDAR detects mUAVs from signals returning after reflecting off of the mUAVs. Contrary to radar, LiDAR emits laser light (typically, 300 THz–500 THz) to measure the range information from the mUAV. LiDAR can provide 3D representations using differences in return times. Therefore, LiDAR can differentiate a target object from a complex background [242].

In one study [241], the authors proposed an algorithm for detecting small UAVs and generating 3D coordinates by employing LiDAR. In another [101], detecting small UAVs was assessed using a LiDAR system mounted on a vehicle.

However, LiDAR has a short range to detect objects and requires a LoS environment owing to the high frequency of the laser light and its low energy. To extend the range of detection, a data augmentation method and a detection algorithm were studied for detecting UAVs using LiDAR [242]. Moreover, as mentioned in Section IV-A1(1), LiDAR is affected by weather phenomena, such as clouds, fog, rain, falling snow, sleet, and direct sunlight.

## B. MITIGATORS

Mitigation methods have been categorized into nonphysical and physical methods based on whether there is physical damage to the mUAV, as summarized in Table

7 and shown in Fig. 7. In this section, nonphysical and physical mitigators are surveyed.

### 1) Nonphysical Mitigators

Nonphysical mitigators employ EM waves to disrupt, disable, and/or destroy mUAVs. Nonphysical mitigators perform the invisible, silent, and mild mitigation, as there is no physical contact between the mitigator and the mUAV. Because nonphysical mitigators use EM waves, instantaneous maneuvers are possible and are not affected by certain aspects of the physical environments, such as gravity and wind. Thus, nonphysical mitigators can readily aim at target mUAVs. Nonphysical mitigators can be realized by various methods, such as high-power electromagnetics, lasers, and cyber-attacks (e.g., RF/GNSS jamming and spoofing, deauthentication attacks, zero-day vulnerabilities, cross layer attack, multi-protocol attack, denial-of-service on UAV/GCS, address resolution protocol cache poisoning [286]). In our survey, among the cyber-attacks, we focus on RF/GNSS jamming and spoofing which are the majority of the cyber-attacks to mUAVs. See [51], [249], [286], [287] and references therein for the comprehensive survey of cyber-attacks.

- RF/GNSS jamming:** The RF jammers can disrupt or disable mUAVs by interfering with their communication links. By interfering with the communication between mUAVs and the malicious operators, jamming decreases the signal-to-noise ratio (SNR) of the mUAV and disrupts the mUAV [133]. To recover the disrupted communications, the communication signal between the mUAV and the malicious op-

erators must increase, which exposes them clearly to the mitigators. Once the communication link is jammed and degraded, the mUAVs may lose the remote control link and may descend or initiate a RTH mode.

There are several jamming schemes. A jammer can transmit all of its power on a single frequency (spot jamming), shift the power rapidly from one frequency to another (sweep jamming), or transmit power simultaneously over a range of frequencies (barrage jamming). In addition, jammers can be classified as active jammers and reactive jammers. The active jammer transmits RF signals continually, or does so randomly to save energy. The deceptive jammer, a type of active jammer, causes the UAV to receive packets continuously without a gap such that the mUAV remains in a receive mode. The reactive jammer transmits signals only when it detects that the monitored spectrums/channels are occupied by unknown signals, i.e., mUAVs, [244], [245]. However, RF jamming can be ineffective for autonomous mUAVs that do not require any remote control or for mUAVs that follow a preprogrammed route via global positioning system (GPS) checkpoints [288]. Thus, GNSS jamming is required to compensate for the limits of RF jamming.

GNSS jammers interfere with navigation systems. Because the GPS signal comes from a satellite, its power is weak and vulnerable to jamming signals. Once the mUAV loses the GNSS signal, it will hover or land without completing its mission [247]. However, GNSS jamming can be ineffective for mUAVs equipped with inertial measurement unit (IMU) sensors and encrypted signals for the navigation. Therefore, the compensation between RF and GNSS is required.

It is important to note that sky platforms can be employed for effective jamming mitigators, as the jamming performance can be dramatically improved as the distance between the mitigators and the mUAVs becomes shorter [49], [132], [246].

- **Spoofing:** Given the overwhelming technology and/or knowledge of mUAVs, taking control of mUAVs or commanding mUAVs to detour away from a protected area is possible, a technique also known as spoofing. Spoofing mitigators can disrupt, disable, or take control of mUAVs. Spoofing mitigators for mUAVs counterfeit RF or GNSS signals to neutralize mUAVs. Advanced technologies which determine fully the communication protocol stacks, GNSS services, and vulnerabilities of the mUAVs are required to implement spoofing.

GNSS spoofing is a common method when the protocols (e.g., code and modulation types) are known. GPS spoofing can cause mUAVs to hover, engage the autopilot, land, and misdirect to the spoofed route [247], [248]. Appropriate spoofing strategies are

needed for different types of mUAVs to manage them when they lose their lock on the authorized GNSS signals [247].

The spoofing of remote control signals can also be implemented by analyzing the communication protocols in use [249], [250]. Taking full control of mUAVs is possible [250], [251] if the protocols are known and available at the mitigators. Vulnerabilities of Wi-Fi-based UAVs have been studied [249]. Cellular-connected UAVs [252] can also be spoofed by analyzing the vulnerabilities of cellular networks. Furthermore, because mUAVs consist of various embedded systems including a navigation system and a communication system [249], various vulnerabilities of mUAVs can be considered to increase the capabilities of spoofing. With rigorous analysis and overwhelming technologies, spoofing by attacking the vulnerabilities of operating systems, GNSS systems, and wireless communication links can be implemented.

- **High-power electromagnetics:** A high-power EM wave can disable an mUAV by impairing its electronic systems, and these methods can be categorized into two classes: those that use narrowband waves and those that use wideband waves. Narrowband EM waves include high power on a nearly single-tone frequency. A high power narrowband EM wave is referred to as HPM. HPM can couple with the UAV and cause damage such that it becomes disabled. HPM requires very high power, i.e., on the order of thousands of volts on a single frequency [253]. The directed energy of HPM can be used to crash a UAV [254]. Finding an effective frequency to cause malfunctions in mUAVs is the key issue.

On the other hand, the wideband EM wave has short pulses in the time domain. The energy is distributed over a wide band, and the wideband wave EM has a low energy density over the bandwidth. Note that a non-nuclear EMP can hardly be implemented with a large low-inductance capacitor that is discharged into a single loop antenna.

However, high-power EM waves should be precisely directed toward the target mUAV to effectively mitigate it; otherwise, the lethality is significantly decreased, i.e., some devices, e.g., radar and RF sensors, can still operate partially after this type of mitigation [255]. Here, the issue is that it is difficult to evaluate the kill assessment after mitigation.

- **Lasers:** While lasers can be employed as laser range finders and designators, laser as mitigators can disable or destroy mUAVs with directed energy [256]–[263]. An electrolaser ionizes the path to the UAV and emits an electric current down the conducting track of ionized plasma. Lasers can be categorized into low-power lasers and high-power lasers [255]. Low-power lasers can neutralize (dazzle) the sensitive

EO/IR sensors of mUAVs. High-power lasers that operate at the mega-watt level can burn a hole in the mUAV and destroy it. Laser mitigators are affordable compared to physical projectiles [289]. However, laser mitigators require challenging research and development and are sensitive to adverse weather conditions. Furthermore, high-power lasers require accurate directions and sufficient time to track the mUAVs.

## 2) Physical Mitigators

Contrary to nonphysical mitigators, physical mitigators disable and destroy mUAVs physically. Physical mitigators are effective, and the results of whether the neutralization was successful are obvious. Physical mitigators require accurate aiming and/or tracking of the mUAVs to remain physically close to the mUAV to effectively neutralize. Physical mitigators can employ projectiles, collision UAVs, nets, and eagles.

- **Projectiles:** Mitigators that employ projectiles can destroy mUAVs. Projectiles include machine guns, munitions, guided missiles, artillery, mortars, and rockets. Guided projectiles require a guidance system to track and hit the mUAVs. In July of 2014, Israel used a Patriot missile to shoot down an incoming reconnaissance UAV from Gaza [264]. In 2019, SmartRounds Inc. announced a 40 mm missile system for anti-UAV munitions, which can be deployed on ground and sky platforms and that operate at high velocity [265]. The projectile is equipped with a vision sensor for object detection and tracking. However, precise aiming considering gravity and wind is required, and the cost of the projectiles per shot is high. Furthermore, the mUAVs go out of control and crash to the ground, possibly causing collateral damage.
- **Collision UAVs:** Collision UAVs with detection and tracking capabilities can follow the mUAVs to crash into and destroy them. A collision UAV requires high speed to pursue the mUAV, e.g., 350 km/h [266], and is effective for contiguous small mUAVs in protected areas. Collision UAVs can employ a computer-vision-aided object-detection method and carry explosives to maximize the collision impact [268]. More examples of collision UAVs can be found in the literature [191], [269]–[271]. Collision UAVs can be interpreted as a hybrid consisting of a missile and a small UAV. Collision UAVs are disposable and cause collateral damage, similar to projectiles. However, collision UAVs require a relatively large neutralization delay compared to projectiles.
- **Nets:** Net catchers ensnare and demobilize mUAVs. The net can be projected by a net cannon [272]–[276] or can be carried by sky platforms [49], [277]–[283]. Nets can be a solution to mitigate small mUAVs which are difficult to neutralize by guns or guided

missiles [282], [283]. In one study [284], a portable mitigator was demonstrated to be able to capture UAVs. Nets can be equipped with parachutes to ensure that the UAV descends safely for forensic analysis and to prevent collateral damage to other facilities [49]. However, the effective range of net mitigation is short.

- **Eagles:** For centuries, people of the Altai region have trained themselves in the art of eagle hunting. They have trained eagles to catch small animals. Motivated by the people of Altai, Dutch and Scottish police trained eagles as a mitigator of CUSs to neutralize and catch mini-UAVs [49], [285]. Eagle training does not require high technology. To train and breed a mitigator eagle may require fewer human resources than other mitigation devices that are developed by researchers and engineers in various areas. However, eagle mitigators can easily be injured by the blades and propellers of mUAVs, and their use is limited to slower and smaller mUAVs relative to the speed and size of the eagles. Furthermore, eagle mitigators may not be appropriate to mitigate multiple mUAVs simultaneously.

## VI. CUS MARKET

Skyrocketing growth in the UAV industry has created both positive and negative externalities. Well-meaning users of UAVs have successfully benefitted from diverse UAV applications that range from recreation to emergency rescue applications, as introduced in Section II-A. Malevolent users of UAVs also have quickly caught up with the possible malicious applications of UAVs, such as terror, security breaches, and invasions of privacy, to name a few. As a result, market needs for counteracting the negative externalities of UAVs have skyrocketed, in tandem with the recent growth of the civilian UAV industry. However, these market needs are bound to be multi-faceted due to the distinctive characteristics of the CUS market, such as its complete dependence on the UAV industry or the possibility of cannibalizing existing markets. In this section, the landscape of the CUS market is scanned to identify market patterns and anomalies. The CUS market is analyzed in terms of rivalries and major acquisitions/partnerships among incumbents, suppliers or partners of incumbents, as well as those complementary to incumbents and emerging organizations entering the CUS market. Based on the market analysis, the distinct characteristics of the CUS market are identified and elaborated. Lastly, practical implications for industry practitioners, especially those which consider entering the CUS market, such as telecom service providers, are also identified.

### A. DANCING LANDSCAPE OF THE GLOBAL CUS MARKET: WHAT DOES IT LOOK LIKE AND HOW IS IT CHANGING?

The size of the commercial UAV industry is anticipated to make an upsurge, reaching USD 6.3 billion in 2026 with a compound annual growth rate (CAGR) of 23.37% from the market size of USD 1.2 billion in 2018 [290]. The prospects of the commercial UAV industry started to become especially hopeful when Jeff Bezos, the CEO of Amazon, made a surprising appearance on “60 Minutes” in December of 2013, and announced Amazon’s future plan to launch a drone delivery service called Amazon Prime Air. Around the same time, however, the portents of commercial UAVs going rogue had been progressively noticeable. A rogue drone was spotted at Gatineau jail in Quebec in November of 2013, which obviously was an attempted contraband drop-off. A few days later, guards at Georgia State Prison spotted a six-rotor drone carrying packs of tobacco hovering over the prison compound. Six and a half years later, while we are still waiting for Amazon drones to drop off packages onto our door steps, the potential threats of mUAVs have surged, subsequently intensifying the market need for CUS solutions.

#### 1) Market Size and Growth

The CUS market remained in its embryonic stage throughout the 2010s only to witness ‘hockey stick’ growth recently. The current CUS market is estimated to have reached the size of USD 1 billion [291] and is expected to grow to USD 4.5 billion by 2026 [292]. The five-year forecast for the CUS market growth ranges, depending on market research firm, from a CAGR of 16.8% [293], 37.2% [294], to 41.1% [291]. Fig. 8 shows the current size of the CUS market and its anticipated growth over the next five years as estimated by Drone Industry Insights, the German market research and analysis company [295].

#### 2) Geographic Composition

The geographic distribution of the CUS market highlights the dominance of North America, whose market share accounts for more than half of the global CUS market [293], [296]. North America’s CUS market dominance is mostly due to the prolonged and extensive R&D investment by the US Department of Defense (DoD), especially up to 2016, and the subsequent procurement of CUS solutions. Starting in 2016, the DoD shifted its investment focus from R&D to integrating existing technologies and solutions into more comprehensive programs [297]. In order to drive this shift further, the DoD requested USD 500 million for CUS development for the 2020 fiscal year. In sum, although the underlying mechanism has evolved from system development to system integrations, North America’s CUS market dominance is expected to remain strong for the foreseeable future. Europe is the next most active geographic region for the CUS market, where the growth rate is estimated to remain steady [298]. The

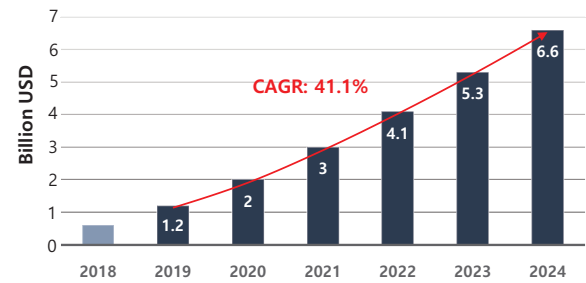


FIGURE 8. CUS (counter-drone) market size and forecast 2019–2024 [295]

strongest driver of the European CUS market’s medium yet steady growth is the presence of globally renowned traditional defense corporations such as the Thales Group in France, Saab AB in Sweden, and BSS Holland BV in the Netherlands. Multiple market research and analysis organizations collectively identify the Asia Pacific CUS market as possessing the most substantial growth potential in the near future [292], [298], [299]. Rapidly increasing government expenditures on defense infrastructure, particularly that of the aerospace industry, in the Asia Pacific region are considered to be the major source of the growth potential. Latin American and African CUS markets are still in their embryonic stages and do not show the potential for robust growth. However, the recently escalating numbers of drone attacks, especially in Latin America, are likely to spark governmental investments in developing CUS technologies, which would subsequently drive market growth in that region.

#### 3) Market Growth Driver

Aside from the obvious market needs to counteract the potential threats posed by mUAVs, the growth drivers of the CUS market are multi-faceted, including both direct and indirect antecedents (as summarized in Table 8).

The most critical and direct driver is the *proliferation of low-price UAVs* that already have created a mass market. While regulations have been keeping pace with the growing UAV industry, as stated in Section II-B, market demands and regulatory changes do not move in sync, forcing regulatory bodies to make continuous updates. Conflicting perspectives on fundamental regulatory issues, such as categorizing UAVs as either ‘flying objects’ or airplanes, prohibits regulatory bodies from reaching a consensus with regard to safety levels. For instance, the National Aeronautics and Space Administration (NASA) considers a relatively narrow industry of UAVs when categorizing them as something between road and air devices, whereas the European Aviation Safety Agency (EASA) maintains a broader view of UAVs, categorizing them at the level of an airline [300]. The expanding UAV

TABLE 8. Drivers and Inhibitors of CUS Market Growth

CUS Market Growth Drivers
<ul style="list-style-type: none"> <li>• <b>Expansion of UAV industry:</b> Recent skyrocketing growth of the UAV industry</li> <li>• <b>Commoditized UAV:</b> The proliferation of inexpensive UAVs</li> <li>• <b>Negative externality:</b> The increasing seriousness of malicious UAV incidents</li> <li>• <b>Favorable conditions for negative externality:</b> increasing accessibility to raw explosive materials</li> <li>• <b>Public perception:</b> Increasing exposure of UAV attacks by the general public</li> </ul>
CUS Market Growth Inhibitors
<ul style="list-style-type: none"> <li>• <b>Technology obsolescence:</b> Rapid technology development and subsequent innovation rates</li> <li>• <b>Security concerns:</b> National security and defense regulation prohibiting CUS exports</li> <li>• <b>Incomplete regulation:</b> Regulatory details for the CUS market, e.g., rules of engagement, being currently developed</li> <li>• <b>Lack of assessment criteria:</b> CUS performance evaluation measures needed</li> <li>• <b>Insufficient cases for analysis:</b> Sufficient number of malicious UAV incidents needed for comprehensive threat profiling</li> </ul>

mass market poses both malicious and benign threats by providing malevolent actors with an asymmetric capability to launch attacks and enabling recreational users to cause unintended security breaches. The other direct driver is the emerging market requirements specifically for portable CUS solutions, i.e., human-packable and mobile platforms.

Indirect drivers are in action as well. Coincident with public exposure to drone swarm technology spiked through international events such as the Winter Olympics [301], major news outlets, e.g., the Financial Times, have recently started to warn the general public about the potential threat of drone swarms [302]. Public perceptions that drone swarms could make coordinated attacks also have kickstarted further R&D investment in drone neutralization technologies. The ever increasing accessibility to raw explosives for building bomblets is another indirect driver of CUS market growth, enabling malevolent culprits to build and detonate DIY bomblets. These market growth drivers are currently adding fuel to the explosion of the CUS market, yet not without mitigating factors.

#### 4) Market Growth Inhibitor

In tandem with multiple market growth drivers, multi-dimensional factors can exist that restrain CUS market growth (summarized in Table 8).

- **Technology obsolescence:** First, new UAV technologies are being developed at a rapid pace. Smaller UAVs that fly longer and are equipped with better aerial imaging units make it progressively difficult for CUS providers to detect and neutralize mUAVs. Knowledge in the area of mUAVs quickly becomes obsolete, which significantly shortens the shelf life of CUS providers' organizational capabilities. Consequently, CUS providers are required to keep up with UAV innovations to launch newly updated countermeasures.

- **Security concerns:** Second, regulatory bodies prohibiting defense-related manufacturers from exporting restrict the global expansion of CUS providers. For instance, the US International Traffic in Arms Regulation prohibits certain American CUS manufacturers from selling overseas. Recently, however, the US government started to clear CUS manufacturers on a case by case basis to export CUS systems strictly to allied nations. For instance, Raytheon was approved by the government to sell the Coyote Block 2 counter-drone weapon to approved allied nations in March of 2020.
- **Incomplete regulation:** Third, the rules of engagement to counteract mUAVs have not yet been fully developed. The US Department of Justice released a guideline to counteract killer drones in August of 2016 based on the 2013 Presidential Policy Guideline to establish standard operating procedures to counteract terror attacks [303]. Although specific rules of drone engagement seem to be in detail, there still exists some wiggle room that could generate multiple interpretations.
- **Lack of assessment criteria:** Fourth, from the perspective of CUS clients, universal assessment criteria to evaluate CUS performance capabilities are non-existent. This seemingly insignificant factor makes it difficult for potential clients to decide whether they need a CUS solution and should choose from among the many CUS companies providing vastly different technologies and solutions. Without standardized assessment criteria, clients are left to compare apples and oranges.
- **Insufficient cases for analysis:** Lastly yet ironically, the general understanding of concrete threat profiles of mUAVs is hardly sufficient at the moment to develop bullet-proof countermeasures due to the limited number of UAV attacks. Akin to the proverbial firefighter in a town where there are no fires,

CUS providers in a market where UAV attacks rarely exist would have a difficult time identifying potential threats and designing a series of counteractions.

##### 5) Market Fragmentation

The civilian CUS market is currently highly fragmented; there is no single dominant player which could exert sufficient influence to drive the entire industry towards its intended direction. Instead, multiple established corporations and diverse small- and medium-sized enterprises (SMEs) together constitute a dynamically evolving ecosystem. The marketplace of solution providers, particularly value-added resellers, is an example of an intrinsically highly fragmented market. Because solution providers are required to customize each solution for individual clients, economies of scale that are usually attained through providing standardized and universally deployable services are unachievable in most cases. The requirements of individual customization and subsequent customer support for an extended period therefore naturally turn away large corporations from entering the market. Local SMEs typically fill this void by leveraging their relatively low-cost structures compared to those of large corporations. The hospitality television market is a typical example of this intrinsically highly fragmented marketplace for solution providers: although many consumer electronics corporations, such as Phillips and Samsung, briefly considered entering the television solution market for hotels, retail outlets, doctors' offices, and cruise ships, none of them found the target market profitable enough. The less than satisfying profitability level can be attributed to the intrinsic nature of this fragmented market, which requires individual customization and continuous customer support. The civilian CUS market followed the footsteps of this intrinsically highly fragmented market until recently: while traditional defense corporations, such as Lockheed Martin and the Thales Group were handling the military needs for CUS hardware and software, regional SMEs such as DroneShield, DeDrone, and Aveillant as new entrants in the CUS market during the 2010s started to provide civilian applications. However, the civilian CUS market growth has shown a significant upsurge recently, becoming substantial enough to attract traditional defense corporations. In this highly fragmented yet organically intertwined market, both established multi-national corporations and regionally based SMEs do not necessarily compete with each other but, rather create symbiotic relationships with one another. Each entity brings the complementary assets to the marketplace, consequently creating overall both competing and cooperating relationships. The next section introduces the current players in the civilian CUS market and the notable acquisitions among them.

##### B. GAME OF DRONES: WHO ARE THE CURRENT MAJOR PLAYERS IN THE CIVILIAN CUS MARKET?

The civilian CUS market has been a dynamically evolving ecosystem which consists of "big fish" in the ocean, i.e., established multinational corporations positioned in the traditional defense industry, such as Lockheed Martin, Thales, Raytheon, Saab, and BSS Holland, and "small fish" in the pond, i.e., emerging startups and SMEs positioned in local civilian CUS markets, such as Aveillant, DroneShield, Dedrone, Citadel Defense, and Liteye, as well as a special batch of "small fish" in the pond, i.e., spinoff companies from SMEs such as Fortem Technologies as a spinoff of ImSAR LLC. Table 9 showcases a selective group of established corporations and small enterprises in the global CUS market. In this section, big fish and small fish are analyzed to understand the current ecosystem of the global civilian CUS market. Recent acquisitions between big fish and small fish which have blurred the boundaries between oceans and regional ponds are also analyzed in this section.

###### 1) Big Fish in the Ocean

North American and European defense industries have been ruled by a group of dominant players.

- **North America:** The North American defense triumvirate, i.e., i) Lockheed Martin, ii) Northrop Grumman, and iii) Raytheon, boasts expansive product and service portfolios catering to the aerospace and defense industries. All three corporations have a strong foothold in the military UAV industry: i) Lockheed Martin's Indago, Condor, and Stalker [317], ii) Northrop Grumman's Global Hawk [318], and iii) Raytheon's Coyote and Silver Fox UAVs are all-time major players in military UAV systems [270], [319]. Among the triumvirate, Lockheed Martin entered the civilian CUS market by introducing ICARUS, a Q-53 radar system that detects mUAVs and triggers a kill chain to defeat targets using its Advanced Test High Energy Asset System (ATHENA), a transportable ground-based system equipped with a 30 kilowatt laser beam [320]. In comparison, both Northrop Grumman's Drone Restricted Access Using Known EW (DRAKE) CUS system [321], which is a radio frequency negation system delivering a non-kinetic electronic attack, and Raytheon's Coyote CUS system [270], which consists of Ku-band multi-spectral detecting and high-energy laser neutralization functions, strictly target military applications.
- **European:** European triumvirate corporations in the CUS market consist of the Thales Group in France, Saab AB in Sweden, and Blihter Surveillance Systems Ltd. in the UK. In contrast to the military-centric product and service portfolio of the North American triumvirate, European triumvirate serves both the military and civilian markets. Compared

**TABLE 9. Exemplary Companies in The Global CUS Market (Alphabetic order)**

Company (Country)	Industry	UAV/CUS Product, Service Portfolio	Strength	Partnerships / M&As
Aveillant (UK) [304]	CUS	–/Gamekeeper 16U	Holographic radar	Acquired by Thales Group (Nov. 2017)
Blighter Surveillance Systems (UK) [305]	Defense	–/AUDS inc. Hawkeye tracker	Turn-key solution	–
Citadel Defense (US) [306]	CUS	–/Titan	Artificial intelligence-based proprietary algorithm	Partnered with Liteye for its hardware competence (Mar. 2020)
Dedrone (US) [39]	CUS	–/DroneTracker	Machine learning-based algorithm with proprietary UAV database	Partnered with Batelle for neutralization features
Drone Defense (UK) [307]	CUS	SkyFence, AeroSentry, AeroSnare, NetGun, Paladyne/–	Turn-key solution, AeroGuards–human CUS guard–service, security consulting	–
DroneShield (AU) [308]	CUS	–/DroneSentinel, RfZero, RfPatrol, DroneGun	Proprietary acoustic detection strategy	Acquired by Thales Group (May 2019)
Liteye (US) [309]	CUS	–/AUDS, mobile AUDS	Radar surveillance technology	Partnered with Citadel Defense for its software competence (Mar. 2020)
Lockheed Martin (US) [310]	Aerospace & defense	Indago3, Condor XEP, Stalker XE/ICARUS + ATHENA	Radar surveillance technology	–
Northrop Grumman (US) [311]	Aerospace & defense	Global Hawk/ DRAKE	Radar surveillance technology	Partnered with Liteye for US Army’s MFI (Nov. 2018)
Raytheon (US) [312]	Aerospace & defense	Silver Fox, Coyote/ Coyote CUS	Radar and missile technology	–
Saab AB (SE) [313]	Aerospace & defense	–/Giraffe ELSS	Radar surveillance technology	–
SkySafe (US) [314]	CUS	–/DroneFox Tactical & Fortify	Turn-key solution, security consulting	–
Thales Group (FR) [315]	Aerospace & defense	WatchkeeperX, Spy ranger, Fulmar/EagleSHIELD inc. Horus Captor	Turn-key solution	Acquired Aveillant (Nov. 2017) and DroneShield (May 2019)
WhiteFox Defense Technologies (US) [316]	CUS	–/DroneFox Tactical & Fortify	Turn-key solution, security consulting	–

to the heavy weight champions of Thales and Saab, whose legacy products and service portfolios heavily rely on military applications, the UK’s Blighter Surveillance System plays a relatively light-weight game specifically focused on the CUS market. Blighter’s Anti-UAV Defense System (AUDS) solution combines Blighter’s A400 Series air security radar with its HawkEye video tracker armed with a directional radio frequency inhibitor for signal jamming in order to serve areas of demand in the civilian market, such as airports, nuclear power plants, and high-end commercial compounds, in addition to defense, national border security, law enforcement, and coastline security. Blighter’s AUDS is the most ambidextrous, full-stack CUS solution among those of the European triumvirate, consisting of Blighter’s hardware capability in radar technology and its proprietary software. Saab and Thales, on the other hand, have a stronger presence in terms of hardware capability. Moreover both corporations also offer a wide range of UAV products and solutions, such

as Saab’s Skeldar Series and Thales’s WatchkeeperX, Spy ranger, and Fulmar models. As a result, the prospect of the emerging and booming CUS market poses a Catch-22 for both Saab and Thales by placing both companies in the position of a locksmith who is tasked with inventing both an unlockable lock and passe-partout. An all-out war in the CUS market by Saab and Thales would cannibalize their own UAV markets. As a result, both Saab and Thales shy away from entering the CUS market in full force, rather adopting an alternative route of focusing on the detecting and tracking functions of the CUS system by leveraging their existing radar technologies. Saab’s Giraffe Enhanced Low, Slow and Small (ELSS) CUS system is built on its Giraffe surveillance radar, whereas Thales’s Horus Captor is built on its short-range, low-altitude surveillance radar. Thales, however, has recently went one step further: Thales acquired Aveillant, a UK company developing drone detection solution using holographic radar technology, in November of 2017, later acquiring

Drone Shield, an Australian CUS solution company, in May of 2019. Mostly owing to these back-to-back major acquisitions, Thales recently made the biggest splash in the civilian CUS market by launching EagleSHIELD, a turn-key CUS solution to detect, track, and neutralize mUAVs, in November of 2019. Thales's Horus Captor is integrated with Drone Shield's neutralization systems, whose defeat functions range from hijacking, jamming, interception, to both electronic and physical destruction. Thales's acquisitions reflect the inherent nature of highly fragmented markets: numerous small fish in local ponds.

## 2) Small Fish in the Pond

The 2010s witnessed the simultaneous sprouting of new entrants in the CUS market; rather dormant market of CUS products and services suddenly became crowded with US firms, such as Aveillant, Dedrone, DroneShield, Airspace Systems, SkySafe, Citadel Defense, WhiteFox Defense Technologies and Liteye Systems. Table 9 summarizes the CUS product and service portfolios of these incumbents. Concurrent with the active market dynamism in the civilian CUS market, the entire CUS ecosystem became more vibrant with large-scale defense contracts, such as the US Army awarding Leonard DRS, one of the top US defense contractors, with a \$42m contract to develop CUS capability in October of 2017 [322]. In 2019, the US DoD spent \$900m on developing CUS solutions [297]. This series of large-scale cash injections by the military sector subsequently fertilized the civilian CUS market through defense contractors teaming up with CUS firms as suppliers. For instance, Liteye Systems partnered with Northrop Grumman to combine Liteye's counter UAS defense system with Northrop Grumman's Stryker Infantry Carrier Vehicle to create a combat-level, powerful CUS solution. The majority of small enterprises in the CUS market possess hardware technologies that offer a competitive advantage, such as DroneShield's proprietary acoustic detection technology, Aveillant's holographic radar technology, and Drone Defense's solar-powered off-grid radio frequency scanning and detection technology [323], to name a few.

A subgroup of firms armed with strong hardware capabilities specifically focus on neutralization technology, such as the DroneHunter interceptor drone by Fortem Technologies equipped with its interdependent subsystem known as DroneHangar, a charging deck, and a netting gun.

On the other hand, a group of small enterprises in the CUS market proudly has a strong competitive advantage in terms of software capabilities. For instance, Dedrone's DroneTracker software is built based on a machine learning-based algorithm to recognize and classify mUAVs. Dedrone also developed a proprietary database of all UAVs currently available in both military and

civilian markets. SkySafe's Airspace Galaxy is also built on top of machine learning-based algorithms to detect and identify mUAVs. Citadel Defense's Titan is built on top of its artificial-intelligence-based proprietary algorithms.

These asymmetric competitive advantages among small enterprises in the CUS market are mostly due to the limited level of slack resources, including both tangible and intangible assets. This asymmetry in competitive advantages motivates small enterprises to search for potential partnerships with existing or potential competitors whose resources and capabilities would complement their own. Partnerships between small enterprises with complementary capabilities are most common. For instance, Citadel Defense recently complemented its weakness in hardware capability by pitching its strength in CUS software and striking a partnership with Liteye, whose strength is in hardware technologies, in March of 2020 [324]. Pathway 1 in Fig. 9 represents the prototypical pathway that SMEs with different competitive advantages take by partnering with competitors whose competitive advantages complement their own. In addition to these types of partnerships among small incumbents in the CUS market, there also exists a particular group of potential competitors which could help small enterprises to expand to the global scale: the big fish in the ocean.

## 3) Small Fish Moving Forward to the Ocean Through Big Fish

Those small enterprises that strike partnerships with established corporations are likely to gain a foothold quickly to expand themselves into larger markets. Pathway 2 of Fig. 9 visualizes the prototypical pathway that SMEs take to reach global markets by partnering with established corporations or even acquiring certain divisions of established corporations. For instance, Dedrone, whose competitive advantage is significantly lopsided given its strong software capability, purchased all assets and intellectual properties associated with Batelle's DroneDefender, a 15-lb man-portable CUS shoulder rifle, in October of 2019 [325]. Dedrone's product and service portfolio initially leaned heavily towards detecting and tracking mUAVs using Dedrone's machine learning-based DroneTracker software integrated with radio frequency sensors and pan-tilt-zoom cameras. SMEs strike partnerships with established corporations for a certain project or product/service portfolio to extend their global reach, as represented by Pathway 3 in Fig. 9. Liteye's series of partnerships with established aerospace and defense corporations, such as Raytheon and Northrop Grumman, are other examples which represent partnerships between small enterprises armed with customizable solutions and established corporations possessing advanced technology-based products. Liteye partnered with Northrop Grumman to integrate Liteye's AUDES into Northrop Grumman's armored vehicle, the Stryker Infantry Carrier Vehicle, and introduced the integrated

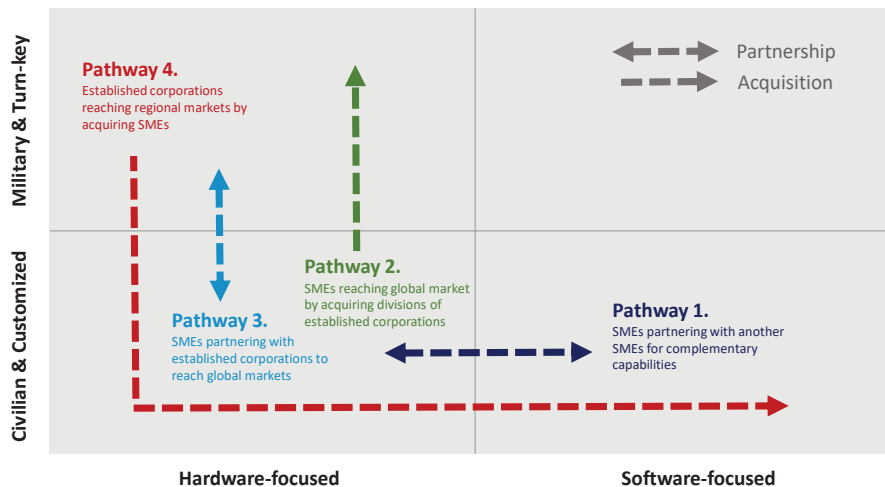


FIGURE 9. Map of CUS market dynamics showing acquisitions (---) and partnerships (---)

system at the US Army’s Maneuver and Fires Integration Exercise in November of 2018 [326]. Most recently, Liteye teamed up with Raytheon Missile & Defense to integrate Liteye’s AUDS with Raytheon’s Phaser™ high-powered microwave system in April of 2020 [327]. DEDRONE’s acquisition of Bettelle’s neutralization system or Liteye’s partnerships with Raytheon and Northrop Grumman showcase partnerships between regional enterprises with a specific yet short range of capabilities and established or even multinational corporations with a diverse portfolio of products and services where regional enterprises seize lucrative opportunities to move forward to larger market while established corporations relatively inexpensively acquire necessary and highly specific assets. Occasionally partnerships between small enterprises and established corporations are leveraged in the opposite direction, where a big fish attempts to reach regional yet highly lucrative ponds by swallowing smaller fish.

#### 4) Big Fish Reaching the Pond Through Small Fish

Established corporations generally expand into solution markets by acquiring regional SMEs with a proven track record. Pathway 4 in Fig. 9 presents the prototypical route used by established corporations in the aerospace and defense industry target to move into to the CUS market, i.e., by acquisition. Thales acquired Aveillant, the British CUS company with proprietary holographic radar technology, in November of 2017 and subsequently established Aveillant Limited Thales Company Operational Solutions Ltd. [328]. Shortly before the acquisition, Aveillant had proved its competency in the civilian CUS market by installing its Gamekeeper CUS system in Monaco on April of 2016 [329]. Aveillant’s grand entrance into the global CUS market immediately sparked clients’ interest in CUS solutions. In April of 2017, Singapore’s ST Electronics

installed Aveillant’s Gamekeeper near the Singapore Flyer attraction [330]. Paris Charles de Galle Airport in Paris was the third international VIP client of Aveillant, installing Gamekeeper in July of 2017 [331]. Three major international installations provided Thales with sufficient validation to its decision to acquire Aveillant. Shortly after the Aveillant acquisition, Thales then acquired DroneShield, an Australian CUS company specialized in acoustic UAV detection technology, in May of 2019 [332].

## VII. CHALLENGES AND FUTURE DIRECTION

In this section, we present the challenges and future direction for the CUS research and the vision of the CUS market.

### A. LIMIT AND CHALLENGES OF CUS NETWORKS

A single platform can hardly cope with unpredictable threats from emerging mUAVs, and multiple platforms in CUS networks providing diversity and reliability will be a promising solution. Intercommunication between the platforms is a critical factor that allows the system effectively to operate integrated CUS and CUS networks. Proper network and communication performance satisfying mission requirements is the key issue to maximize the performance of an integrated CUS network.

Integrated CUS networks can consist of static/mobile ground platforms, human-packable platforms, and high/low altitude sky platforms. These networks among (quasi-)static ground platforms are represented as a mobile ad hoc network (MANET); networks among mobile ground platforms are represented as a vehicle ad hoc network (VANET); and networks among sky platforms are represented as a flying ad hoc network (FANET). These respective ad hoc networks have unique characteristics in terms of mobility, topology, topology changes, energy

constraints, and uses [69]. Furthermore, networks having different objectives, e.g., detection, computation, and neutralization, have different communication requirements, e.g., rates, latencies, and mobility levels.

Therefore, incorporating the unique characteristics of the network type (i.e., MANET, VANET, and FANET) and the network role, integrated CUS networks must be flexible and manageable. These networks must balance/optimize the requirements, e.g., platform mobility, robust transmission links, delay, scalability, multiple access schemes, and limited resource allocation. To deal with CUS network optimization, software-defined networking (SDN) and network function virtualization (NFV) technologies can effectively manage the resources for an inter-operable CUS with various platforms [333], [334]. It is worth noting that the UAVs in a CUS network not only be benefitted by SDN/NFV, but also support other platforms as programmable network nodes [56], [335]–[337] (see [333] and references therein for the survey of UAV related SDN/NFV). For example, SDN and NFV can handle flexible power allocation, coordination of the bandwidth/channel allocation, and routing algorithms. Unified management and optimization of the dynamic configuration of the networks can be realized through SDN and NFV. SDN decouples the control plane from the data plane and simplifies network management and control [338], [339]. NFV decouples the hardware and software and enhances the flexibility of the networks by using virtualization techniques [340]. It is noteworthy that *network slicing* can also achieve flexible and manageable networks that can be realized with SDN and NFV. Network slicing refers to a logical network that can provide mission-specific capabilities [341]. Satellite communications beyond HAPs can also be considered to implement SDN-based high-performance communications. Heterogeneous satellite communication networks can be interoperable with ground/sky platforms and can provide flexibility according to the service requirements based on SDN and NFV [342], [343].

CUS networks need to be designed carefully to satisfy multiple objectives with the capabilities of flexibility and manageability. These networks can be centralized/decentralized and homogeneous/heterogeneous to balance the tradeoff between robustness and performance; however, their architecture is fixed which limits their performance. Emerging technologies such as SDN, NFV, network slicing, and resource optimization will enable these networks to be flexible and manageable in terms of communications and networking performances.

### B. DEARTH OF ASSESSMENT CRITERIA FOR CUSS

To tackle with dearth of assessment criteria which was explained in Section VI-A, several objectives as well as analytical and experimental studies can be investigated. We propose a few performance objectives including mUAV neutralization probability (mUNP), expected loss of profit

(ELP), covering space per cost (CSC), mitigation completion time (MCT), mitigation completion power (MCP), capacity of mitigation (COM), mitigation cycle of CUS (MCC), and operating duration of CUS (ODC), as follows:

- **mUNP:** It is defined as  $P_d P_m$  where  $P_d$  and  $P_m$  are detection and mitigation probabilities, respectively. The mUNP then represents the success probability of CUS mission. An instantaneous mUNP can be maximized by allocating resources, e.g., power, spectrum, and sensing time, to the devices and functions for the given CUS platforms and architectures, and an average mUNP can be employed by designing and deploying the CUS platforms and architectures. When an mUAV approaches from a blind spot, we can consider the worst-case mUNP and maximize it so that lower bound of neutralization performance is increased, resulting in a robust CUS.
- **ELP:** It is defined as  $(1 - P_d P_m)E[C_p] + P_f E[C_c]$ , where  $E[C_p]$  denotes the expected damage cost in a protective area,  $P_f$  denotes a false alarm probability, and  $E[C_c]$  denotes expected collateral damage caused by the false alarm. The ELP represents the expected net cost by operating the CUS, which should be minimized in the design of CUS.
- **CSC:** It is space that can be covered by a single CUS with the normalized cost of resources. In other words, CSC represents how broad space can be effectively covered by a CUS by using normalized resources, such as power, spectrum, and sensing time. In open space, the CSC is equivalent to the maximum range (distance) of the effective mitigation of CUS per unit resource use.
- **MCT/MCP:** It is a required time/power to successively mitigate a single mUAV. Based on MCT/MCP, we can predict the required time/power consumption to mitigate multiple mUAVs and to complete a mission in various attack scenarios of mUAV.
- **COM:** It is the largest number of mUAVs that CUS can *simultaneously* mitigate. COM can be used to determine how many CUSs are required to cover the target area and how to schedule them to effectively protect the target area.
- **MCC:** It is a number of mUAVs that CUS can mitigate per unit time. MCC can be used with COM to design the defense systems.
- **ODC:** It is an operating duration that CUS can continuously operate without recharging or returning to a base. These performance criteria should be studied and employed according to several specific scenarios (e.g., 24/7-operation requirement and ultra-sensitive areas).

### C. TECHNOLOGICAL CHALLENGES AND STRATEGIES

To enhance the performance of CUSs and achieve the objectives introduced in the previous subsection, there are still numerous technological challenges remaining.

The technological challenges/issues and strategies to achieve/resolve them are summarized as follows:

- **Fundamental framework and prototype for CUS:** Fundamental framework for CUS has not been fully characterized and analyzed in both academia and industries. Since CUS is an integration of various technologies, such as wireless communications, networks, control theory, mechanics, and computer science, more comprehensive frameworks are required to effectively integrate them.
- **Dynamic and flexible CUS networks:** Since each platform has unique benefits and limitations in terms of the mobility, topology, energy cases, and usages, a dynamic and flexible CUS network is desired to significantly improve the CUS performance. For example, networking the sensing, C2, and mitigation systems to flatten the hierarchy, reduce the operational pause, enhance precision, and increase the response speed of command [156]. Here, SDN/NFV could be a relevant solution to establish the dynamic and flexible networks.
- **Fusion or confusion?:** The CUS consists of various sensors, each of which collects and provides heterogeneous information. Direct merge of various data with the lack of caution may confuse rather than clarify the decision of CUS. The heterogeneous data should be intelligently fused to establish robust and effective sensing systems that can correctly detect/identify, authorize, localize, and track the mUAVs. For the intelligent fusion of sensing data, recently and dramatically developed artificial intelligent (AI) technologies could enhance performance of data fusion.
- **Automation and fast computation:** MCT is a critical factor to protect skies. Inefficient computing strategies of C2 systems as well as human interventions cause significant latency and large MCT. To reduce the computing time, edge computing can be employed in which nearby edge nodes provide computation to CUS. Edge computing can also provide stronger security and better interoperability. On the other hand, AI can minimize human interventions to enhance CUS performance.
- **Catch me if you can:** The rapid and innovative development of UAVs make the existing CUS obsolete. To prepare for every eventualities including attacks from mUAVs performing cyberattacks (e.g., GNSS/RF jamming and spoofing), the knowledge of the state-of-the-art mUAV is required. It is however challenging to identify all types of mUAVs and obtain the information of the mUAVs. Therefore, the physical mitigation which uses less or none of knowledge about mUAVs is required (see Section V.B.2). For the physical mitigation, the mUAV tracking and chasing algorithms should be developed as stated in Section

III.B. Also, the fast and accurate mobility of mobile platforms (e.g., ground mobile and sky platforms) should be studied.

- **Price reduction:** The price of UAVs is decreasing and more affordable, whereas the price of CUS is much more expensive than UAVs. The asymmetric cost between UAV and CUS would hinder the defenders from protecting wide exposed area. Therefore, improving the energy efficiency of CUS is important to make CUS sustainable and reusable to cover wide area. Furthermore, developing the low-cost sensors/mitigators is critical to reduce the price of CUS, so that wide area can be protected with low cost.

#### ***D. YIN AND YANG OF THE CUS INDUSTRY: WHAT ARE THE LESSONS FOR ADJACENT MARKET PLAYERS?***

The rise of the UAV industry has become the backdrop of a modern-day gold rush: multiple stakeholders ranging from manufacturers to service providers have quickly filled the emerging ecosystem of UAVs. One group of the stakeholders has arrived at the scene with malevolent intentions and has abused the newly developing UAV innovations. The global CUS market blossomed as a direct response to this unmet market need that had been created by negative externalities of the UAV industry. As a result, the CUS market shows a few characteristics that are distinctively different from the majority of newly created technology markets (as summarized in Table 10).

- First, the current market needs in the CUS market entirely depend on the activities, especially those with negative impacts, in the UAV industry. On the other hand, the UAV industry also partially depends on the activities in the CUS market to a certain degree, although the level of dependence is much lower than that of the CUS market. This mutual dependence creates a type of yin and yang dynamics between the UAV industry and the CUS market: one system's activities have direct impacts on the other system, and vice versa, and one system can hardly exist independently without the other system's prosperity. However, it is quite a stretch to label the UAV and CUS market as yin and yang dynamics owing to the mutual yet asymmetric interdependence that exists.
- This creates the second characteristic of the CUS market: temporal precedence of the UAV industry, which is necessary for the CUS market to emerge. Without negative externalities in the UAV industry, the market need for the CUS market would never have existed.
- Third, the market size and growth rate of the CUS market entirely depend on the size and growth rate of negative externalities in the UAV industry as well. Without the perceived threats of mUAVs,

**TABLE 10.** Yin and Yang of the UAV and CUS Industries: What are the Lessons for Adjacent Market Players?

• <b>Asymmetric interdependence of UAV &amp; CUS industry</b>	Complete dependence of the current CUS needs on the UAV industry versus partial dependence of the UAV industry on the growth of the CUS market
• <b>Temporal precedence of the UAV industry</b>	Negative externalities of the UAV industry precede the market needs for CUSs
• <b>Bounded growth potential of the CUS market</b>	Complete dependence of the CUS market size and growth on the UAV industry
• <b>Wild card in regulatory changes</b>	Market saturation and demise of CUSs being a function of future regulatory changes and those of the UAV industry
• <b>Risk of cannibalization</b>	Tapping into both UAV and CUS markets requires a willingness to cannibalize

the anticipated growth of the CUS market is highly unlikely.

- Fourth, market saturation and the demise of the CUS market in future depend not only on that of the UAV industry but also on potential changes in UAV regulations. If UAV regulatory changes are geared towards more a laissez-faireism approach, negative externalities of the UAV industry are also expected to be substantiated, which consequently would facilitate the growth of the CUS market. On the other hand, if UAV regulations move towards more conservative and strict domains, the negative externalities of the UAV industry would automatically be contained, thus inhibiting the growth of the CUS market.
- Lastly, tapping into both the UAV and CUS markets will create the ultimate Catch-22 of cannibalizing one's own product and service portfolio. These distinct characteristics of the global CUS market pose unique opportunities for industry players in adjacent markets, such as telecommunication service providers, consumer electronics companies, and software companies. Although still highly uncertain, potential entrants to the CUS market, especially established corporations, may have to draw an analogy from large corporations in the aerospace and defense industry, such as Lockheed Martin, Northrop Grumman, and Thales. Due to the limited nature of market opportunities in the CUS market, as explained in this section, corporate entrants should heed Thales's strategy of acquiring regional small enterprises with strong capabilities in integrated CUS solutions.

We also investigate the new industry emergence and market dynamics of CUS in this study. Our findings in this section highlight the emergence process of the CUS industry and the distinctive characteristics of the current CUS market. Due to the limited number of market incumbents which is the innate limitation of the newly emerging industry and market, however, qualitative analysis approach was the only viable option for this study. As the CUS industry evolves and more incumbents enter the CUS market, future research would be able to leverage diverse methodologies including quantitative or mixed method. For instance, as the CUS industry matures, markets are likely to be further multi-layered,

i.e., incumbents becoming more specialized in narrowly focused product and service portfolios. Based on the findings of this study, further investigation on prototypical incumbents and their alliance networks would reveal further market dynamism of the CUS industry.

## VIII. CONCLUSION

In this paper, we have provided a comprehensive survey of CUSs based on a top-down approach. Starting with UAV applications, the survey has explored the platforms, architectures, and devices and functions of CUSs. Various types of platforms, systems, and devices have been introduced and their pros and cons and associated challenging issues have been examined. CUS platforms have been categorized as ground and sky platforms with the networks connecting them based on the operating region. A lower-level taxonomy of CUSs, i.e., an architecture, was then introduced, including three systems, sensing, C2, and mitigation systems. In the lowest level of the CUS taxonomy, two essential devices for CUSs, sensors and mitigators, were reviewed. Finally, we surveyed the CUS market and revealed its dynamics and unique characteristics. From this survey, we have identified rapidly and dynamically growing studies and businesses related to CUSs. We believe that this in-depth survey of CUSs provides a timely and unique guideline for CUS development, regulation implementation, and industry collaboration.

## ACKNOWLEDGMENT

The authors wish to express their deep appreciation for the support rendered by the members of the Next-Generation Unmanned Vehicle Wireless Communication Lab (including the Mobile Communication Lab and Intelligent Wireless Systems Lab) at Chung-Ang University. In particular, the authors thank Saquib Khan, Jimin Lee, and Hangyeol Lee for their help with the collection and summarizing of some data parts in Sections II, V, and VI.

## REFERENCES

- [1] S. Herrick. (2017, Nov.) What's the difference between a drone, UAV, and UAS? [Online]. Available: <https://botlink.com/blog/whats-the-difference-between-a-drone-uav-and-uas>
- [2] M. Germen, "Alternative cityscape visualisation: Drone shooting as a new dimension in urban photography," *Electronic visualisation and the arts*, pp. 150–157, Jul. 2016.

- [3] E. Kaufmann, M. Gehrig, P. Foehn, et al., "Beauty and the beast: Optimal methods meet learning for drone racing," in *2019 Int. Conf. on Robotics and Automation (ICRA)*, May 2019, pp. 690–696.
- [4] E. Kaufmann, A. Loquercio, R. Ranftl, A. Dosovitskiy, V. Koltun, and D. Scaramuzza, "Deep drone racing: Learning agile flight in dynamic environments," in *Conf. on Robotic Learning (CoRL)*, 2018, Oct. 2018.
- [5] T. Tozer, D. Grace, J. Thompson, and P. Baynham, "UAVs and HAPs-potential convergence for military communications," in *IEE Colloquium on Military Satellite Commun. (Ref. No. 2000/024)*, Jun. 2000, pp. 10/1–10/6.
- [6] M. Quigley, M. A. Goodrich, S. Griffiths, A. Eldredge, and R. W. Beard, "Target acquisition, localization, and surveillance using a fixed-wing mini-UAV and gimbaled camera," in *Proceedings of the 2005 IEEE Int. Conf. on Robotics and Automation*, Apr. 2005, pp. 2600–2605.
- [7] R. Schneideman, "Unmanned drones are flying high in the military/aerospace sector [special reports]," *IEEE Signal Process. Mag.*, vol. 29, no. 1, pp. 8–11, Jan. 2012.
- [8] P. Iscold, G. A. S. Pereira, and L. A. B. Torres, "Development of a hand-launched small UAV for ground reconnaissance," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 46, no. 1, pp. 335–348, Jan. 2010.
- [9] J. Y. C. Chen, "UAV-guided navigation for ground robot tele-operation in a military reconnaissance environment," *Ergonomics*, vol. 53, no. 8, pp. 940–950, Jul. 2010.
- [10] T. Coffey and J. A. Montgomery, "The emergence of mini UAVs for military applications," *Defense Horizons*, no. 22, p. 1, Dec. 2002.
- [11] A. Butt, S. Irtiza Ali Shah, and Q. Zaheer, "Weapon launch system design of anti-terrorist UAV," in *2019 Int. Conf. on Engineering and Emerging Technologies (ICEET)*, Feb. 2019, pp. 1–8.
- [12] (2020, Sep.) Federal aviation administration. [Online]. Available: [https://www.faa.gov/uas/resources/by\\_the\\_numbers](https://www.faa.gov/uas/resources/by_the_numbers)
- [13] EY India. (2019, Nov.) What's the right strategy to counter rogue drones? [Online]. Available: [https://www.ey.com/en\\_in/emerging-technologies/whats-the-right-strategy-to-counter-rogue-drones](https://www.ey.com/en_in/emerging-technologies/whats-the-right-strategy-to-counter-rogue-drones)
- [14] P. Tokekar, J. V. Hook, D. Mulla, and V. Isler, "Sensor planning for a symbiotic UAV and UGV system for precision agriculture," *IEEE Transactions on Robotics*, vol. 32, no. 6, pp. 1498–1511, Dec. 2016.
- [15] H. Xiang and L. Tian, "Development of a low-cost agricultural remote-sensing system based on an autonomous unmanned aerial vehicle (UAV)," *Elsevier Biosystems Engineering*, vol. 108, no. 2, pp. 174–190, Feb. 2011.
- [16] P. Grippa, "Decision making in a UAV-based delivery system with impatient customers," in *2016 IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, Oct. 2016, pp. 5034–5039.
- [17] K. T. San, S. J. Mun, Y. H. Choe, and Y. S. Chang, "UAV delivery monitoring system," in *2017 Asia Conf. on Mechanical and Aerospace Engineering (ACMAE 2017)*, vol. 151, no. 04011, Feb. 2018.
- [18] N. K. Yang, K. T. San, and Y. S. Chang, "A novel approach for real time monitoring system to manage UAV delivery," in *2016 5th IIAI Int. Congress on Advanced Applied Informatics (IIAI-AAI)*, Jul. 2016, pp. 1054–1057.
- [19] B. D. Song, K. Park, and J. Kim, "Persistent UAV delivery logistics: MILP formulation and efficient heuristic," *Elsevier Computers Industrial Engineering*, vol. 120, pp. 418–428, Jun. 2018.
- [20] S. Bang, H. Kim, and H. Kim, "UAV-based automatic generation of high-resolution panorama at a construction site with a focus on pre-processing for image stitching," *Automation in Construction*, vol. 84, pp. 70–80, Dec. 2017.
- [21] Z. Shang and Z. Shen, "Real-time 3d reconstruction on construction site using visual SLAM and UAV," *arXiv preprint arXiv:1712.07122*, Dec. 2017.
- [22] A. Mohamed, E. K. Amr, L. Faraj, and Y. Halim, "3-D placement of an unmanned aerial vehicle base station (UAV-BS) for energy-efficient maximal coverage," *IEEE Wireless Commun. Letts.*, vol. 6, no. 4, pp. 434–437, May 2017.
- [23] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, "Placement optimization of UAV-mounted mobile base stations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 604–607, Mar. 2017.
- [24] C. T. Cicek, H. Gultekin, B. Tavli, and H. Yanikomeroglu, "UAV base station location optimization for next generation wireless networks: Overview and Future Research Directions," in *2019 1st Int. Conf. on Unmanned Vehicle Systems (UVS)*, Feb. 2019, pp. 1–6.
- [25] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.
- [26] S. Zhang, H. Zhang, Q. He, K. Bian, and L. Song, "Joint trajectory and power optimization for UAV relay networks," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 161–164, Jan. 2018.
- [27] Y. Chen, W. Feng, and G. Zheng, "Optimum placement of UAV as relays," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 248–251, Feb. 2018.
- [28] P. D. Bravo-Mosquera, L. Botero-Bolivar, D. Acevedo-Giraldo, and H. D. Cerón-Muñoz, "Aerodynamic design analysis of a UAV for superficial research of volcanic environments," *Aerospace Sci. and Technol.*, vol. 70, pp. 600–614, Nov. 2017.
- [29] K. Kanistras, G. Martins, M. J. Rutherford, and K. P. Valavanis, "A survey of unmanned aerial vehicles (UAVs) for traffic monitoring," in *2013 Int. Conf. on Unmanned Aircraft Systems (ICUAS)*, May 2013, pp. 221–234.
- [30] T. E. Villa, F. Salimi, K. Morton et al., "Development and validation of a UAV based system for air pollution measurements," *Sensors*, vol. 16, no. 12, p. 2202, Nov. 2016.
- [31] J. Moore, "UAV fire-fighting system," U.S. Patent US20130134254A1, May, 2013.
- [32] S. Gallagher. (2013, Sep.) German chancellor's drone "attack" shows the threat of weaponized UAVs. [Online]. Available: <https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/>
- [33] M. S. Schmidt and M. D. Shear. (2015, Jan.) A drone, too small for radar to detect, rattles the white house. [Online]. Available: <https://www.nytimes.com/2015/01/27/us/white-house-drone.html>
- [34] S. White. (2015, Apr.) Japanese man arrested for landing drone on PM's office in nuclear protest. [Online]. Available: <https://www.reuters.com/article/us-japan-nuclear-drone/japanese-man-arrested-for-landing-drone-on-pms-office-in-nuclear-protest-idUSKBN0NG04520150425>
- [35] R. Whittle. (2015, Jul.) Military exercise black dart to tackle nightmare drone scenario. [Online]. Available: <https://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/>
- [36] E. Zorn. (2015, Feb.) We must ban drones before it's too late. [Online]. Available: <https://www.chicagotribune.com/columns/eric-zorn/ct-drones-ban-chuy-garcia-rahm-emanuel-perspec-0302-jm-20150227-column.html>
- [37] D. Cenciotti. (2018, Aug.) Video shows what appears to be the first known drone attack on a head of state. [Online]. Available: <https://www.businessinsider.com/drone-attack-on-venezuela-nicolas-maduro-may-be-first-against-leader-2018-8>
- [38] A. H. Michel, "Counter-drone systems," Center for the Study of the Drone at Bard College, Tech. Rep., Dec. 2019. [Online]. Available: <https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>
- [39] (2020) DEDrone. [Online]. Available: <https://www.dedrone.com>
- [40] H. Nakamura and Y. Kajikawa, "Regulation and innovation: How should small unmanned aerial vehicles be regulated?" *Technol. Forecasting and Social Change*, vol. 128, pp. 262–274, Mar. 2018.
- [41] C. Stöcker, R. Bennett, F. Nex, M. Gerke, and J. Zevenbergen, "Review of the current state of UAV regulations," *Remote Sensing*, vol. 9, no. 5, p. 459, May 2017.
- [42] T. Jones, *Int. Commercial Drone Regulation and Drone Delivery Services*. Santa Monica, CA, USA: RAND, 2017.
- [43] A. Fotouhi, H. Qiang, M. Ding, et al., "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, Fourth Quarter 2019.
- [44] (2020) UAV coach. [Online]. Available: <https://uavcoach.com/drone-laws/>
- [45] G. C. Birch and B. L. Woo, "Counter unmanned aerial systems testing: Evaluation of VIS SWIR MWIR and LWIR passive imagers," SNL-NM, Tech. Rep. SAND2017-0921 650791, 2017.
- [46] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "SoK-security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps," *arXiv preprint arXiv:1903.05155*, 2019.
- [47] S. Samaras, E. Diamantidou, D. Ataloglou, et al., "Deep learning on multi sensor data for counter UAV Applications—A systematic review," *Sensors*, vol. 19, no. 22, pp. 4837–4872, Nov. 2019.
- [48] 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 Commun. Mag.*, vol. 56, no. 4, pp. 68–74, Apr. 2018.
- [49] I. Guvenc, F. Koohifar, S. Singh, et al., "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

- [50] G. Ding, Q. Wu, L. Zhang, Y. Lin, et al., "An amateur drone surveillance system based on the cognitive internet of things," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 29–35, Jan. 2018.
- [51] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Nov. 2016.
- [52] R. L. Sturdivant and E. K. Chong, "Systems engineering baseline concept of a multispectral drone detection solution for airports," *IEEE Access*, vol. 5, pp. 7123–7138, Apr. 2017.
- [53] C. Kennedy and J. I. Rogers, "The emergence of mini UAVs for military applications," *Taylor & Francis, The Int. J. of Human Rights*, no. 19, pp. 212–227, Feb. 2015.
- [54] D. Orfanus, E. P. de Freitas, and F. Eliassen, "Self-Organization as a supporting paradigm for military UAV relay networks," *IEEE Commun. Letts.*, vol. 20, no. 4, pp. 804–807, Feb. 2016.
- [55] G. S. L. K. Chand, M. Lee, and S. Y. Shin, "Drone based wireless mesh network for disaster/military environment," *J. of Computer and Commun.*, vol. 6, no. 04, p. 44, Apr. 2018.
- [56] F. Xiong, A. Li, H. Wang, and L. Tang, "An SDN-MQTT based communication system for battlefield UAV swarms," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 41–47, Aug. 2019.
- [57] K. Daniel and C. Wietfeld, "Using public network infrastructures for UAV remote sensing in civilian security operations," *DTIC Document, Tech. Rep.*, Mar. 2011.
- [58] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 22–28, Mar. 2017.
- [59] W. DeBusk, "Unmanned aerial vehicle systems for disaster relief: Tornado alley," in *AIAA Infotech@ Aerospace 2010*, 2010, p. 3506.
- [60] A. Kim. (2020, Feb.) The Korea Herald. [Online]. Available: <http://www.koreaherald.com/view.php?ud=20200227000901>
- [61] F. G. Costa, J. Ueyama, T. Braun, et al., "The use of unmanned aerial vehicles and wireless sensor network in agricultural applications," in *2012 IEEE Int. Geoscience and Remote Sensing Symp.*, Jul. 2012, pp. 5045–5048.
- [62] J. Chanyoung and S. Hyoung, "Multiple UAV systems for agricultural applications: Control, Implementation, and Evaluation," *Electronics*, vol. 162, no. 9, Aug. 2018.
- [63] J. W. Rosenarchive. (2017, Jun.) Zipline's ambitious medical drone delivery in Africa. MIT Technol. Review. [Online]. Available: <https://www.technologyreview.com/2017/06/08/151339/blood-from-the-sky-ziplines-ambitious-medical-drone-delivery-in-africa/>
- [64] R. L. Hotz, "In Rwanda, drones deliver medical supplies to remote areas," *Tech. Rep.*, Dec. 2017, the Wall Street J. [Online]. Available: <https://www.wsj.com/articles/in-rwanda-drones-deliver-medical-supplies-to-remote-areas-1512124200>
- [65] Ric, "Drones going postal—A summary of postal service delivery drone trials," *Tech. Rep.*, Jun. 2016. [Online]. Available: <http://unmannedcargo.org/drones-going-postal-summary-postal-service-delivery-drone-trials>
- [66] MultiGP. [Online]. Available: <https://www.multigp.com>
- [67] S. Karapantazis and F. Pavlidou, "Broadband communications via high-altitude platforms: A survey," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 1, pp. 2–31, First Quarter 2005.
- [68] Y. Chen, H. Zhang, and M. Xu, "The coverage problem in UAV network: A survey," in *Fifth Int. Conf. on Computing, Commun. and Netw. Technologies (ICCCNT)*. IEEE, 2014, pp. 1–5.
- [69] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, Second Quarter 2016.
- [70] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet of Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.
- [71] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, Fourth Quarter 2016.
- [72] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.
- [73] O. S. Oubbati, A. Lakas, F. Zhou, M. Güneş, and M. B. Yagoubi, "A survey on position-based routing protocols for flying ad hoc networks (FANETs)," *Elsevier, Veh. Commun.*, vol. 10, pp. 29–56, Oct. 2017.
- [74] X. Cao, P. Yang, M. Alzenad, X. Xi, et al., "Airborne communication networks: A survey," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1907–1926, Sep. 2018.
- [75] A. A. Khuwaja, Y. Chen, N. Zhao, et al., "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, Fourth Quarter 2018.
- [76] W. Khawaja, I. Guvenc, D. W. Matolak, et al., "A survey of air-to-ground propagation channel modeling for unmanned aerial vehicles," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2361–2391, Third Quarter 2019.
- [77] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond," *Proceedings of the IEEE*, vol. 107, no. 12, pp. 2327–2375, Dec. 2019.
- [78] H. Kang, J. Joung, J. Ahn, and J. Kang, "Secrecy-aware altitude optimization for quasi-static UAV base station without eavesdropper location information," *IEEE Commun. Lett.*, vol. 23, no. 5, pp. 851–854, May 2019.
- [79] J. Seo, S. Pack, and H. Jin, "Uplink NOMA random access for UAV-assisted communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8289–8293, Aug. 2019.
- [80] M. Zolanvari, R. Jain, and T. Salman, "Potential data link candidates for civilian unmanned aircraft systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 292–319, First Quarter 2020.
- [81] O. S. Oubbati, A. Lakas, P. Lorenz, et al., "Leveraging communicating UAVs for emergency vehicle guidance in urban areas," *IEEE Trans. Emerg. Topics Comput.*, pp. 1–12, Jul. 2019 (early access articles).
- [82] H. Shakhtrah, A. H. Sawalmeh, A. Al-Fuqaha, et al., "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634, Apr. 2019.
- [83] B. Alzahrani, O. S. Oubbati, A. Barnawi, et al., "UAV assistance paradigm: State-of-the-art in applications and challenges," *J. of Network and Computer Applications*, vol. 166, p. 102706, Sep. 2020.
- [84] "5G Enhancement for UAVs," 3GPP, Tech. Rep. TS 22.125, Nov. 2019.
- [85] Amazon. (2020, Aug.) First prime air delivery. [Online]. Available: <https://www.amazon.com/b?node=8037720011>
- [86] J. Joung, "Random space-time line code with proportional fairness scheduling," *IEEE Access*, vol. 8, pp. 35 253–35 262, Feb. 2020.
- [87] H.-T. Ye, X. Kang, J. Joung, and Y.-C. Liang, "Joint uplink and downlink 3D optimization of UAV swarm for wireless-powered NB-IoT," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Hawaii, USA, Dec. 2019, pp. 1–6.
- [88] H.-T. Ye, X. Kang, Y.-C. Liang, and J. Joung, "Optimal time allocation for full-duplex wireless-powered IoT networks with unmanned aerial vehicle," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6.
- [89] H.-T. Ye, X. Kang, J. Joung, and Y.-C. Liang, "Optimization for full-duplex rotary-wing UAV-enabled wireless-powered IoT networks," *IEEE Trans. Wireless Commun.*, Apr. 2020.
- [90] C. Secchi, A. Franchi, H. H. Büthoff, and P. R. Giordano, "Bilateral teleoperation of a group of UAVs with communication delays and switching topology," in *IEEE Int. Conf. Robotics and Automation*, Saint Paul, USA, May 2012, pp. 4307–4314.
- [91] D. Ho, E. I. Grøtli, P. B. Sujit, T. A. Johansen, and J. B. Sousa, "Cluster-based communication topology selection and UAV path planning in wireless sensor networks," in *2013 Int. Conf. on Unmanned Aircraft Systems (ICUAS)*, Atlanta, USA, May 2013, pp. 59–68.
- [92] M. Mozaffari, W. Saad, M. Bennis, et al., "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, Third Quarter 2019.
- [93] A. Sanjab, W. Saad, and T. Başar, "A game of drones: Cyber-physical security of time-critical UAV applications with cumulative prospect theory perceptions and valuations," *arXiv preprint arXiv:1902.03506*, 2019.
- [94] (2020) Blighter Surveillance Systems/Chess Dynamics/Enterprise Control Systems: Anti-UAV Defence System (AUDS). [Online]. Available: <https://www.homelandsecurity-technology.com/projects/anti-uav-defence-system-auds/>
- [95] (2020) Commun. & Systemes/HGH/Spectracom: Boreades. [Online]. Available: <https://c-s-inc.us/products/boreades/>
- [96] (2020) MyDefence Communication: KNOX. [Online]. Available: <https://mydefence.dk/anti-drone-solutions/knox-anti-drone-solution/>

- [97] (2015) Airbus Defence and Space: Counter UAV System. [Online]. Available: <https://www.airbus.com/newsroom/press-releases/en/2015/09/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion.html>
- [98] (2019) Raytheon: Windshear. [Online]. Available: <https://www.raytheon.com/news/feature/bad-drone>
- [99] (2020) Prime Consulting & Technologies: Mini/Small-range counter-UAV system. [Online]. Available: <https://dronemajor.net/brands/prime-consulting-technologies/products/counter-uav-system>
- [100] (2020) Aselsan: IHTAR. [Online]. Available: <https://www.aselsan.com.tr/en/capabilities/air-and-missile-defense-systems/air-and-missile-defense-systems/ihtar-antidrone-system>
- [101] M. Laurenzis, S. Hengy, M. Hammer, et al., "An adaptive sensing approach for the detection of small UAV: First investigation of static sensor network and moving sensor platform," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII*, I. Kadar, Ed., vol. 10646, Int. Society for Optics and Photonics. Orlando, FL, USA: SPIE, Apr. 2018, pp. 197–205.
- [102] (2020) Applied Technology Associates: Low-Cost Counter-Unmanned Aerial System for Targeting (LOCUST). [Online]. Available: <http://www.atocorp.com/locust.html>
- [103] (2020) Boeing:GBAD DE OTM Ground-Based Air Defense Directed Energy On-the-Move. [Online]. Available: <https://www.globalsecurity.org/military/systems/ground/gbad-de-otm.htm>
- [104] (2020) Rohde & Schwarz/ESG/Diehl: Guardian. [Online]. Available: <https://guardion.eu/>
- [105] (2020) Thales: Gecko-M. [Online]. Available: <https://www.thalesgroup.com/en/gecko-m>
- [106] (2020) Aselsan: GERGEDAN. [Online]. Available: <https://www.aselsan.com.tr/en/capabilities/electronic-warfare-systems/electronik-support-and-electronic-attack-systems/gergedan-portable-rcied-jammer-system-vehicle-type>
- [107] (2020) Orion anti-drone system. [Online]. Available: <http://www.trd.sg/product.php>
- [108] (2020) INT-AU002 Anti UAV System. [Online]. Available: <https://4intelligence.com/product/int-au002-anti-uav-system/>
- [109] (2020) Take down your threats tactical and automatic disruptors. [Online]. Available: <https://www.blacksagetech.com/disruptors>
- [110] (2020) Wingman 100 personal drone alarm for police and security officers. [Online]. Available: <https://mydefence.dk/civil-customers/mobile-stationary-installations/wingman-100/>
- [111] (2020) Drone detection & defense systems dronewatcherrf. [Online]. Available: <https://detect-inc.com/drone-detection-defense-systems/>
- [112] K. Osborn. (2017, Oct.) Army fast-tracks new man-packable counter-drone EW weapons. [Online]. Available: <https://defensesystems.com/articles/2017/10/cw/caci-ew-army-beam.aspx>
- [113] (2020) Scorpion 2 handheld counter-drone technology. [Online]. Available: <https://www.whitefoxdefense.com/scorpion>
- [114] (2020) Telescope portable drone detection device. [Online]. Available: <https://dronetrackingtechnologies.com/products.html>
- [115] R. Isaacs, *Differential Games*. Newyork: Wiley, 1965.
- [116] Y. Ho, A. Bryson, and S. Baron, "Differential games and optimal pursuit-evasion strategies," *IEEE Trans. Autom. Control*, vol. 10, no. 4, pp. 385–389, Oct. 1965.
- [117] J. Z. Ben-Asher, S. Levinson, J. Shinar, and H. Weiss, "Trajectory shaping in linear-quadratic pursuit-evasion games," *Jour. Guid., Cont., & Dyna.*, vol. 27, no. 6, pp. 1102–1105, Nov. 2004.
- [118] S. Liu, Z. Zhou, C. Tomlin, and K. Hedrick, "Evasion as a team against a faster pursuer," in *2013 American Control Conf.*, Washington, DC, USA, Jun. 2013, pp. 5368–5373.
- [119] K. Margellos and J. Lygeros, "Hamilton-Jacobi formulation for reach-avoid differential games," *IEEE Trans. Autom. Control*, vol. 56, no. 8, pp. 1849–1861, Aug. 2011.
- [120] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, "Reach-avoid problems with time-varying dynamics, targets and constraints," in *Proc. 18th Inter. Conf. Hybrid Sys.: Comput. Cont.*, Seattle, Washington, USA, Apr. 2015, pp. 11–20.
- [121] J. Lorenzetti, M. Chen, B. Landry, and M. Pavone, "Reach-avoid games via mixed-integer second-order cone programming," in *Proc. IEEE Conf. on Decision and Control (CDC)*, Miami Beach, FL, USA, Dec. 2018, pp. 4409–4416.
- [122] D. W. Oyler, P. T. Kabamba, and A. R. Girard, "Pursuit-evasion games in the presence of obstacles," *Automatica*, vol. 65, pp. 1–11, Mar. 2016.
- [123] X. Fang, C. Wang, L. Xie, and J. Chen, "Cooperative pursuit with multi-pursuer and one faster free-moving evader," Jan. 2020, arXiv:2001.04731.
- [124] Z. E. Fuchs, P. P. Khargonekar, and J. Evers, "Cooperative defense within a single-pursuer, two-evader pursuit evasion differential game," in *49th IEEE Conf. on Decision and Control (CDC)*, Atlanta, GA, USA, Dec. 2010, pp. 3091–3097.
- [125] W. Scott and N. E. Leonard, "Pursuit, herding and evasion: A three-agent model of caribou predation," in *2013 American Control Conf.*, Washington, DC, USA, Jun. 2013, pp. 2978–2983.
- [126] E. Garcia, D. W. Casbeer, and M. Pachter, "Design and analysis of state-feedback optimal strategies for the differential game of active defense," *IEEE Trans. Autom. Control*, vol. 64, no. 2, pp. 553–568, Feb. 2019.
- [127] L. Liang, F. Deng, Z. Peng, X. Li, and W. Zha, "A differential game for cooperative target defense," *Automatica*, vol. 102, pp. 58–71, Apr. 2019.
- [128] A. Pierson, Z. Wang, and M. Schwager, "Intercepting rogue robots: An algorithm for capturing multiple evaders with multiple pursuers," *IEEE Robot. Autom. Lett.*, vol. 2, no. 2, pp. 530–537, Apr. 2017.
- [129] D. Li and J. B. Cruz, "Defending an asset: A linear quadratic game approach," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 2, pp. 1026–1044, Apr. 2011.
- [130] R. Opromolla, G. Fasano, and D. Accardo, "A vision-based approach to UAV detection and tracking in cooperative applications," *Sensors*, vol. 18, no. 10, p. 3391, Oct. 2018.
- [131] M. Hua, Y. Wang, Q. Wu, et al., "Energy-efficient cooperative secure transmission in multi-UAV-enabled wireless networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7761–7775, Aug. 2019.
- [132] Y. Roh, S. Jung, and J. Kang, "Cooperative UAV jammer for enhancing physical layer security: Robust design for jamming power and trajectory," in *Proc. IEEE Military Commun. Conf. (MILCOM)*. Norfolk, VA, USA: IEEE, Nov. 2019, pp. 464–469.
- [133] K. Li, R. C. Voicu, S. S. Kanhere, et al., "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2283–2293, Mar. 2019.
- [134] S. Jeong, O. Simeone, and J. Kang, "Mobile edge computing via a UAV-mounted cloudlet: Optimization of bit allocation and path planning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2049–2063, Mar. 2018.
- [135] H. Ahmadi, K. Katzis, and M. Z. Shakir, "A novel airborne self-organising architecture for 5G+ networks," in *Proc. IEEE Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, Sep. 2017, pp. 1–5.
- [136] Y. Zeng, J. Xu, and R. Zhang, "Energy minimization for wireless communication with rotary-wing UAV," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2329–2345, Apr. 2019.
- [137] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.
- [138] B. Galkin, J. Kibilda, and L. A. DaSilva, "UAVs as mobile infrastructure: Addressing battery lifetime," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 132–137, Jun. 2019.
- [139] O. M. Bushnaq, M. A. Kishk, A. Çelik, et al., "Cellular traffic offloading through tethered-UAV deployment and user association," *arXiv preprint arXiv:2003.00713*, 2020.
- [140] (2019) Kratos Defense & Rocket Support Services: Aethon. [Online]. Available: <https://www.kratosdefense.com/systems-and-platforms/unmanned-systems/aerial/aethon>
- [141] AerialX. (2020, Apr.) Dronebullet. [Online]. Available: <https://www.aerialx.com/>
- [142] J. Mannes. (2016, Nov.) Airspace Systems: Interceptor can catch high-speed drones all by itself. [Online]. Available: <https://techcrunch.com/2016/11/18/airspace-systems-interceptor-can-catch-high-speed-drones-all-by-itself/>
- [143] Z. Alkhalisi. (2016, Nov.) Exponent: Drone Hunter. [Online]. Available: <https://money.cnn.com/2016/11/04/technology/dubai-airport-drone-hunter/>
- [144] J. Plaza. (2017, Jun.) ALX systems announces new operating system at commercial UAV expo europe. [Online]. Available: <https://www.commercialuavnews.com/infrastructure/alx-systems-new-operating-system-uav-europe>
- [145] K. D. Atherton. (2018, Dec.) Russia's carnivora is designed for a drone-eat-drone world. [Online]. Available: <https://www.c4isrnet.com/unmanned/2018/12/14/russias-carnivora-is-designed-for-a-drone-eat-drone-world/>

- [146] (1990) Lockheed Martin: Blackbird. [Online]. Available: <https://www.lockheedmartin.com/en-us/news/features/history/blackbird.html>
- [147] (2015) General Atomics: MQ-9 Reaper. [Online]. Available: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/>
- [148] (2015) General Atomics: MQ-1B Predator. [Online]. Available: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/>
- [149] (2014) Northrop Grumman: RQ-4 Global Hawk. [Online]. Available: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/>
- [150] (2020) General Atomics: Gray Eagle UAS. [Online]. Available: <http://www.ga-asi.com/gray-eagle>
- [151] Google X: Project Loon. [Online]. Available: <https://x.company/projects/loon/>
- [152] (2015) ECA Group/Group Gorge: IT180 drone. [Online]. Available: <https://www.ecagroup.com/en/event/neutralization-malicious-drones-eca-group-innovating-and-validates-unique-technology-locate>
- [153] M. Tewksbury. (2019, Jun.) Raytheon: Howler. [Online]. Available: <http://raytheon.mediaroom.com/2019-06-18-US-Army-deploys-Howler-counter-UAS-capability-into-the-battlefield>
- [154] (2018) Sierra Nevada Corporation: Advanced Electronic Warfare System – Modular (AEWS-M). [Online]. Available: [https://www.sncorp.com/media/2403/snc\\_aews-m-product-sheet\\_2018.pdf](https://www.sncorp.com/media/2403/snc_aews-m-product-sheet_2018.pdf)
- [155] (2020) TRD Consultancy: Fixed Site Area Protection. [Online]. Available: [http://www.trd.sg/images/fixd\\_site\\_solution\\_brochure.pdf](http://www.trd.sg/images/fixd_site_solution_brochure.pdf)
- [156] A. Dekker, "A taxonomy of network centric warfare architectures," in *Systems Engineering/Test and Evaluation (SETE) 2005*, Brisbane, Australia, 2008.
- [157] N. Gageik, P. Benz, and S. Montenegro, "Obstacle detection and collision avoidance for a UAV with complementary low-cost sensors," *IEEE Access*, vol. 3, pp. 599–609, May 2015.
- [158] J. S. G. Guerrero, A. F. C. González, J. I. H. Vega, and L. A. N. Tovar, "Instrumentation of an array of ultrasonic sensors and data processing for unmanned aerial vehicle (UAV) for teaching the application of the Kalman filter," *Procedia Computer Science*, vol. 75, pp. 375–380, 2015.
- [159] D. G. Davies, R. C. Bolam, Y. Vagapov, and P. Excell, "Ultrasonic sensor for UAV flight navigation," in *Proc. Int. Workshop on Electric Drives: Optimization in Control of Electric Drives (IWED)*. Moscow, Russia: IEEE, Jan. 2018, pp. 1–7.
- [160] M. F. bin Misnan, N. M. Arshad, and N. A. Razak, "Construction sonar sensor model of low altitude field mapping sensors for application on a UAV," in *2012 IEEE 8th Int. Colloquium on Signal Processing and its Applications*, Melaka, Malaysia, Mar. 2012, pp. 446–450.
- [161] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Modeling air-troground path loss for low altitude platforms in urban environments," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec., pp. 2898–2904.
- [162] H. F. Durrant-Whyte, "Sensor models and multisensor integration," in *Autonomous robot vehicles*. Springer, 1990, pp. 73–89.
- [163] B. V. Dasarathy, "Sensor fusion potential exploitation-innovative architectures and illustrative applications," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 24–38, Jan. 1997.
- [164] E. Blasch and D. A. Lambert, *High-Level Information Fusion Management and Systems Design*, 1st ed. Norwood, MA, USA: Artech House, 2012.
- [165] M. Liggins II, D. Hall, and J. Llinas, *Handbook of Multisensor Data Fusion: Theory and Practice*, 2nd ed. Boca Raton, FL: CRC press, 2008.
- [166] F. Castanedo, "A review of data fusion techniques," *The Scientific World J.*, vol. 2013, Oct. 2013.
- [167] 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 Commun. Mag.*, vol. 56, no. 4, pp. 68–74, Apr. 2018.
- [168] S. Park, S. Shin, Y. Kim, et al., "Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles (UAVs)," in *2015 IEEE SENSORS*. Busan, South Korea: IEEE, Nov. 2015, pp. 1–4.
- [169] G. L. Charvat, A. J. Fenn, and B. T. Perry, "The MIT IAP radar course: Build a small radar system capable of sensing range, Doppler, and synthetic aperture (SAR) imaging," in *Proc. IEEE Radar Conference*, Atlanta, GA, USA, May 2012, pp. 138–144.
- [170] E. Diamantidou, A. Lalas, K. Votis, and D. Tzovaras, "Multimodal deep learning framework for enhanced accuracy of UAV detection," in *Int. Conf. on Computer Vision Systems*. Thessaloniki, Greece: Springer, Sep. 2019, pp. 768–777.
- [171] F. Fioranelli, M. Ritchie, H. Griffiths, and H. Borrión, "Classification of loaded/unloaded micro-drones using multistatic radar," *Electron. Lett.*, vol. 51, no. 22, pp. 1813–1815, Oct. 2015.
- [172] M. Ritchie, F. Fioranelli, H. Borrión, and H. Griffiths, "Multistatic micro-Doppler radar feature extraction for classification of unloaded/loaded micro-drones," *IET Radar, Sonar & Navigation*, vol. 11, no. 1, pp. 116–124, 2016.
- [173] Y. Gu, A. Lo, and I. Niemegeers, "A survey of indoor positioning systems for wireless personal networks," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 13–32, First Quarter 2009.
- [174] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2568–2599, Third Quarter 2019.
- [175] J. Joung, S. Jung, S. Chung, and E.-R. Jeong, "CNN-based Tx-Rx distance estimation for UWB system localisation," *IET Electron. Lett.*, vol. 55, no. 17, pp. 938–940, Aug. 2019.
- [176] E. Mazidi, "Introducing new localization and positioning system for aerial vehicles," *IEEE Embedded Systems Letters*, vol. 5, no. 4, pp. 57–60, Dec. 2013.
- [177] I. A. Mantilla-Gaviria, M. Leonardi, G. Galati, and J. V. Balbastre-Tejedor, "Time-difference-of-arrival regularised location estimator for multilateration systems," *IET Radar, Sonar Navigation*, vol. 8, no. 5, pp. 479–489, Jun. 2014.
- [178] Y. Wang and K. C. Ho, "TDOA positioning irrespective of source range," *IEEE Trans. Signal Process.*, vol. 65, no. 6, pp. 1447–1460, Mar. 2017.
- [179] W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*. John Wiley & Sons, 2010.
- [180] S. Basak and B. Scheers, "Passive radio system for real-time drone detection and doa estimation," in *Proc. Int. Conf. on Military Commun. and Information Systems (ICMCIS)*, Warsaw, Poland, May 2018, pp. 1–6.
- [181] R. K. Miranda, D. A. Ando, J. P. C. L. da Costa, and M. T. de Oliveira, "Enhanced direction of arrival estimation via received signal strength of directional antennas," in *Proc. IEEE Int. Symp. on Signal Processing and Inf. Technol. (ISSPIT)*, Louisville, KY, USA, Dec. 2018, pp. 162–167.
- [182] I.-F. Kenmogne, V. Drevelle, and E. Marchand, "Image-based UAV localization using interval methods," in *Proc. IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*. Vancouver, BC, Canada: IEEE, Sep. 2017, pp. 5285–5291.
- [183] M. Vrba, D. Heřt, and M. Saska, "Onboard marker-less detection and localization of non-cooperating drones for their safe interception by an autonomous aerial system," *IEEE Robot. Autom. Lett.*, vol. 4, no. 4, pp. 3402–3409, Oct. 2019.
- [184] M. Vrba and M. Saska, "Marker-less micro aerial vehicle detection and localization using convolutional neural networks," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 2459–2466, Apr. 2020.
- [185] F. Gökçe, G. Üçoluk, and E. Kalkan, "Vision-based detection and distance estimation of micro unmanned aerial vehicles," *Sensors*, vol. 14, pp. 23 805–23 846, 2015.
- [186] F. Hoffmann, M. Ritchie, F. Fioranelli, et al., "Micro-Doppler based detection and tracking of UAVs with multistatic radar," in *Proc. IEEE Radar Conf. (RadarConf)*. Philadelphia, PA, USA: IEEE, May 2016, pp. 1–6.
- [187] U.S. Federal Aviation Administration. (2019) Unmanned aircraft system detection - technical considerations. [Online]. Available: [https://www.faa.gov/airports/airport\\_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf](https://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf)
- [188] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, May 2018.
- [189] Y. Mao, C. You, J. Zhang, et al., "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, Fourth Quarter 2017.
- [190] DJI Support. (2017, Aug.) How to use DJI's return to home (RTH) safely. [Online]. Available: <https://store.dji.com/guides/how-to-use-the-djis-return-to-home/>
- [191] RoboTiCan. (2020, Apr.) Goshawk. [Online]. Available: <https://robotican.net/goshawk/>
- [192] L. Hauzenberger and E. Holmberg Ohlsson, "Drone detection using audio analysis," Master's thesis, Lund University, Sweden, Jun. 2015.

- [193] DronesShield. (2020, Apr.) Dronesentry. [Online]. Available: <https://www.dronesshield.com/sentry>
- [194] Alsok. (2020, Apr.). [Online]. Available: <https://www.alsok.co.jp/en/>
- [195] B. Harvey and S. O'Young, "Acoustic detection of a fixed-wing UAV," *Drones*, vol. 2, no. 1, pp. 4–22, Jan. 2018.
- [196] G. Ottoy and L. De Strycker, "An improved 2D triangulation algorithm for use with linear arrays," *IEEE Sensors J.*, vol. 16, no. 23, pp. 8238–8243, Dec. 2016.
- [197] E. E. Case, A. M. Zelnio, and B. D. Rigling, "Low-cost acoustic array for small UAV detection and tracking," in *2008 IEEE National Aerospace and Electronics Conf.*, Dayton, OH, USA, Jul. 2008, pp. 110–113.
- [198] A. Yakubovskiy, H. Sallou, A. Sutin, et al., "Feature extraction for acoustic classification of small aircraft," in *2015 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics (WASPAA)*, New Paltz, NY, USA, Oct. 2015, pp. 1–5.
- [199] A. Bernardini, F. Mangiardi, E. Pallotti, and L. Capodiferro, "Drone detection by acoustic signature identification," *Electron. Imag.*, vol. 2017, pp. 60–64, Jan. 2017.
- [200] J. Kim and D. Kim, "Neural network based real-time UAV detection and analysis by sound," *Jour. Adv. Inf. Technol. Converg.*, vol. 8, no. 1, pp. 43–52, Jul. 2018.
- [201] V. Phipatanasuphorn and P. Ramanathan, "Vulnerability of sensor networks to unauthorized traversal and monitoring," *IEEE Trans. Commun.*, vol. 53, no. 3, pp. 364–369, Mar. 2004.
- [202] P. Nguyen, M. Ravindranathan, A. Nguyen, et al., "Investigating cost-effective RF-based detection of drones," in *Workshop on Micro Aerial Vehicle Netw., Systems, and Applications for Civilian Use*, Singapore, Jun. 2016, pp. 17–22.
- [203] P. Nguyen, H. Truong, M. Ravindranathan, et al., "Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication," in *Proc. Int. Conf. on Mobile Systems, Applications, and Services*, Niagara Falls, New York, USA, Jun. 2017, pp. 211–224.
- [204] M. Ezuma, F. Erden, C. K. Anjinappa, et al., "Micro-UAV detection and classification from RF fingerprints using machine learning techniques," in *Proc. IEEE Aerospace Conf.*, Big Sky, MT, USA, Mar. 2019, pp. 1–13.
- [205] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, First Quarter 2009.
- [206] P. Molchanov, K. Egiazarian, J. Astola, et al., "Classification of small uavs and birds by micro-Doppler signatures," in *Proc. European Radar Conf.*, Nuremberg, Germany, Dec. 2013, pp. 172–175.
- [207] P. Molchanov, K. Egiazarian, J. Astola, et al., "Classification of aircraft using micro-Doppler bicoherence-based features," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 2, pp. 1455–1467, Apr. 2014.
- [208] B. Torvik, K. E. Olsen, and H. Griffiths, "Classification of birds and uavs based on radar polarimetry," *IEEE Geosci. Remote Sens. Lett.*, vol. 13, no. 9, pp. 1305–1309, Sep. 2016.
- [209] J. Ren and X. Jiang, "Regularized 2-d complex-log spectral analysis and subspace reliability analysis of micro-Doppler signature for UAV detection," *Pattern Recog.*, vol. 69, pp. 225–237, Sep. 2017.
- [210] B. K. Kim, H. Kang, and S. Park, "Drone classification using convolutional neural networks with merged Doppler images," *IEEE Geosci. Remote Sens. Lett.*, vol. 14, no. 1, pp. 38–42, Jan. 2017.
- [211] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*. FL, USA: CRC Press, 2013.
- [212] A. Stateczny and J. Lubczonek, "FMCW radar implementation in river information services in Poland," in *2015 16th Int. Radar Symp. (IRS)*, Dresden, Germany, Aug. 2015, pp. 852–857.
- [213] J. Farlik, M. Kratky, J. Casar, and V. Stary, "Multispectral detection of commercial unmanned aerial vehicles," *Sensors*, vol. 19, no. 7, p. 1517, Apr. 2019.
- [214] N. Eriksson, "Conceptual study of a future drone detection system - countering a threat posed by a disruptive technology," Master's thesis, Chalmers Univ. Tech., Gothenburg, Sweden, 2018.
- [215] V. C. Chen, *The Micro-Doppler Effect in Radar*. Boston: Artech House, 2019.
- [216] B. K. Kim, H. Kang, and S. Park, "Experimental analysis of small drone polarimetry based on micro-Doppler signature," *IEEE Geosci. Remote Sens. Lett.*, vol. 14, no. 10, pp. 1670–1674, Aug. 2017.
- [217] R. Guay, G. Drolet, and J. R. Bray, "Measurement and modelling of the dynamic radar cross-section of an unmanned aerial vehicle," *IET Radar, Sonar Navigation*, vol. 11, no. 7, pp. 1155–1160, Jul. 2017.
- [218] V. C. Chen, F. Li, S. S. Ho, and H. Wechsler, "Analysis of micro-Doppler signatures," *IEE Proceedings - Radar, Sonar and Navigation*, vol. 150, no. 4, p. 271, Nov. 2003.
- [219] —, "Micro-Doppler effect in radar: Phenomenon, model, and simulation study," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 1, pp. 2–21, Jan. 2006.
- [220] V. C. Chen and S. Qian, "Joint time-frequency transform for radar range-Doppler imaging," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 34, no. 2, pp. 486–499, Apr. 1998.
- [221] V. C. Chen, D. Tahmouh, and W. J. Miceli, *Radar Micro-Doppler Signature: Processing and Applications*. London, UK: The Institution of Engineering and Technol., 2014.
- [222] J. J. M. de Wit, R. I. A. Harmanny, and G. Prémel-Cabic, "Micro-Doppler analysis of small uavs," in *Proc. Int. European Radar Conf.*, Amsterdam, Netherlands, Feb. 2012, pp. 210–213.
- [223] J. J. M. de Wit, R. I. A. Harmanny, and P. Molchanov, "Radar micro-Doppler feature extraction using the singular value decomposition," in *2014 Int. Radar Conf.*, Lille, France, Mar. 2014.
- [224] S. Rahman and D. A. Robertson, "Millimeter-wave micro-Doppler measurements of small uavs," in *Proc. SPIE 10188, Radar Sensor Technol. XXI, 101880T*, Anaheim, California, USA, May 2017, pp. 30–33.
- [225] R. J. Fontana, E. A. Richley, A. J. Marzullo, et al., "An ultra wideband radar for micro air vehicle applications," in *2002 IEEE Conf. on Ultra Wideband Systems and Technologies (IEEE Cat. No.02EX580)*, Baltimore, MD, USA, May 2002, pp. 187–191.
- [226] T. Mizushima, R. Nakamura, and H. Hadama, "Reflection characteristics of ultra-wideband radar echoes from various drones in flight," in *Proc. IEEE Topical Conf. on Wireless Sensors and Sensor Netw. (WiS-NeT)*, San Antonio, TX, USA, Jan. 2020.
- [227] C. J. Li and H. Ling, "An investigation on the radar signatures of small consumer drones," *IEEE Antennas Wireless Propag. Lett.*, vol. 16, pp. 649–652, Jul. 2017.
- [228] B. Torvik, A. Knapskog, . Lie-Svendsen, et al., "Amplitude modulation on echoes from large birds," in *Proc. European Radar Conf.*, Rome, Italy, Oct. 2014, pp. 177–180.
- [229] I. Güvenç, O. Ozdemir, Y. Yapici, et al., "Detection, localization, and tracking of unauthorized UAS and jammers," in *Proc. IEEE/AIAA 36th Digital Avionics Systems Conf. (DASC)*, St. Petersburg, FL, USA, Sep. 2017, pp. 1–10.
- [230] M. Ritchie, F. Fioranelli, H. Griffiths, and B. Torvik, "Monostatic and bistatic radar measurements of birds and micro-drone," in *Proc. IEEE Radar Conf. (RadarConf)*, Philadelphia, PA, USA, May 2016, pp. 1–5.
- [231] T. Müller, "Robust drone detection for day/night counter-UAV with static VIS and SWIR cameras," in *Ground/Air Multisensor Interoperability, Integration, and Netw. for Persistent ISR VIII*, vol. 10190, May 2017, pp. 302–313.
- [232] P. Andrašić, T. Radišić, M. Muštra, and J. Ivošević, "Night-time detection of UAVs using thermal infrared camera," *Transportation Research Procedia*, vol. 28, pp. 183–190, 2017.
- [233] A. Rozantsev, V. Lepetit, and P. Fua, "Detecting flying objects using a single moving camera," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 5, pp. 879–892, May 2017.
- [234] M. Saqib, S. Daud Khan, N. Sharma, and M. Blumenstein, "A study on detecting drones using deep convolutional neural networks," in *Proc. IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS)*, Lecce, Italy, Aug. 2017, pp. 1–5.
- [235] C. Craye and S. Ardjoune, "Spatio-temporal semantic segmentation for drone detection," in *Proc. IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS)*, Taipei, Taiwan, Sep. 2019.
- [236] V. Magoulaniotis, D. Ataloglou, A. Dimou, D. Zarpalas, and P. Daras, "Does deep super-resolution enhance UAV detection?" in *Proc. IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS)*, Taipei, Taiwan, Sep. 2019, pp. 1–6.
- [237] C. Cigla, R. Thakker, and L. Matthies, "Onboard stereo vision for drone pursuit or sense and avoid," in *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR) Workshops*, Salt Lake City, UT, USA, Jun. 2018, pp. 738–746.
- [238] A. Schumann, L. Sommer, J. Klatte, et al., "Deep cross-domain flying object classification for robust UAV detection," in *Proc. IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS)*, Lecce, Italy, Aug. 2017, pp. 1–6.
- [239] T. Ringwald, L. Sommer, A. Schumann, et al., "UAV-Net: A fast aerial vehicle detector for mobile platforms," in *Proc. IEEE Conf. on Computer*

- Vision and Pattern Recognition (CVPR) Workshops*, Long Beach, CA, USA, Jun. 2019, pp. 1–9.
- [240] C. Aker and S. Kalkan. "Using deep networks for drone detection," in *Proc. IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS)*, Lecce, Italy, Aug. 2017, pp. 1–6.
- [241] M. Hammer, M. Hebel, B. Borgmann, et al., "Potential of lidar sensors for the detection of UAVs," in *Laser Radar Technol. and Applications XXIII*, M. D. Turner and G. W. Kamerman, Eds., vol. 10636, Int. Society for Optics and Photonics. Orlando, FL, USA: SPIE, May 2018, pp. 39–45.
- [242] B. H. Kim, D. Khan, C. Bohak, et al., "V-RBNN based small drone detection in augmented datasets for 3D LADAR system," *Sensors*, vol. 18, no. 11, p. 3825, Nov. 2018.
- [243] S. Rahman and D. A. Robertson, "Radar micro-Doppler signatures of drones and birds at K-band and W-band," *Sci. Rep.*, vol. 8, pp. 1–11, Nov. 2018.
- [244] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/June. 2006.
- [245] A. Mpitzopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, Fourth Quarter 2009.
- [246] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," vol. 8, no. 1, pp. 181–184, Feb. 2018.
- [247] J. Noh, Y. Kwon, Y. Son, et al., "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Trans. Privacy and Security (TOPS)*, vol. 22, no. 2, pp. 12:1–12, Apr. 2019.
- [248] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robotics*, vol. 31, no. 4, pp. 617–636, Apr. 2014.
- [249] M. Hooper, Y. Tian, R. Zhou, et al., "Securing commercial WiFi-based UAVs from common security attacks," in *Proc. IEEE Military Commun. Conf.*, Baltimore, MD, USA, Nov. 2016, pp. 1213–1218.
- [250] N. Summers. (2016, Oct.) 'Icarus' machine can commandeer a drone mid-flight. [Online]. Available: <https://www.engadget.com/2016-10-28-icarus-hijack-dmsx-drones.html>
- [251] K. Moskvitch. (2014, Feb.) Are drones the next target for hackers? [Online]. Available: <https://www.bbc.com/future/article/20140206-can-drones-be-hacked>
- [252] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected UAV: Potential, challenges, and promising technologies," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 120–127, Feb. 2019.
- [253] W. A. Radasky, C. E. Baum, and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HP EM) and intentional electromagnetic interference (IEMI)," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 314–321, Aug. 2004.
- [254] Raytheon. (2020, Apr.) Phaser high-power microwave system. [Online]. Available: <https://www.raytheon.com/capabilities/products/phaser-high-power-microwave-system>
- [255] B. Zohuri, *High-Power Microwave Energy as Weapon*. Cham: Springer Int. Publishing, 2019, pp. 269–308. [Online]. Available: [https://doi.org/10.1007/978-3-030-20794-6\\_4](https://doi.org/10.1007/978-3-030-20794-6_4)
- [256] J. Lin and P. Singer. (2017, Feb.) Drones, lasers, and tanks: China shows off its latest weapons. [Online]. Available: <https://www.popsci.com/china-new-weapons-lasers-drones-tanks/>
- [257] India Today. (2015, Sep.) KALI: India's weapon to destroy any uninvited missiles and aircrafts. [Online]. Available: <https://www.indiatoday.in/education-today/gk-current-affairs/story/indias-top-secret-weapon-264111-2015-09-21>
- [258] D. Sudakov. (2016, Aug.) Russia's combat laser weapons declassified. [Online]. Available: [https://www.pravdareport.com/russia/135198-russia\\_laser\\_weapons/](https://www.pravdareport.com/russia/135198-russia_laser_weapons/)
- [259] MBDA Missile Systems. (2017, Sep.) Dragonfire laser turret unveiled at dsei 2017. [Online]. Available: <https://www.mbd-systems.com/press-releases/dragonfire-laser-turret-unveiled-dsei-2017/>
- [260] Daily Sabah. (2019, Sep.) Turkey's laser weapon ARMOL passes acceptance tests. [Online]. Available: <https://www.dailysabah.com/defense/2019/09/30/turkeys-laser-weapon-arnol-passes-acceptance-tests>
- [261] K. D. Atherton. (2015, Aug.) Boeing unveils its anti-drone laser weapon. [Online]. Available: <https://www.popsci.com/boeing-unveils-compact-anti-drone-laser/>
- [262] Agence France-Presse in Beijing. (2014, Nov.) China unveils laser drone defence system. [Online]. Available: <https://www.theguardian.com/world/2014/nov/03/china-unveils-laser-drone-defence-system>
- [263] Raytheon. (2020, Apr.) Forty-five down. [Online]. Available: <https://www.raytheon.com/news/feature/forty-five-down>
- [264] D. Gettinger and A. H. Michel. (2014, Jul.) A brief history of hamas and hezbollah's drones. [Online]. Available: <https://dronecenter.bard.edu/hezbollah-hamas-drones/>
- [265] Smart Rounds, Inc. (2019, Oct.) SAVAGE - Smart anti-drone weapon. [Online]. Available: <https://www.prnewswire.com/news-releases/savage--smart-anti-drone-weapon-300941541.html>
- [266] (2020) AerialX: DroneBullet. [Online]. Available: <https://www.aerialx.com/defeat.shtml>
- [267] G. Olivares, L. Gomez, J. E. Monteros, et al., "Volume II – UAS airborne collision severity evaluation – Quadcopter," National Institute for Aviation Research, Tech. Rep., Jul. 2017.
- [268] Ban Lethal. (2020, Apr.) Slaughterbots. [Online]. Available: <https://autonomousweapons.org/>
- [269] Anduril Industries. (2020, Apr.) Anvil. [Online]. Available: <https://www.anduril.com/>
- [270] Raytheon. (2020, Apr.) Coyote. [Online]. Available: <https://www.raytheon.com/capabilities/products/coyote>
- [271] CDET. (2020, Apr.) RAM UAV. [Online]. Available: <https://ramuav.com/>
- [272] Chenega. (2020, Apr.) Counter-UAV solutions. [Online]. Available: <https://www.chenegaeurope.com/media/1221/counteruav.pdf>
- [273] Dronedefence. (2020, Apr.) NetGun X1. [Online]. Available: <https://www.dronedefence.co.uk/products/netgun-x1/>
- [274] Droptec. (2020, Apr.) Dropster Net gun. [Online]. Available: <https://www.droptec.ch/product>
- [275] UAVOS. (2020, Apr.) Interception system for small sized unmanned vehicles. [Online]. Available: <https://www.uavos.com/products/uas-payloads/interception-system-for-uav>
- [276] ALS Defense. (2020, Apr.) SKYNET Mi-5. [Online]. Available: <https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail>
- [277] Delft Dynamics. (2020, Apr.) Dronecatcher. [Online]. Available: <https://dronecatcher.nl/>
- [278] Fortem Technologies. (2020, Apr.) Drone hunter. [Online]. Available: <https://fortemtech.com/products/dronehunter/>
- [279] SCI Technol.. (2020, Apr.) Aeroguard. [Online]. Available: <https://www.sci.com/aeroguard/>
- [280] Search Systems. (2020, Apr.) SPARROWHAWK. [Online]. Available: <http://www.searchsystems.eu/sparrowhawk.html>
- [281] SKYLOCK. (2020, Apr.) Counter drone net catcher. [Online]. Available: <https://www.skylock1.com/counter-drone-systems/>
- [282] D. Sathyamoorthy, "A review of security threats of unmanned aerial vehicles and mitigation steps," *The J. Defence and Security*, vol. 6, no. 1, pp. 81–97, Oct. 2015.
- [283] E. Ackerman. (2015, Apr.) South Korea prepares for drone vs. drone combat. [Online]. Available: <https://spectrum.ieee.org/automaton/robotics/drones/south-korea-drone-vs-drone>
- [284] OpenWorks Engineering. (2020, Apr.) Skywall. [Online]. Available: <https://openworkengineering.com/skywall-patrol/>
- [285] K. D. Atherton. (2016, Feb.) Trained police eagles attack drones on command. [Online]. Available: <https://www.popsci.com/eagles-attack-drones-at-police-command/>
- [286] A. Y. Javid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proc. IEEE Conf. on Technol. for Homeland Security (HST)*, Waltham, MA, USA, Nov. 2012, pp. 585–590.
- [287] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. IEEE Int. Symp. on Safety, Security and Rescue Robotics (SSRR)*, Shanghai, China, Oct. 2017, pp. 194–199.
- [288] (2020, Apr.) Pixhawk. [Online]. Available: <https://pixhawk.org/>
- [289] Our Bureau. (2014, Dec.) Us navy laser weapon fires at \$1 per shot. [Online]. Available: [https://www.defenseworld.net/news/11684/US\\_Navy\\_Laser\\_Weapon\\_Fires\\_at\\_1\\_Per\\_Shot#.XrdHc2gzaUI](https://www.defenseworld.net/news/11684/US_Navy_Laser_Weapon_Fires_at_1_Per_Shot#.XrdHc2gzaUI)
- [290] Fortune Business Insights. (2020, Feb.) Commercial drones market size, share & industry analysis, by product, by technology, by system, by industry, and regional forecast, 2019–2026. [Online]. Available: <https://www.fortunebusinessinsights.com/commercial-drone-market-102171>

- [291] K. Wackwitz. (2019, Dec.) The counter-drone market report 2020. [Online]. Available: <https://www.droneii.com/project/counter-drone-market-report-2020>
- [292] Grand View Research. (2019, May) Anti-drone market size worth \$4.5 billion by 2026. [Online]. Available: <https://www.grandviewresearch.com/press-release/global-anti-drone-market>
- [293] Research and Markets. (2019, Sep.) Global counter-UAS market: Focus on technology, application, end users - analysis and forecast, 2019-2024. [Online]. Available: <https://www.researchandmarkets.com/reports/4845575/global-counter-uas-anti-drone-market-focus-on>
- [294] Homeland Security Market Research. (2019, Feb.) Anti-drone market & technologies - 2019-2023. [Online]. Available: <https://homelandsecurityresearch.com/reports/counter-drone-market/>
- [295] (2020) Droneii: Drone industry insight. [Online]. Available: <https://www.droneii.com/>
- [296] Markets and Markets. (2019, Nov.) Anti-drone market by technology, application, vertical, and geography - global forecast to 2024. [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/anti-drone-market-177013645.html>
- [297] S. Kanowitz. (2019, Dec.) DOD invests in counter-drone technologies. [Online]. Available: <https://gcn.com/articles/2019/12/11/counter-uas.aspx>
- [298] Zion Market Research. (2019, Feb.) Anti-drone market by system, by technology, and by end-user: Global industry perspective, comprehensive analysis, and forecast, 2016-2025. [Online]. Available: <https://www.zionmarketresearch.com/market-analysis/anti-drone-market>
- [299] Modor Intelligence. (2019) Anti-drone market - Growth, trends, and forecast (2020-2025). [Online]. Available: <https://www.mordorintelligence.com/industry-reports/anti-drone-market>
- [300] A. Charlton. (2019, Dec.) Forbes: Drone (regulation) wars: U.S. and E.U. face off. [Online]. Available: <https://www.forbes.com/sites/andrewcharlton5/2019/12/09/drone-regulation-wars-and-eu-face-off/#5dd37c343412>
- [301] T. McMullan. (2019, Mar.) How swarming drones will change warfare. [Online]. Available: <https://www.bbc.com/news/technology-4755588>
- [302] J. Spero. (2019, Jun.) Concerns rise over use of drones in a swarm attack. [Online]. Available: <https://www.ft.com/content/c51fa3f8-8d10-11e9-a1c1-51bf8f989972>
- [303] C. Scotti. (2016, Aug.) Who can be killed by a drone? US reveals the rules of engagement. [Online]. Available: <http://www.thefiscaltimes.com/2016/08/09/Who-Can-Be-Killed-Drone-US-Reveals-Rules-Engagement>
- [304] Aveillant. [Online]. Available: <https://www.aveillant.com/>
- [305] Blihter. [Online]. Available: <https://www.blihter.com/>
- [306] Drone Citadel. [Online]. Available: <https://dronecitadel.com/>
- [307] (2020) Dronedefence. [Online]. Available: <https://www.dronedefence.co.uk/>
- [308] DroneShield. [Online]. Available: <https://www.droneshield.com/>
- [309] Liteye. [Online]. Available: <https://liteye.com>
- [310] Lockheed Martin. [Online]. Available: <https://www.lockheedmartin.com/en-us/index.html>
- [311] Northrop Grumman. [Online]. Available: <https://www.northropgrumman.com/>
- [312] Raytheon. [Online]. Available: <https://www.raytheon.com>
- [313] Saab AB. [Online]. Available: <https://saabgroup.com/>
- [314] SkySafe. [Online]. Available: <https://www.skysafe.io/>
- [315] Thales. [Online]. Available: <https://www.thalesgroup.com/en>
- [316] Whitefox defense technologies. [Online]. Available: <https://www.whitefoxdefense.com/>
- [317] Lockheed Martin. [Online]. Available: <https://www.lockheedmartin.com/en-us/products/indago-vtol-uav.html>
- [318] Northrop: Globalhawk. [Online]. Available: <https://www.northropgrumman.com/air/globalhawk/>
- [319] Raytheon: Silverfox. [Online]. Available: <https://www.raytheon.com/capabilities/products/silverfox>
- [320] Lockheed Martin: Drone Swarms. [Online]. Available: <https://www.lockheedmartin.com/en-us/news/features/2016/webt-laser-swarms-drones.html>
- [321] (2020) Northrop Grumman: Mobile Application for UAS Identification (MAUI). [Online]. Available: <https://news.northropgrumman.com/news/releases/northrop-grumman-demonstrates-counter-uas-technologies-at-black-dart-exercise>
- [322] Leonardo DRS Press Release. (2017, Oct.) U.S. army awards leonardo drs contract for production of counter-drone capability. [Online]. Available: <https://www.verticalmag.com/press-releases/u-s-army-awards-leonardo-drs-contract-production-counter-drone-capability/>
- [323] S. Lewis. (2020, Feb.) Drone defence releases solar sentinel drone detection system. [Online]. Available: <https://www.commercialdroneprofessional.com/drone-defence-releases-solar-sentinel-drone-detection-system/>
- [324] Liteye Press Release. (2020, Mar.) Liteye & Citadel push the envelope for state-of-the-art in countering UAS threats. [Online]. Available: <https://liteye.com/liteye-citadel-push-the-envelope-for-state-of-the-art-in-countering-uas-threats/>
- [325] C. Lee. (2019, Dec.) Web exclusive: Counter-UAS company purchases anti-drone shoulder rifle. [Online]. Available: <https://www.nationaldefensemagazine.org/articles/2019/12/19/counter-uas-company-purchases-anti-drone-shoulder-rifle>
- [326] MFI Press Release. (2018, Nov.) Liteye and Northrop Grumman demonstrate mobile, networked, electronic and kinetic capabilities to counter unmanned threat systems during army's maneuver and fires integration exercise (MFI 18). [Online]. Available: <https://liteye.com/liteye-and-northrop-grumman-demonstrate-mobile-networked-electronic-and-kinetic-capabilities-to-counter-unmanned-threat-systems-during-armys-maneuver-and-fires-integration-exercise-mfi-18/>
- [327] Liteye Press Release. (2020, Apr.) Liteye expands their counter UAS layered approach with Raytheon missiles & defense's phaser. [Online]. Available: <https://liteye.com/liteye-expands-their-counter-uas-layered-approach-with-raytheon-missiles-defenses-phaaser/>
- [328] Paris La Défense. (2017, Nov.) Thales completes the acquisition of Aveillant, world pioneer in holographic radar technology. [Online]. Available: <https://www.aveillant.com/thales-completes-the-acquisition-of-aveillant-world-pioneer-in-holographic-radar-technology/>
- [329] B. Stevenson. (2016, Apr.) Monaco to operate counter-UAV system. [Online]. Available: <https://www.flightglobal.com/civil-uavs/monaco-to-operate-counter-uav-system/120293.article>
- [330] A. Chua. (2017, Aug.) Singapore acquires radar system able to spot small drones up to 5km away. [Online]. Available: <https://www.todayonline.com/singapore/spore-acquires-radar-system-able-spot-small-drones-5km-away>
- [331] Airport Technol. (2017, Jul.) Aveillant installs drone detection radar at Paris Charles de Gaulle airport. [Online]. Available: <https://www.airport-technology.com/news/newsaveillant-installs-first-airport-drone-detection-radar-at-charles-de-gaulle-5863816/>
- [332] DroneShield. (2019, May) Thales purchases droneshield limited solutions, aims for integration with existing technologies. [Online]. Available: <https://www.droneshield.com/all-press-coverage/2019/5/1/thales-purchases-droneshield-limited-solutions-aims-for-integration-with-existing-technologies>
- [333] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, "Softwarization of UAV networks: A survey of applications and future trends," *IEEE Access*, vol. 8, pp. 98 073–98 125, May 2020.
- [334] J. McCoy and D. B. Rawat, "Software-defined networking for unmanned aerial vehicular networking and security: A survey," *Electronics*, vol. 8, no. 12, p. 1468, Dec. 2019.
- [335] G. Secinti, P. B. Darian, B. Canberk, and K. R. Chowdhury, "SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 16–21, Jan. 2018.
- [336] K. Chen, S. Zhao, N. Lv, et al., "Segment routing based traffic scheduling for the software-defined airborne backbone network," *IEEE Access*, vol. 7, pp. 106 162–106 178, Jul. 2019.
- [337] B. Nogales, V. Sanchez-Aguero, I. Vidal, and F. Valera, "Adaptable and automated small UAV deployments via virtualization," *Sensors*, vol. 18, no. 12, p. 4116, Nov. 2018.
- [338] S. Sezer, S. Scott-Hayward, P. K. Chouhan, et al., "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.
- [339] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3259–3306, Fourth Quarter 2018.
- [340] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

- [341] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.
- [342] B. Deng, C. Jiang, H. Yao, S. Guo, and S. Zhao, "The next generation heterogeneous satellite communication networks: Integration of resource management and deep reinforcement learning," *IEEE Wireless Commun.*, vol. 27, pp. 105–111, Apr. 2020.
- [343] T. Hong, W. Zhao, R. Liu, and M. Kadoch, "Space-air-ground IoT network and related key technologies," *IEEE Wireless Commun.*, vol. 27, pp. 96–104, Apr. 2020.



HONGGU KANG received the B.Sc. degrees in Electronic Engineering (*Summa Cum Laude*) from Hanyang University, Seoul, South Korea in 2017, and the M.Sc. degree in the School of Electrical Engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2019, where he is currently pursuing the Ph.D. degree. His research interests include signal processing for wireless communications, unmanned aerial vehicle communications, and machine learning. He was a recipient of the Korean Institute of Communications and Information Sciences (KICS) Fall Symposium Best Paper Award in 2019.

He was a recipient of the Korean Institute of Communications and Information Sciences (KICS) Fall Symposium Best Paper Award in 2019.



JINGON JOUNG (S'03–M'07–SM'15) received the B.S. degree in Radio Communication Engineering from Yonsei University, Seoul, South Korea, in 2001, and the M.S. and Ph.D. degrees in Electrical Engineering and Computer Science from KAIST, Daejeon, South Korea, in 2003 and 2007, respectively.

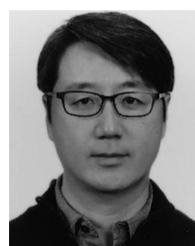
He was a Postdoctoral Fellow with KAIST, South Korea and UCLA, CA, USA, in 2007 and 2008, respectively. He was a Scientist with the Institute for Infocomm Research (I<sup>2</sup>R), Agency for Science, Technology and Research (A\*STAR) Singapore, from 2009 to 2015, and joined Chung-Ang University (CAU), Seoul, South Korea, in 2016, as a faculty member. He is currently an Associate Professor with the School of Electrical and Electronics Engineering, CAU, where he is also the Principal Investigator of the Intelligent Wireless Systems Laboratory. His research interests include communication signal processing, numerical analysis, algorithms, and machine learning.

Dr. Joung was a recipient of the First Prize of the Intel-ITRC Student Paper Contest in 2006. He was recognized as the Exemplary Reviewers of the *IEEE Communications Letters* in 2012 and the *IEEE Wireless Communications Letters* in 2012, 2013, 2014, and 2019. He served as the Guest Editor for the *IEEE ACCESS* in 2016. He served on the Editorial Board of the *APSIPA Transactions on Signal and Information Processing* from 2014 to 2019, and served as a Guest Editor for the *MDPI Electronics* in 2019. He is currently serving as an Associate Editor for the *IEEE Transactions on Vehicular Technology* and *MDPI Sensors*.



JINYOUNG KIM received the B.S. degree in Electrical Engineering from KAIST, Daejeon, South Korea, in 2001, and the Ph.D. degree in Business Management from Nanyang Business School at Nanyang Technological University, Singapore, in 2017.

Dr. Kim attended Technology and Policy Program of Engineering Systems Division at Massachusetts Institute Technology (MIT), USA, from 2002 to 2005, and was an assistant manager at Samsung Electronics, Suwon, South Korea from 2005 to 2008. She was also an in-house startup mentor at Seoul Global Startup Center from 2016 to 2017. She was a lecturer at Dongguk University from 2017 to 2019, and at Chung-Ang University in 2018. She is currently a research professor at Korea University Business School, Seoul, South Korea, since 2017. Her research interest includes entrepreneurship, technology innovation, and decision-making process under uncertainty. She is a member of Decision Science Institute and Academy of Management.



JOONHYUK KANG (Member, IEEE) received the B.S.E. and M.S.E. degrees from Seoul National University, Seoul, South Korea, in 1991 and 1993, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Texas, Austin, in 2002. He is currently a Faculty Member with the Dept. EE, KAIST, Daejeon, South Korea. From 1993 to 1998, he was a Research Staff Member with Samsung Electronics, Suwon, South Korea,

where he was involved in the Development of DSP-based real-time control systems. In 2000, he was with Cwill Telecommunications, Austin, TX, USA, where he participated in the project for multicarrier CDMA systems with antenna array. He was a Visiting Scholar with the School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA, from 2008 to 2009. His research interest includes signal processing for cognitive radio, cooperative communication, physical-layer security, and wireless localization. He was a recipient of the Texas Telecommunication Consortium Graduate Fellowship from 2000 to 2002. He is a member of the Korea Information and Communications Society and Tau Beta Pi (The Engineering Honor Society).



YONG SOO CHO was born in South Korea. He received the B.S. degree in electronics engineering from Chung-Ang University, Seoul, South Korea, in 1984, the M.S. degree in electronics engineering from Yonsei University, Seoul, South Korea in 1987, and the Ph.D. degree in electrical and computer engineering from the University of Texas, Austin, TX, USA, in 1991.

During 1984, he was a Research Engineer at Goldstar Electrical Company, Osan, Korea. In 2001, he was a Visiting Research Fellow at Electronics and Telecommunications Research Institute. Since 1992, he has been a Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, South Korea. He is the author of twelve books, more than 400 conference and articles, and more than 120 patents. His research interests include the area of mobile communication and digital signal processing, especially for MIMO OFDM and 5G.

Dr. Cho served as the President of the Korean Institute of Communications and Information Sciences, in 2016, and was a recipient of Dr. Irwin Jacobs Award in 2013.