Internet of Things 11 (2020) 100218

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Security analysis of drones systems: Attacks, limitations, and recommendations

Jean-Paul Yaacoub, Hassan Noura, Ola Salman*, Ali Chehab

AUB, Bliss Street Beirut Lebanon

ARTICLE INFO

Article history:
Received 22 July 2019
Revised 31 March 2020
Accepted 2 May 2020
Available online 8 May 2020

Keywords:
UAV
UAS
UUV
Armed drones
Drone/UAV warfare
Terrorism/counter-Terrorism
Drones security
Drones threats and vulnerabilities
Drones attacks
Drones security countermeasures techniques
Drones forensics

ABSTRACT

Recently, the world witnessed a significant increase in the number of used drones, with a global and continuous rise in the demand for their multi-purpose applications. The pervasive aspect of these drones is due to their ability to answer people's needs. Drones are providing users with a bird's eye that can be activated and used almost anywhere and at any time. However, recently, the malicious use of drones began to emerge among criminals and cyber-criminals alike. The probability and frequency of these attacks are both high and their impact can be very dangerous with devastating effects. Therefore, the need for detective, protective and preventive counter-measures is highly required. The aim of this survey is to investigate the emerging threats of using drones in cyber-attacks, along the countermeasures to thwart these attacks. The different uses of drones for malicious purposes are also reviewed, along the possible detection methods. As such, this paper analyzes the exploitation of drones vulnerabilities within communication links, as well as smart devices and hardware, including smart-phones and tablets. Moreover, this paper presents a detailed review on the drone/Unmanned Aerial Vehicle (UAV) usage in multiple domains (i.e civilian, military, terrorism, etc.) and for different purposes. A realistic attack scenario is also presented, which details how the authors performed a simulated attack on a given drone following the hacking cycle. This review would greatly help ethical hackers to understand the existing vulnerabilities of UAVs in both military and civilian domains. Moreover, it allows them to adopt and come up with new techniques and technologies for enhanced UAV attack detection and protection. As a result, various civilian and military anti-drones/UAVs (detective and preventive) countermeasures will be reviewed.

© 2020 Elsevier B.V. All rights reserved.

1. Introduction

The reliance and use of drones is constantly rising in numerous domains. This is due to the drones' ability to offer a live-stream, real-time video and image capture, along with the ability to fly and transport goods [1]. As a result, more than 10,000 drones will be operational for commercial use within the next five years. This is mainly due to their advantages over commercial helicopters when it comes to costs and budget [2]. Moreover, the technological advancement enables easy manipulations via smart-phones to fly mini-drones instead of using remote controllers. In fact, the use of drones is not limited to commercial and personal aims. Drones are being used by law enforcement and border control surveillance teams. In case of natural disasters, search and rescue teams employ them to gather information or to drop essential supplies.

* Corresponding author.
E-mail address: oms15@mail.aub.edu (O. Salman).

https://doi.org/10.1016/j.iot.2020.100218
2542-6605/© 2020 Elsevier B.V. All rights reserved.

However, drones are not being used exclusively by "good guys"; "bad guys" are leveraging drones to achieve their malicious objectives. Being easy to control, drones can be used to perform different attacks. On the other hand, drones expose security vulnerabilities that make them prone to hijacking. In this paper, we review the attacks from/to drones, along with their existing countermeasures.

1.1. Motivation

The reliance on wireless communications makes drones vulnerable to various attacks. These attacks can have drastic effects, including commercial and non-commercial losses. In this context, there is a lack of proper understanding on how hackers perform their attacks and hijack a drone, in order to intercept it or even crash it. In fact, drones can also be compromised for malicious purposes. Hence, there is a need to detect them and prevent them from causing any damage.

1.2. Related work

The security of civilian drones was reviewed in [3]. Also, different security attacks on drones were analyzed in [4–8]. Drones detection methods were reviewed in [9–12]. However, a main limitation of the previous work is the lack of a comprehensive analysis of the drones security vulnerabilities and the attack life cycle. Moreover, only one aspect of drones' security threats was addressed, attacks on drones. The existing countermeasures need to be analyzed, and new techniques need to be proposed to overcome the limitations of the existing security solutions.

1.3. Contributions

In this work, we conduct a comprehensive review of the different aspects of drones' cyber-security including two main aspects: drones' security vulnerabilities, and the security concerns associated with compromised drones. Then, we review the countermeasures to secure drone systems, and to detect malicious ones. These contributions are summarized below:

- Identifying the main architecture of drones and their various communication types.
- Drone security and privacy concerns are discussed, mainly drone vulnerabilities, threats and attacks.
- Existing countermeasures of drones security vulnerabilities and threats are reviewed, in addition to countermeasures in case of compromised (malicious) drones.
- Finally, the limitations of the existing works, and recommendations for future research directions are included.

1.4. Organization

This paper is organized as follows: in Section 2, an overview of drones regulations, architecture, communication types, and classification is presented. Section 3 discusses drones' applications and domains of use. In Section 4, the drones security concerns and the effects of security breaches are analysed. Section 5 reviews the main drones security vulnerabilities and threats. The existing solutions and countermeasures for securing drones are reviewed in Section 6. In Section 7, the anti-drones countermeasures are presented. The current limitations, and recommendations for future research directions are included in Section 8. Finally, we conclude our work in Section 9.

2. Background and overview

According to the Federal Aviation Administration (FAA), more than 2.5 million drones are currently flying over the United States (U.S.) alone. In fact, this number is expected to reach 7 million active drones by 2020 [13]. Moreover, the technological and economical growth of e-commerce enabled many applications that leverage the use of drones [14]. On the other hand, this gives rise to opportunities for cyber-criminals to compromise or even exploit drones availability and capability for malicious purposes.

Since the early introduction of Unmanned Aerial Vehicles (UAVs), drones are looked upon as being associated with major security issues [15], rendering them legitimate targets that are prone to various cyber-attack types. Moreover, they can also be used as a potential attack vector for malicious users. Thus, boosting the chances for a new asymmetric type of warfare. In fact, drones operate at different wireless communication frequencies, as illustrated in Table 1, which compares the two main drones communication frequencies, 2.4 GHz and 5GHz.

2.1. Regulations

Many governments including EU State members, the US, United Kingdom (UK) and South Africa [16–20] have so far issued a warning for drone owners, urging them to get official licenses in order to fly their photography drones. The statement warned against the "threats of flying UAVs over private territories, especially military centers, and sensitive locations without a license issued by the orientation directorate." In Lebanon, the Lebanese Army stated that any drone being flown illegally without meeting the requirements "will be brought down whilst its owners will be legally prosecuted", due to the

Table 1
Comparison between 2.4 GHz and 5GHz.

Parameters	2.4 GHz	5 GHz
Frequency band	Lower frequency	Higher frequency
Cost	Less expensive	More expensive
Range	Covers long ranges	Covers short ranges
Effect of noise	Noisy	Less noisy
Interference	High chance of interference	Low Chance of interference
Physical barriers	Able to overcome certain physical barriers	Unable to overcome physical barriers
Performance	Affects Wi-Fi network speed	Does not affect Wi-Fi network speed

fact that they impose a "serious risk to the official institutions, the security, and public safety." As part of a constant reminder, the army's command of each country reminds all citizens to obtain the legally required certificates and to request a permit in order to use a drone; such requests can be made online using official websites. According to British Broadcasting Corporation (BBC) News [21], the civil aviation authority launched its drone-code to clarify the rules that each drone owner must follow and comply to

- Do not fly the drone above 400 feet.
- At all times, keep the drone away from aircraft, helicopters, airports, and airfields.
- Fly safely or face prosecution.
- As for drones fitted with cameras, they should not be flown:
  - Within 50 m of people, vehicles, buildings or structures.
  - Over large gatherings like concerts or/and sports events.

Many of these rules already came into effect by the end of July 2018, restricting all drones from flying above 400 ft. In fact, violators could be punished with unlimited fines or/and up to five years in jail. For this reason, this paper presents and classifies the main regulations applied in different countries per continent as illustrated in Table 2, while relying on a series of conducted surveys, reviews and comparative studies in [22–26].

2.2. Drone architecture

Typically, any UAV or drone architecture consists of three main elements: Unmanned Aircraft (UmA), Ground Control Station (GCS), and Communication Data-Link (CDL) [3,27]. These components are briefly described in the following:

- **Flight Controller:** it is classified as the drone's central processing unit [3].
- **Ground Control Station:** it is based on an On-Land Facility (OLF), which provides human operators with the necessary capabilities to control and/or monitor UAVs during their operations from a distance. GCSs differ depending on the size, type, and drones' missions.
- **Data Links:** are wireless links used to control the information flow between the drone and the GCS. This depends on the operational range of UAVs. Based on the research in [3], drones' control can be categorized based on their distance from the GCS:
  - **Visual Line-of-sight (VLOS) Distance:** allows control signals to be sent and received via the use of direct radio waves.
  - **Beyond Visual Line-of-Sight (BVLOS) Distance:** allows drones to be controlled via satellite communications [27].

2.3. Drones communications types

Drone communications can be classified into four main types, Drone-to-Drone (D2D), Drone-to-Ground Station (D2GS), Drone-to-Network (D2N), and Drone-to-Satellite (D2S). The communication framework is illustrated in Fig. 1.

2.3.1. Drone-To-Drone

Such communication is not yet standardized. In fact, Machine Learning can be leveraged in order to design and optimize a smart UAV-based wireless communication system [28]. In most cases, D2D communications can be modeled as Peer-to-Peer (P2P) communication. This would make it vulnerable to various types of P2P attacks including jamming (i.e Distributed Denial of Service (D-DoS) and sybil attacks) [29–31].

2.3.2. Drone-To-Ground station

This communication type is based on the already known and standardized industrial protocols, which are based on wireless communications such as Bluetooth and Wi-Fi 802.11 including 2.4 GHz and 5 GHz. However, most drone-to-ground communications are public and not secure, using a single factor authentication, which can be easily broken, making them vulnerable to passive (eavesdropping) and active (man-in-the-middle) attacks.

Table 2
World-Wide UAS regulations.

Global Appliance		Initial Regulations				Operational Requirements						Flight Path			
Continent	Country	Weight (<25 Kg)	Requirements	Weight (>25 KG)	Requirements	Spatial Restriction	Radio Communication	Visual Line of Sight	Safety Features	Insurance	Privacy	Jurisdiction	Registration & Labelling	Flight Authorisation Details	Operator Qualification
Europe	**France**	**If applied**	**No special permit**	**If applied**	**Subject to EU-Level regulation**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**100m-1km**	**Design certificate, call-to-base**	**Local law**	**No specified privacy regulation**	**National government**	**Operators name, address, telephone**	**Description of flights & undertaken safety measures**	**Theoretical competence certificate**
	United Kingdom	**If applied**	**License requirements**	**If applied**	**Airworthiness & flight-crew requirements**	**Military installations, airports, prisons, nuclear power plants**	**35 MHz/ Standard 2.4–5 GHz**	**Direct unaided visual contact**	**Design certificate, call-to-base**	**Liability insurance**	**Restricted recording of individuals**	**Local government**	**Name, address, date-of-birth, purpose**	**Predefined path, usage purpose & details**	**Proof of experience, knowledge & training**
	Germany	**If applied**	**Specific flight authorisation permit**	**If applied**	**Not authorised**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**100m-1km**	**Design certificate, call-to-base**	**Liability insurance**	**Restricted recording of individuals**	**Local government**	**Name, address, date-of-birth, purpose**	**Predefined path, usage purpose & details**	**Proof of experience, knowledge & training**
	Poland	**If applied**	**No registration**	**If applied**	**Permit is required W/O restriction**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Allowed beyond VLOS**	**Design certificate, call-to-base**	**Liability insurance**	**Unspecified**	**Local government**	**Name, address, details**	**Predefined path, usage purpose & details**	**Medical checkup, theoretical & practical tests**
	Sweden	**If applied**	**Depending on use**	**If applied**	**License from Swedish Transport Agency (STA)**	**Not authorised**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS**	**Liability insurance**	**Restricted recording of individuals**	**Swedish Post & Telecom Authority-Local government**	**Name, address, number, license, registration number**	**Embedded emergency device, enabled UAS shutdown system**	**Adult, less than 67, medical checkup, obtain an STA certificate**

(*continued on next page*)

Table 2 (*continued*)

Global Appliance		Initial Regulations				Operational Requirements						Flight Path			
Continent	Country	Weight (<25 Kg)	Requirements	Weight (>25 KG)	Requirements	Spatial Restriction	Radio Communication	Visual Line of Sight	Safety Features	Insurance	Privacy	Jurisdiction	Registration & Labelling	Flight Authorisation Details	Operator Qualification
	Ukraine	**If applied**	**No registration**	**If applied**	**Must be registered**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS**	**Unspecified**	**Not required**	**No firm restrictions**	**Local government**	**Name, address, phone number, purpose**	**Purpose of use**	**National, adult**
Oceania	**Australia**	**If applied**	**No permit needed**	**If applied**	**Remote pilot license or operator certificate**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS unless approved**	**Design certificate, call-to-base**	**Liability insurance**	**Restricted recording of individuals**	**Local government**	**Name, address, date-of-birth, purpose**	**Predefined path, usage purpose & details**	**Aside certificate, complete certain UAS flying hours**
	New Zealand	**If applied**	**Must be inspected & approved**	**If applied**	**Unmanned aircraft operator certificate**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**BVLOS if certified**	**Design certificate, call-to-base, emergency landing**	**Liability insurance**	**New Zealand privacy Act**	**Civil Aviation Authority-Department of Conservation**	**Name, address, date-of-birth, purpose**	**Physical location, risk/hazard assessment, aircraft details**	**Evidence of license, skill, knowledge & experience to operate a UAS**
Asia	**China**	**If applied**	**Not required**	**If applied**	**Interim UAS regulation provisions**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**VLOS daytime, BVLOS for emergencies**	**Not enforced**	**Not always applied**	**Still debatable**	**China's civil flight regulatory**	**Name, address, phone number**	**Flight purpose, filmed locations, flight path**	**National, adult, licensed**
	Japan	**If applied**	**Must be licensed**	**If applied**	**Not authorised/permit required**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS**	**Design certificate, call-to-base**	**Liability insurance**	**Restricted recording of individuals & places**	**Local government**	**Name, address & purpose**	**Predefined path, usage purpose & details**	**National, adult, Proof of license & experience**

(*continued on next page*)

Table 2 (*continued*)

Global Appliance		Initial Regulations				Operational Requirements						Flight Path			
Continent	Country	Weight (<25 Kg)	Requirements	Weight (>25 KG)	Requirements	Spatial Restriction	Radio Communication	Visual Line of Sight	Safety Features	Insurance	Privacy	Jurisdiction	Registration & Labelling	Flight Authorisation Details	Operator Qualification
Middle East	**Lebanon**	**If applied**	**Flight license**	**If applied**	**Prohibited/ forbidden**	**Military installations, airports, prisons, police stations**	**Standard 2.4–5 GHz**	**Within VLOS daytime**	**To be applied**	**N/A**	**Forbidden to record individuals/places**	**Ministry of Defense**	**Name, date-of-birth, address, job, flight date**	**Predefined path, specified date, aircraft type & location**	**Licensed & experienced pperator**
	Israel	**If applied**	**Subject to extensive regulations**	**If applied**	**Subject to extensive regulations**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS daytime**	**Design certificate, call-to-base, emergency landing**	**Liability insurance**	**Forbidden to record individuals/places**	**Israeli Civil Aviation Agency-Local Government**	**Only owned by authorised citizens & incorporation, fire-resistant plates, aircraft type, model & serial number**	**Predefined path, location, type, place & purpose**	**National, adult, location, work, address, authorised, operator characteristics**

(*continued on next page*)

Table 2 (*continued*)

Global Appliance		Initial Regulations				Operational Requirements						Flight Path			
Continent	Country	Weight (<25 Kg)	Requirements	Weight (>25 KG)	Requirements	Spatial Restriction	Radio Communication	Visual Line of Sight	Safety Features	Insurance	Privacy	Jurisdiction	Registration & Labelling	Flight Authorisation Details	Operator Qualification
Africa	**South Africa**	**If applied**	**Approval letter, registration certification, & UAS operator certificate**	**If applied**	**Not authorised/special permit**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**BVLOS if certified**	**Design certificate, call-to-base**	**Liability insurance**	**To be applied**	**Civil Aviation Authority-Local Government**	**National, nationality & registration marks**	**Approval letter, flight purpose, registration certificate, UAV design type**	**Medical assessment, evidence of training completion, adult, security background check**
America	**Canada**	**If applied**	**No permit needed**	**If applied**	**Special flight operations certificate**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS**	**Design certificate, call-to-base, safe landing**	**Local government**	**Liability insurance**	**Restricted recording of individuals/places**	**Name, address, date-of-birth, purpose**	**Predefined path, usage purpose & details**	**Adult, special flight operations certificate**
	United States	**If applied**	**License/ permit**	**If applied**	**Not authorised/special permit**	**Military installations, airports, prisons, nuclear power plants**	**Standard 2.4–5 GHz**	**Within VLOS**	**Design certificate, call-to-base, safe landing**	**Federal Aviation Administration**	**Liability insurance**	**Restricted recording of individuals**	**Name, address, date-of-birth, purpose**	**Predefined path, Usage purpose & details**	**Adult, flight certificate**

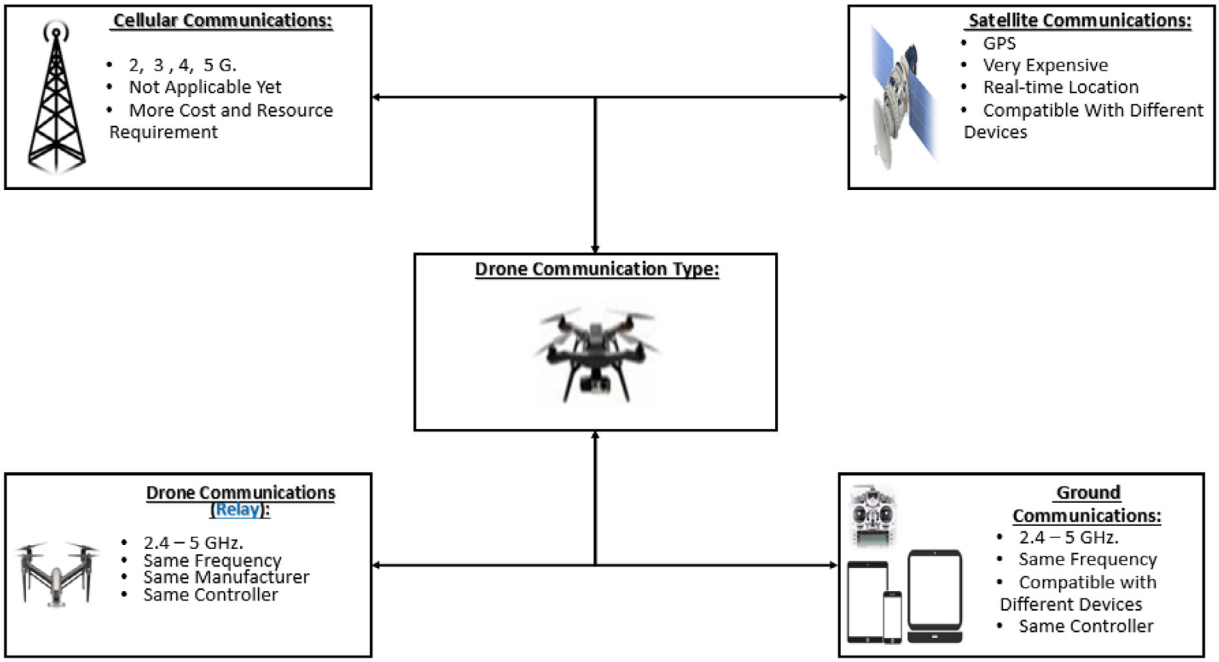


Fig. 1. The different possible drone communication

2.3.3. Drone-To-Network

This communication type allows the choice of the network based on the required security level. It may also include cellular communications, which means relying on 3 GHz, 4 GHz, 4G+ (LTE) and 5 GHz. It is essential to secure such wireless communications networks when being used.

2.3.4. Drone-To-Satellite

This is the type of communication needed for sending real-time coordinates via the Global Positioning System (GPS). This allows any drone to be called back to its initial station in case it went beyond the line of control or outside the line of sight. Satellite communications are deemed secure and safe. However, they exhibit a high cost and maintenance requirements. This is why they are heavily used by armed forces.

2.4. UAV Types

All UAVs are drones, however, not all drones are UAVs. This paper details the difference between drones, UAVs, and Unmanned Aircraft Systems (UAS); Fig. 2 presents a classification of UAVs.

2.4.1. Drones

This term is commonly used to refer to remotely (autonomously) guided aircraft. This term also describes various vehicles including submarines or land-based autonomous vehicles. In fact, drones can be classified into three main types, according to their flying mechanisms [32], as described next.

- **Multi-Rotor Drones:** they are also known as rotary-wing drones. They are based on the Vertical Take-Off and Landing (VTOL) principle. Moreover, due to their manoeuvrability, they can hover over a fixed location, which allows them to provide a constant cellular coverage over certain areas. Therefore, multi-rotor drones can act as base stations at their intended locations with high accuracy and precision. However, their mobility is very limited and they consume large amounts of energy.
- **Fixed-Wing Drones:** these are more energy efficient [33,34] than multi-rotor drones. This is due to their ability to glide and travel at a high speed, while carrying heavy payloads. The main drawback of fixed-wing drones is the need for a runway to take off and land [35], due to their Horizontal Take-Off and Landing (HTOL) nature. Another drawback is their inability to hover over fixed locations, in addition to their expensive software/hardware nature.
- **Hybrid-Wing Drones:** these are fixed/rotary wing drones that recently made it the market. This type of drones is able to reach the destination quickly by gliding over the air and hovering through the use of four rotors.

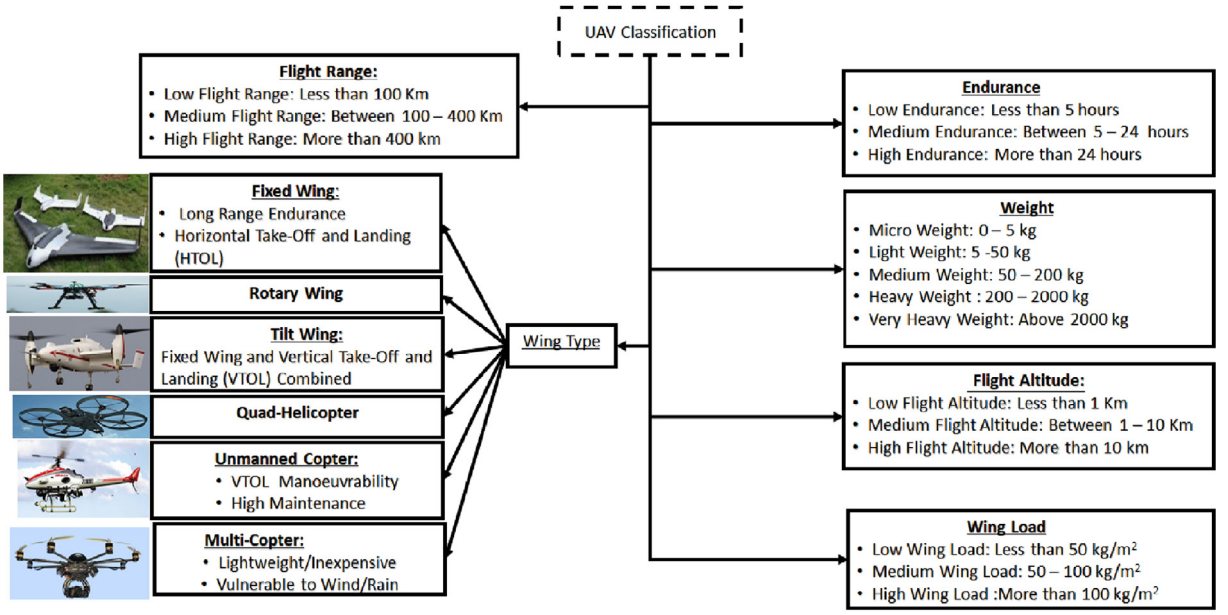


Fig. 2. UAV classification

2.4.2. UAVs

A UAV can fly remotely/autonomously using a controller, mobile phone, computer or even a tablet [36]. They are characterised by their autonomous flight capabilities and ability to operate over long distances with a secure live feed transmission. Moreover, UAVs control can be classified and divided into three main categories [3]:

- **Remote Pilot Control:** known as operator static automation, where all decisions are made by a human remote operator.
- **Remote Supervised Control:** known as adaptive automation. It offers the drones the ability to launch and carry out a given mission process independently, while allowing for human intervention, if needed.
- **Full Autonomous Control:** known as system static automation, where drones can make all required decisions for a successful mission completion, without the need for any human intervention.

2.4.3. UAS

These include UAVs and drones, and the operators controlling them [37]. A UAV is a type of UAS since it refers to a controlled vehicle or aircraft [38].

2.4.4. RPA

RPA stands for Remotely Piloted Aircraft, which requires intensive skills and training over a long period of time (a couple of years) to operate and control these complex flights [37].

2.5. Crash avoidance methods

Various drone types are now equipped with crash avoidance systems, to navigate around objects and to return back to base on a programmed route. This is possible using Radio-Frequency Identification (RFIDs) and low power Radio-Frequency (RF) transmitters continually broadcasting their identities. This ensures that the asset is protected, and located at legitimate entry points at all times.

2.6. Collision avoidance (CA) methods

Due to the continuous and close encounters between aircraft and UAVs, it is critical to avoid any collision between them. As a result, in [39], several methods were discussed along the modeling and evaluation of drones safety, and by applying these methods on Unmanned Aircraft Systems (UASs). The aim was to develop a UA-Sense-and-Avoid (SAA) system, based on the ability to sense and avoid obstacles, in coordination with the Federal Aviation Administration (FAA) standard (RTCA SC-203) [40]. Another method for SAA was also presented by Barfield in [41]. The method is based on an autonomous CA system that offers protection to prevent any collision. This was successfully done without causing any failure in the flight operation. In fact, CA algorithms were developed in [42] to perform certain tasks including Individual Collision Avoidance (ICA) in 2D and Group Collision Avoidance (GCA) in the 3D plane. Another method was presented by Yang et al. in [43] and

it is based on the UAV 3D path planning, which consists of locating a collision-free path in a 3D cluttered environment based on three main constraints, geometric, physical and temporal.

2.7. Obstacle-Collision avoidance methods

Different obstacle-collision avoidance methods were also presented to overcome any obstacle facing the UAVs. In [44], Ueno et al. presented a law that enables an aircraft to accurately localize objects in its vicinity. In [45], Brandt et al. stated that quad-rotors are more suitable to operate indoors due to their flexible operations in small and confined areas. Furthermore, an algorithm was presented by Israelsen et al. in [46] to manually tele-operate UAVs using automatic Obstacle Collision Avoidance (OCA).

2.8. UAV Routing

It is important to ensure a safe routing path for drones to avoid accidents, damage or/and injuries. To do that, one must take into consideration the threat, risk, target, and terrain, along with the UAV restrictions. As a result, in [47], Tulum et al. introduced an agent-based approach for the UAV mission route planning problem, by using situation awareness algorithms. Moreover, deterministic and probabilistic path planning strategies for autonomous UAV networks were followed through the exploration of obstacles in an area [48]. In [49], Hernández et al. applied a graph-based method for a multi-objective route planning of a simulated UAV to adhere to the required safety considerations.

This section described briefly the drone architecture, communications types, and UAV types. Also, the difference between drones, UAV, and UAS. Note that firmer regulations are still needed to ensure a safer use of UAV and UAS, especially with the recent encounters between drones/UAVs and other aircrafts. In the next section, the security of main UAV applications will be presented.

3. Domains of use

Drones will play a major role in the near future, by delivering goods and merchandise, or even serving as flying mobile hot-spots for broadband wireless access. In fact, when drones are deployed as hot-spots, the most suitable solution for bandwidth allocation is the Binomial and Poisson cluster processes, as presented in [50]. The main goal is to serve a massive number of users in a specific area. Moreover, drones can be used to maintain all the needed security and surveillance techniques, which are implemented to ensure the usage of these drones safely, securely and properly according to [14].

Therefore, the focus is on the multi-purpose usage of these drones, both in the civilian and military domains. The multi-purpose uses of drones are illustrated in Fig. 3 and discussed next.

3.1. Civilian multi-Purpose use cases

Lately, drones have been used in various civilian domains [3]. Many of these domains are mentioned and discussed in [51], including search and rescue, and disaster management. The main civilian applications of drones include:

- **Cinematography:** Drones are currently being used by various filmmakers to ensure aerial filming like never before, enabling a new level of creativity with a bird's eye view [52].
- **Natural Disaster Response and Control:** UAVs are being deployed for disaster control and assessments ever since the Katrina hurricane in 2005, where roads were blocked by fallen trees, cars, road signs, etc. This helped in assessing the disaster consequences and in checking for missing, injured and trapped survivors.
- **Search and Rescue:** UAVs can be used for the purpose of searching for lost, scattered or stranded people, especially when human presence is deemed dangerous or limited.
- **Tourism:** UAVs can also be used to capture stunning views including the bird's eye view. This can be used to attract tourists and to promote touristic places and areas of interest [53], which enhances the overall tourism industry.
- **Commercial Ads:** Drones are also being used in commercial ads since they can be used to capture (film) a scene with High Definition (HD) quality and for a specific amount of time. This reduces the need for expensive equipment and human interaction.
- **Crisis Management:** In case of a terrorist attack or a natural disaster (earthquake floods), UAVs can act as hot spots or base stations, which allows for the collection of short messages sent by affected people [54], or used to alert response teams [55]. In other cases, it helps in locating people based on their GPS location or MAC addresses. However, in case of a terrorist attack, they might act as an Access Point (AP) for a suicide bomber's detonator, which facilitates the activation and detonation of a bomb.
- **Emergency Response:** Drones are currently being used as mobile medical kits that can be sent to first aid response teams on scene [56]. This offers the necessary help without delays, in contrast to ambulance cars. In fact, drones were deployed across the streets of Spain and China (mainly Wuhan), using cameras and speakers to raise awareness and warm people, using aerial spray and disinfection to fight the corona-virus (COVID-19) spread [57,58]. In addition, drones were used as a flying delivery mean to supply isolated/infected patients with goods (i.e food and medicine), and also as a flying mean to transport testing samples at a faster pace, reducing human interaction [59].

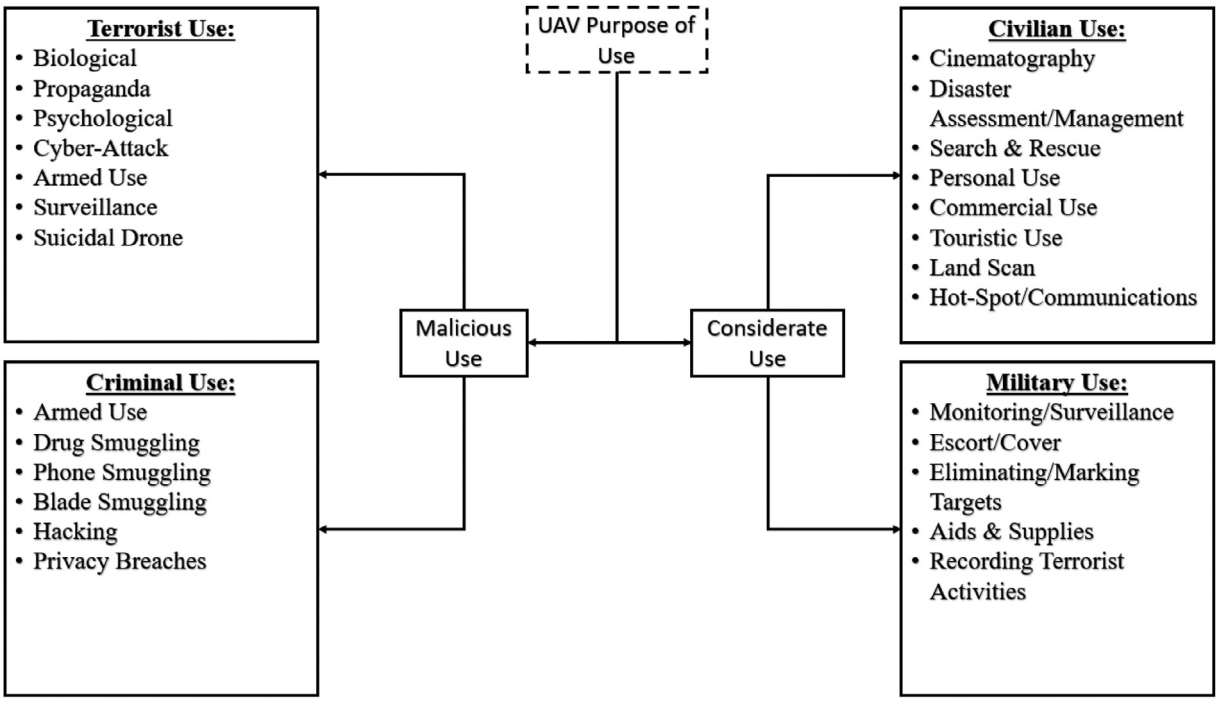


Fig. 3. Drone multi-purpose usage

- **Environmental Management:** Drones can be used to perform pollution measuring tasks [60] (i.e environmental drones for air quality measurement and analysis [60–62]), agricultural tasks [63] (i.e soil analysis, crop/seed/livestock management and pest control [64–67]), or nature/wildlife research/conservation tasks (i.e anti-poaching, endangered species protection [68–71]).
- **Underwater/Maritime Purposes:** Underwater drones or Unmanned Ocean Vehicles (UOV) saw an increase use of underwater search-and-rescue operations [72,73], environmental and coastal data collection [74,75] and detecting and monitoring maritime fauma (animals) [76,77].

3.2. Police multi-Purpose usage

Drones are used to track down suspects using the aerial bird watch view. This proved to be cheaper and more maneuverable than a helicopter. In fact, drones will soon have the ability to contain thermal, motion, and night vision detection, which can be used to track down suspects at any time of the day. Furthermore, drones can be used to enhance traffic efficiency by offering quick response and identification of road conditions. This helps in avoiding traffic congestion, and in responding to a traffic accident or emergency. Moreover, these drones can be used for surveillance purposes, with the ability to detect suspicious targets hidden within public domains, which proved to be more flexible than fixed cameras. The reason is due to their capability in identifying and recognizing suspects from their height, size, and facial recognition, and thus, making it very difficult for suspects to hide in public.

In fact, according to BBC News, the UK prison service and the police are investing their resources to stop drone pilots from flying drugs, mobile phones, blades, knives, Subscriber Identity Module (SIM) cards, Universal Serial Bus (USBs) etc. into prisons [78]. These drones were being flown over walls and physical barriers. As a result, reports revealed that almost £ 3m may possibly be spent on the newly assigned task force to overcome this problem.

As a result, due to the autonomous and operational nature of drones, they became more and more adaptable and operational. This reduces and replaces the use of choppers, decreasing the response time and needed resources. Drones are capable of capturing a live bird-view of different types of incidents ranging from crimes, theft, to even riots. This leads to a firmer response with a more enhanced plan due to the ability to identify suspects while locating and tracking them down before arresting them.

Also, UAVs can be used by the police and other agencies to gather crucial information in dangerous situations with less manpower and money [79,80]; drones were used by the police 372 times across Northern Ireland since 2013. The paper explains the reasons for using drones in the case of aerial surveillance based on real-case incidents as shown below:

- **Traffic Monitoring:** UAVs are being used to monitor traffic and accident scenes, such as the case of their use in the state of Illinois since 2015, and in India including Kanpur city [81], as well as their use in Spain to monitor traffic black-spots [82].
- **Tracking Escapees:** UAVs were used to monitor escapees from crime scenes and prisons. A prime example of that is when in 2016 the Ohio police department managed to track down an escaped inmate using a drone, which led to his arrest. In 2010, the UK police managed to capture a car thief in the city of Merseyside. In 2011, a Predator drone was used to assist in the arrest of a suspect in North Dakota [83].
- **Forensics Search & Rescue:** UAVs were used in solving crimes incidents such as the case of Ms. Tara Grinstead 2005 murder, where a fixed wing drone, called Spectra, was used by the Irwin County Sheriff's Office in Georgia, while another drone was used by the specialist Gene Robinson to cover large areas in search of her whereabouts. The case was not solved until February 2017, when one of her students confessed to her murder to the Georgia Bureau of Investigations (GBI) [84,85].
- **Anti-Rioting:** UAVs saw recent use in counter-protest efforts, as part of crowd control tactic used by Israel towards Palestinians [86]. As early as 2015, experiments were conducted by using drones armed with tear gas [87], and the Indian police considered using drones armed with pepper-spray [88]. Around March, 2018, the Israeli Defense Force (IDF) and police started using drones armed with tear-gas to disperse Gaza protesters from the Israeli-Palestinian borders [89,90].

3.3. Military applications

UAVs became the perfect choice for military usage [91], especially for intelligence and reconnaissance purposes [92] performing **Surveillance, Target Acquisition and Reconnaissance (STAR), Joint Surveillance Target Attack Radar (JSTAR), Reconnaissance, Surveillance and Target Acquisition (RSTA)** [93–95] tasks. Their deployment is a key part to counter insurgency and terrorism, offering the ability to Track and Identify Dismounted Personnel (TIDP) in urban environments, especially in Areas of Operation (AO) [96].

Fig. 3 presents a summary about several Drone/UAV types being used in overt/covert military operations, which are described next.

- **P-CAS:** more efforts are directed to enable UAVs to offer a Persistent-Close Air Support (P-CAS)/Precision Strikes for real-time protection of ground troops [97,98] and for a quick target elimination through the use of laser-guided missiles and without waiting for an airstrike-call [99]. This method was applied by the American, (British) and French armed forces in Mali [100–103], Somalia and Djibouti [104,105], Kenya [106] and Nigeria [107] (mainly against Boko-Haram [108,109], and Al-Shabaab [110–112]); hence, the Unmanned Combat Aerial Vehicle (UCAV) term was introduced [113]. These drones can also be used to help (elite) troops in their covert, overt or clandestine operations by offering guidance, close air-support or currently active/passive enemy movement as part of **Surveillance, Target Acquisition, and Reconnaissance (STAR), Reconnaissance Surveillance Target Acquisition (RSTA)**, and/or **Combat, Intelligence, Surveillance, Reconnaissance (CISR)** [114], to enhance the **Command, Control, Communications, Computers, Intelligence, Surveillance, & Reconnaissance (C4ISR) role** [115] and overcoming the limited **Intelligence, Surveillance, and Reconnaissance (ISR)** role of Unmanned Ground Vehicles (UGVs).
- **Precision Shelling:** UAVs were also used to conduct precision shelling against terrorist targets [116]. In fact, Russia has been relying on this Guided Artillery Rounds technique as early as July 2015 [117–119]. This technique was also adopted by Pro-Russian separatists against Ukrainian forces in 2014 [120,121], and by Ukrainian forces against Pro-Russian separatists in 2019.
- **Aerial Surveillance/Reconnaissance:** unlike the reliance on Human Intelligence (HUMINT), UAVs were also deployed as part of aerial intelligence and information gathering, allowing the identification and tracking of insurgents (i.e training, movement and camps), vehicles (i.e movement, types), weapons, weapon caches, and Improvised Explosive Devices (IED) (i.e factories, equipment, market, and planting), especially in Afghanistan [92,96]. In fact, they were also used by both Ukrainian forces and pro-Russians [122] for reconnaissance and counter-reconnaissance purposes during the Ukraine war [120,123]. Recently, a new Russian drones' footage emerged on February 2020, exposing how Turkish artillery batteries are targeting the Syrian army in support of anti-government rebels [124] in Idlib [125].
- **Unmanned Airstrikes:** were the prime choice of the US as early as 2002, especially in the elimination of Al-Qaeda operatives in Yemen [126] with their use of predator drones [116,127], before evolving into their authorised use in their Global War Against Terror (GWAT) [128] along their British counterparts [129]. Moreover, Israel also relied on the extensive use of drones and UAVs [130] to perform unmanned airstrikes against key targets/figures in the West Bank, and military installations in Iraq and Syria [131–133]. The same goes for Russia and Iran (Shahed-129 drone [134]) using UAVs to counter uprising insurgencies and terrorism in Syria [135]. Recently, after the loss/injury of more than 59 Turkish soldiers by Syrian airstrikes as part of "Dawn of Idlib 2" [136], the Turkish army extensively used drones in retaliation attacks to target the Syrian Regime's troops and allies' military targets and installations in series of well-coordinated drone strikes [137,138], before a cease-fire was established [139–141], and before risking further escalation with Russia [142].
- **UAV Hijacking:** This is done mainly through GPS spoofing/jamming, and it was very effective in the Ukrainian conflict [143] and in countering ISIL's threat, especially over the city of Mosul, until its liberation in 2017 [144].

Table 3
Military drone/UAV classification.

Table 4
Drones/counter-drones cyber-attacks.

Attack		Targets					Security Measures	
Type	Nature	Privacy	Data Confidentiality	Integrity	Availability	Authentication	Non-Cryptographic	Cryptographic
Malware	Infection	✓	✓	✓	✓	✓	Hybrid lightweight IDS	Control access, system integrity solutions and multi-factor authentication
BackDoor Access	Infection	✓	✓	✓	✓	✓	Hybrid lightweight IDS, vulnerability assessment	Multi-factor robust authentication scheme
Social Engineering	Exploitation	✓	✓	X	X	✓	Raising awareness, training operators	N/A
Baiting	Exploitation	✓	✓	✓	X	✓	Raising awareness, training operators	N/A
Injection/Modification	Exploitation	✓	X	✓	X	X	Machine-Learning hybrid IDS, time stamps	Message authentication or digital signature
Fabrication	Exploitation	✓	X	✓	X	✓	, Assigning privilege	Multi-factor authentication, message authentication or digital signature
Reconnaissance	Information gathering	✓	✓	X	X	X	Hybrid lightweight IDS	Encrypted traffic/stream
Scanning	Information gathering	✓	✓	✓	X	X	Hybrid lightweight IDS or Honeypot	Encrypted traffic/stream
Three-Way Handshake	Interception	X	X	X	✓	✓	Traffic filtering, close unused TCP/FTP ports	X
Eavesdropping	Interception	✓	✓	X	X	X	N/A	Securing communication/traffic, secure connection
Traffic Analysis	Interception	✓	X	X	X	X	N/A	Securing communication/traffic, secure connection
Man-in-the-Middle	Authentication	✓	✓	✓	X	X	Lightweight hybrid IDS	Multi-factor authentication & lightweight strong cryptographic authentication protocol
Password Breaking	Cracking	X	X	X	X	✓	Lightweight IDS	Strong periodic passwords, strong encryption
Wi-Fi Aircrack	Cracking	X	X	X	X	✓	Lightweight IDS at the physical layer	Strong & periodic passwords, strong encryption algorithm
Wi-Fi Jamming	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
De-Authentication	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Replay	Jamming	X	X	X	X	✓	Frequency hopping, time stamps	N/A
Buffer Overflow	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Denial of Service	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
ARP Cache Poison	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Ping-of-Death	Jamming	X	X	X	X	✓	Frequency range variation	N/A
GPS Spoofing	Jamming	X	X	X	X	✓	Return-to-base, frequency range variation	N/A

- **Covert Aerial Surveillance/Reconnaissance:** UAVs were being developed and produced as early as world war one [145], using Archibald Montgomery Low's radio control techniques to counter the Zeppelins threat [146], before their covert use in the cold war era for spying purposes, and during the Vietnam war as part of reconnaissance [147]. This included their use by the US-led coalition forces, mainly the British in operation Herrick [148,148–150], Afghanistan.
- **Evading Radar-Detection:** another military purpose of drones is to avoid radar detection. The Harop IAI [151], or HARPY IAI 2 [152] along the British "Fire Shadow" [153], are classified as anti-radiation drones. They are capable of autonomously reaching their targets without the need to carry a warhead by self-destruction into the main target. However, IAI Harop showed a higher success and accuracy rate compared to the Fire Shadow, yet the British Ministry of Defense (MoD) stated that the project will be extended in the future [152]. This is due to their ability and capability to evade SAMs [154] and radar detection systems, which are either designed to target a much larger aircraft or to intercept fixed-trajectory missiles [155].
- **Interception of Footage:** military analysts are capable of analyzing the footage taken and filmed by a terrorist's drone in an attempt to thwart a domestic terror attack [156]. This allows them to identify their tactics, operational geographical location, along with their skills, weapons, and training.
- **Underwater Surveillance:** underwater drones were used for covert underwater surveillance and reconnaissance operations, especially by the US Navy [157,158] near and across the China sea [159,160]; many sensors were caught by Chinese authorities, mainly between 2016 and 2018 [161–163]. Such operations includes various underwater drones types such as the Unmanned Underwater Vehicles (UUV), Amphibious Underwater Vehicles (AUV) and Underwater Maritime Vehicles (UMV) [164–166], which are also used as part of naval counter-mine warfare [167–169].
- **Targeted Assassination & Killing:** the adoption of this term came as part of the US approval of use of lethal force [170,171] as part of new rules of engagements [172] for counter-terrorism and counter-insurgency tasks/purposes [128,173,174] (i.e Afghanistan [175–177], Yemen [178], Iraq [179], Syria [180] and Libya [181]). Its adoption can be based on the use of drone strikes or explosive-laden drones. Kamikaze drones/UAVs or loitering munitions [182,183] might also be used for "Target Assassination" purposes, as part of the so called explosive-laden drones [184]. This specific concept was demonstrated by the Israeli K1-UAV [185], which can be adapted and used by intelligence and spying agencies, where Israel Aerospace Industries (IAI) [186] also unveiled their newest Loitering Munitions (LM) called IAI Harpi at the Singapore Airshow in 2016 [187] and the IAI Mini-Harpi in 2019 [188,189]. However, not far from now, on August 4th, 2018, a drone-led assassination attempt was foiled when two drones wrapped with explosives were used to assassinate the Venezuelan president; they were shot down by snipers injuring 8 soldiers and 1 civilian [190–192]. Targeted killing is executed via drone strikes by what is referred to as "Killer Drones" [193] such as the case of the Global Hawk [194,195], Predator and Reaper Drones [196,197], as well as the British "Protector RG Mk.1" UAV [198] for the elimination of key terrorist figures/targets [199–205]. However, the adoption of this method resulted into further civilian casualties [206], and the rise of new insurgencies [207,208].

After presenting the different purposes for the use of UAVs, we list the malicious usages of drones by terrorists and/or criminals to launch malicious attacks such as having drones perform some types of physical or even logical attacks. In general, UAV malicious use can be divided between criminal usage and terrorist usage as described below:

3.4. Criminal attackers

Such attacks include physical as well as logical attacks:

- **Physical Attacks:** the main threat is related to the issue of private property surveillance, where drones can be easily used to breach the physical privacy of people. This is a very serious issue whereby drones are able to break through the geo-boundaries [209]. According to BBC News [210], smuggling drugs, phones, and even blades to prisoners within highly secure prisons, were being carried out while avoiding ground detection. This is typically achieved via an octo-copter that is capable of lifting 20lbs [211]. Moreover, such attacks include crashing drones into certain people (accidentally or intentionally) or crashing them into people's properties, which may cause low to serious damages. Another threat is related to small quad-copters such as the DJI Phantom 3, which can reach an altitude of 1600ft (488 m) and a distance of 16,000ft (4800 m) [212]. This imposes a serious problem, especially with bird-related incidents, which can cause serious problems to airplanes engines.
- **Logical Attacks:** Logical attacks include, among others, the setup of a fake mobile Wi-Fi network or a rogue Access Point (AP) [213], which leads to the interception of smart-phones traffic by luring users to connect to a nearby "Open AP", typically titled as "Free Wi-Fi". Thus, an attacker can capture users sensitive information like passwords and credit cards credentials. This also includes hijacking other drones by connecting a raspberry-pi device into a drone and programming it to intercept and hijack other nearby drones [214,215]. This turns the malicious drone into a rogue AP for nearby devices and drones, and injecting malware into connected smartphones through the interception and redirection of users data traffic, or through phishing (malicious links, fake advertisement, or false update). In fact, various drone attacks including jamming and spoofing were mentioned and discussed in [216].

Finally, UAV sensor inputs may also be targeted and exploited by an attacker who would manipulate such parameters and trick the sensors.

3.5. Terrorist & insurgent attacks

After the proliferation of drones, serious threats and challenges emerged since these drones could be used by terrorists for malicious purposes [217]. Having drones in the wrong hands can lead to serious consequences [218]. Actually, drones are being used by insurgents and terrorists alike [219,220]; drones and UAVs were used by ISIS to drop bombs (i.e weaponized drones [221]) and to film propaganda videos (i.e training, battle tactics, simulated attacks, location/geography, reconnaissance etc.) [222,223] in conflict zones such as the targeting of Iraqi and Syrian military personnel [224–227]. Also, against the backdrop of its increasing use of attack drones in Iraq and Syria, ISIS has released an informative graphic detailing its attacks in February 2017 using a pro-ISIS channel known by "Ninawa Province", to show the footage taken prior to a terrorist attack [228].

This alarmed the whole world about the drones' serious safety and security threats, and their devastating effects on the moral of both military and civilian personnel. Typically, the use of drones by terrorists is associated with the following purposes:

- **Online Propaganda:** recently, terrorists have been using drones [227,229] to film their attacks, training and operations using in some cases drones with High Definition (HD) cameras in an effort to boost the moral of their jihadists and urge sympathisers and world-wide supporters to join them [218,230].
- **UAV-Surveillance:** is a new method used by terrorists to capture live footage (i.e images/videos) while planning an attack [229,231,232], or potential future attacks [203,233].
- **UAV-Aided Shelling:** is also a new terrorist choice to guide and adjust their (artillery/mortar) shelling against a given military/civilian target [234] (i.e ISIS/ISIL [116,235]).
- **UAV-Guided & UAV-led Attacks:** is a technique that was used between 2016 and late 2017 [234] to target military personnel, convoys and checkpoints or installations [221,236,237] using the Vehicle-Borne Improvised Explosive Devices (VBIED) [238]; in addition to the old car bomb style [239], or the dropping of homemade bombs (i.e bomblets, grenades, 20–40 mm, or modified shells) or leaflets [240]. Moreover, they can be used as loitering munition to target airports, military installations and oil refineries (i.e in Saudi Arabia and United Arab Emirates (UAE)) [241–245].
- **Loitering Munition:** the Samad UAV is a family of long-range UAVs built and used by the Iranian armed forces and handed over to Hezbullah in the Middle East, and extensively used by the Houthis in Yemen for reconnaissance purposes [246,247], and also as loitering munition to target Saudi Arabia and United Arab Emirates facilities (oil refineries, airports and military installations, i.e Abqaiq-Khurais attack [242]). It was named after the assassination of Saleh Al-Sammad in a drone strike by the United Arab Emirates in 2018 [248], and includes three models, Samad-1 (wingspan of 3.5 m, 500 Km range, surveillance), Samad-2 (UAV-X, wingspan of 4.5 m, 500 Km+ range, surveillance or explosive payload) and Samad-3 (wingspan of 4.5 m, 1500 Km range, explosive payload).
- **Drone Footage Interception:** military drones/UAVs were prone to stream/footage interception attempts, many of which were successful. One example is the case of Israeli drone footage being intercepted in 1997 [249] before applying further encryption [250]. Another case occurred during the Iraqi war with insurgents intercepting US predator drones using first, a $26-value software [251,252] and then, the SkyGrabber software [253].
- **Airstrike Disruption:** this technique was adopted by ISIS to disrupt airstrikes against them in Raqqa; they wait on their opponents to fly a drone, then ISIS operators would fly and target the airstrike calling team, tricking their opponents into thinking its a friendly drone hovering overhead. Such drones were of10 armed with 40-mm grenade-sized munitions and can hit their target with high accuracy [254].
- **Burning/Incendiary Kites:** these were used in March 2018 during the Palestinian protests on the Palestinian-Israeli borders, and included the use of helium balloons, or strapping a kite, or an aerial unmanned device with a bomb, incendiary device, or Molotov cocktail and crashing it on the Israeli side causing a huge wildfire to nearby farmlands [255–258].

In summary, the use of drones/UAVs can be be applied into different domains. As described above, the threat of Drones/UAVs is highly alarming and taking place at an increasing rate especially as the year 2020 is unfolding, with the increasing terrorist and criminal use of drones/UAVs to conduct malicious activities. As stated in this section, drones have been employed in different domains for good purposes, but also for malicious ones. Accordingly, there are new challenges related to several security, safety and privacy concerns when drones/UAVs are employed for malicious goals, which we discuss in the next section.

4. Drones security, safety and privacy concerns

The use of drones offered advantages on so many levels, from commercial to personal. However, drone systems suffer from different security, safety, and privacy issues [259].The breaches of security and privacy led by drones should be addressed by the highest national level. Moreover, there should exist a very strict approach to limit the drones' ability to gather images and record videos of people and properties without authorized permission. From the perspective of security and threat analysis, drone-assisted public safety network is different from traditional wireless networks such as Wireless Sensor Networks (WSNs) and Mobile Ad-hoc Networks (MANETs) [260]. This is attributed to carrying less information and requiring less power compared to a drone-assisted public safety network. Moreover, the drone's coverage area is broader and wider than WSNs and MANETs. Therefore, security challenges are primary related to the resources constraints along with

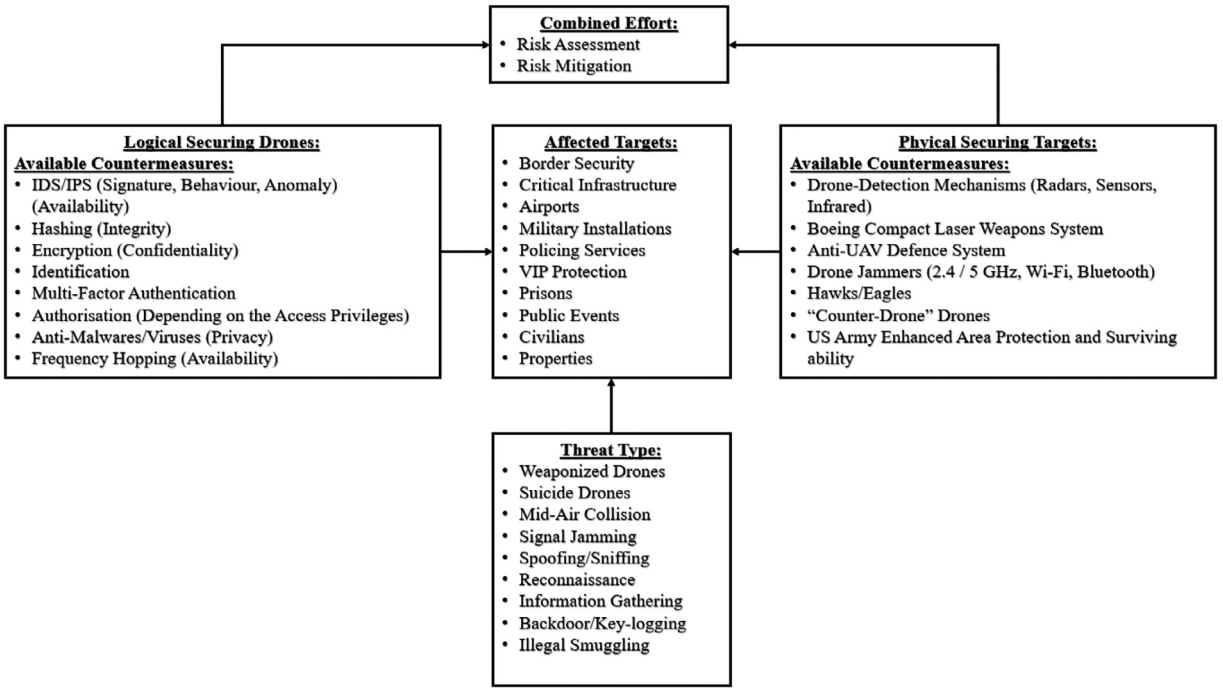


Fig. 4. Drone threats taxonomy

the delay constraints of UAVs. Moreover, it is essential to ensure that confidentiality, integrity, availability, authentication, and non-repudiation properties over communication channels are fulfilled. This is done in accordance to the AAA process and guidelines:

- **Authorisation:** by assigning privileges to the personnel controlling the UAV.
- **Authentication:** by ensuring a multi-factor authentication using something you know (strong constantly changing password), something you have (username), something you are (biometric) properties.
- **Auditing/Accounting:** by tracking down and/or arresting drone/UAV legitimate owners in case of criminal/malicious activities.

The use of drones, by malicious entities to conduct physical and cyber-attacks, threatens the society by breaching the privacy of its residents along with threatening the public's safety. In fact, various technical and operational drone properties are being exploited and misused for potential attacks. This includes performing critical operations based on offensive reconnaissance, as well as surveillance aimed at tracking specific people and certain properties, causing safety and privacy issues [261].

On the other hand, it is essential to prevent the use of drones above residential areas, which leads to privacy breaches through reckless behaviours, since the captured footage may be used for either scamming and/or blackmailing purposes. Safety breaches may also occur in case a drone malfunctions and crashes into a nearby house, park, parked car or civilians. This would result into material loss/damage and humans casualties/fatalities.

Moreover, drones are predominantly used to target guest Wi-Fi connections and/or short-range Wi-Fi, Bluetooth and other wireless devices, such as Bluetooth-connected keyboards. Such connections are not protected due to current security measures, which assume that no one could get close enough to compromise them or to access internal networks via wireless signals. These assumptions lead to weak single factor authentication and the use of typical passwords that can be easily cracked, especially with the absence of encrypted connection. This makes it as easy to intercept information in a private building and in a public café [262].

An attacker would leverage such vulnerabilities to breach security, safety and/or privacy.

Fig. 4, lists the main drones security threats as well as the corresponding techniques to overcome them.

Next, we summarize the current and future security challenges.

4.1. Security concerns

The drones characteristics (small size, low cost, and ease of manoeuvrability and maintenance) made them a preferred choice for criminals. Also, terrorists started to divert their attention towards using these drones to carry out terrorist attacks [263], mainly due to the nature of drones that makes them less prone to detection.

In fact, drones can be armed and modified to carry deadly chemicals, or be fit with explosives to attack critical infrastructures. Moreover, drones carrying explosives may be detonated around people gathering in a hard to reach places. This makes the task easier for a terrorist to achieve, especially since drones provide the stealth of a suicide bomber with the range of an aircraft [232]. Military analysts are concerned about drones being used against the US for espionage purposes. This is due to ISIS being able to re-arm commercially available drones, and make them fit for combat roles over Iraq and Syria.

4.2. Safety concerns

Security does not always mean safety, and vice versa. Outside the military domain, civilian drones/UAVs [264] can also malfunction and crash into a nearby house or a group of people, causing property/material damage [80], and human injuries/fatalities [265], ranging from trauma/blunt force trauma, deep cut injuries (caused by drone blades) and laceration. On August 9th, 2016, a young woman lost her life in a car crash in the first non-military related drone incident after reports of a drone being flown near Wandsworth Prison in London. On November 2016, an 18-month old toddler from Stourport-on-Severn, Worcester UK, sliced his eyeball in half by the propeller of an out-of-control drone. In April 2016, a British Airways passenger jet, flight BA727 was hit by a drone before landing at Heathrow Airport. However, no injuries were reported and all 132 passengers and five crew members were safe. As a result of these incidents, we list below the main safety concerns:

- **Lack of Safety Feature By Design:** which could result into drones going out of control and flying aimlessly and autonomously without having the ability to shut it down or to re-gain control [266].
- **Lack of Technological & Operational Standards:** especially as related to the crash avoidance mechanisms, which would result into the UAV's inability to recognise and identify aircraft and airborne objects and avoid them [267].
- **Signal Distortion-Jamming:** this makes a UAV prone to hacking, hijacking and GPS/Sginal-jamming as part of cyber-terrorism or cyber-criminal activity, mainly due to the UAV's command-and-control operation center being prone to exploitation.
- **Lack of Governments Regulation & Awareness:** especially in terms of safety practices and features to ensure safe UAs integration into the national airspace domain [268].

4.3. Privacy concerns

People's privacy is also at high risk of being exposed by unwanted flying guests that can record their movement and capture images at anytime, without their knowledge or permission. This is an indication of how much our privacy is vulnerable to such an emerging threat.

According to the Canadian Public Safety, UAV technologies raised a broad range of issues that relate to the collection of images and videos [269]. This was associated with blackmailing and scamming by threatening the disclosure of personal images or videos captured without the victims knowledge from an aerial position. In general, the privacy threats can be divided into three main categories.

- **Physical Privacy:** is based on flying drones over someone's property or at their window level. This allows attackers to covertly gather images and record videos of certain people in possibly inappropriate ways, threatening their personal freedom.
- **Location Privacy:** is based on tracking and detecting people with a drone flying and buzzing above them without them knowing that they are under surveillance [270].
- **Behaviour Privacy:** is where the presence of a flying drone can affect the way people act and react [271], especially when knowing that they are under surveillance. As a consequence, this would also limit their liberty, breach their privacy, and restrict their freedom.

Security, safety and privacy are key requirements for the adoption of any new IoT technology, especially drones and UAVs [272,273]. In this section, we review the main privacy, safety and security concerns that can be imposed by security breaches. These key concerns must be addressed to as soon as possible, otherwise their illegal use will remain on a constant rise, especially with the absence of firm laws, legal restrictions and sanctions. In the next section, we present the main security vulnerabilities and threats that can be exploited in order to compromise the drones security.

5. Drones existing threats & vulnerabilities

UAVs and drones are being perceived as viable and vital threats to information security. Many UAVs have serious design flaws, and most of them are designed without wireless security protection and footage encryption [274].

- **Prone to Spoofing:** analysis of the configuration and flight controllers of UAV models, with multiple rotors, revealed many weaknesses. These are associated with both the telemetry links streaming data to/from a drone via serial port connections, especially due to its weak communication nature, which is in most cases not encrypted [275,276]. The experiments done in [277,278] showed that, through GPS spoofing, the information can be easily captured, modified, or injected. This vulnerability in the data link enables the interception and spoofing, giving hackers complete control of the drone.

- **Prone to Malware Infection:** the communication protocols are enabled within the UAVs to allow users to pilot drones via wireless remote control such as tablets, laptops and mobile phones. However, this technique was found to be insecure [279,280]; it allows hackers to create a reverse-shell TCP payload, injects it into the drone's memory, which will covertly install malware on the systems running the ground stations.
- **Prone to Data Interference & Interception:** telemetry feeds are used to monitor the vehicles and facilitate information transfer through open non-secure wireless transmission [281], making them vulnerable to various threats. These include data interception, malicious data injection, and alteration of pre-set flight paths. This allows the installation and insertion of many infected digital files (videos, images) from the drone to the ground station [282]. Another vulnerability was revealed in [4], and related to the UAV's communication module, which uses wireless communication to exchange both data and commands with the ground station [283].
- **Prone to Manipulation:** since drones fly pre-programmed and pre-defined routes, manipulation can occur and could potentially have serious consequences [284]. This ranges from stealing high-value cargo, to redirecting UAVs to deliver explosives, biological weapons, or other terrorist payloads, through RF or GPS spoofing, which allows the attacker to gain control over the drone by sending counterfeit signals, or jamming it with the purpose of crashing it.
- **Prone to Technical Issues:** many drones suffer from various technical failures [285]. This includes application errors such as connection failure between a user's device and the drone, causing it to either crash or fly away. Other issues are related to the lack of stable connection, especially under challenging natural causes [286]; the battery life, which results in a very limited flight time before being fit to fly again. Note that in cold weathers, the batteries' life span is reduced, leading to a shorter flying time, as well as possible malfunctioning [287,288].
- **Prone to Operational Issues:** another major issue is the lack of flying skills by drone owners and the type of drones in use [289]. This can cause serious damage and/or injuries against properties and/or personnel [290]. In fact, drones are sensitively made, so a small accident could bring the drone down. In many cases, if one of the rotaries dysfunctions or stops working, it would cause a serious turbulence with a hard to maintain control of the drone [266]. This, in most cases, would lead to the crashing of the drone. For example, [291] mentioned an incident of an Israeli drone, which broke into the Lebanese airspace and crashed in the south of Lebanon due to technical and operational failure.
- **Prone To Natural Issues:** in many cases, drones cannot withstand wind due to their lightweight nature. Moreover, extreme heat conditions can lead to engine failure, bringing the drone down. Also, the battery could explode and cause serious damage and harm. Another issue is the inability of drones to fly through rain since they are not equipped with waterproof protection [292,293]. Usually, when drones crash into lakes, rivers, beaches or even pools, they immediately stop working. Furthermore, during fog, owners are not advised to fly drones due to the limited visibility, which shrinks from few meters to less than a meter leading to the disruption of communications between the drone and the GPS, sending the drone outside its control area till it crashes.
- **Prone to Wi-Fi Jamming:** drones can also be hijacked by sending a de-authentication process between the access point and the device controlling the drone, which can be done temporarily or permanently, such as jamming the intended drone frequency, and luring it to connect to the hacker's Wi-Fi; this can be done by installing and configuring a raspberry-pi for such a job [215].

6. Drones existing cyber-Countermeasures

The main countermeasures that can be adopted to safeguard drones against security attacks can be classified into the following types based on an attacker's main motives, objectives and goals. In the following, the existing solutions to secure drones' networks, communications, and data are discussed. Moreover, the existing forensics solutions, used during the investigations of drone attacks, and aiming to identify the root causes of such attacks, are listed and described.

6.1. Securing drones/UAVs networks

Drone networks suffer from several security threats and issues. Recently, Intrusion Detection Systems (IDSes) have been deployed to detect UAVs/drones' malicious activities and to detect suspicious attacks that may target them. Typically, an IDS monitors incoming and outgoing network traffic, and analyzes them to detect anomalies. Their aim is to detect and identify cyber-attacks by examining data audits (trails) that were collected at different network parts. In the following, we present the various IDS approaches to protect drone networks against intruders.

- **Rule-Based Intrusion Detection** Rule-based intrusion detection systems are being used in the UAV domain. In [294], Strohmeier et al. developed a rule-based intrusion detection scheme to protect the communication between an aircraft and the ground station. The goal is to detect false data injection attacks, especially those targeting the signal strength. They proved that attackers can be detected within 40 seconds. In [295], Mitchell and Chen presented a specification-based detection technique to guard a UAV system against various types of cyber-attacks. The authors relied on a behaviour rule-based UAV-IDS. The behaviour rules were constructed based on defined attack models, including reckless, random, and opportunistic attacks. This allowed the minimization of detection errors including false positive and false negative rates, with a critical trade-off between UAVs' security and performance. In [296], Mitchell et al. presented BRUIDS, an adaptive behaviour-rule specification-based IDS, which detects malicious UAVs in airborne systems. The authors also investigated the effectiveness of BRUIDS on reckless, random, and opportunistic attacker behaviours to quickly

assess the UAV's survivability against malicious attacks. The simulation results showed that BRUIDS achieves a higher detection rate compared to the multi-trust anomaly-based IDS approach, and with a lower false positive rate. However, rule-based IDSes suffer from their complexity management, which requires human intervention for rules configuration. In addition, this type of IDS is incapable of detecting unknown attacks.

- **Signature-Based Intrusion Detection** In [297], Kacem et al. presented an ADS-B intrusion detection framework to secure an aircraft against cyber-attacks that target ADS-B messages. Such a framework is based on signature detection techniques that analyze the GPS position of an aircraft. In [298], Casals et al. developed a bio-inspired detection scheme to detect cyber-attacks that target airborne networks. However, similarly to a rule-based IDS, a signature based IDS cannot detect unknown attacks or attacks with dynamic signatures.
- **Anomaly-Based Detection** An anomaly-based detection IDS, in the UAV domain, is mainly used to prevent jamming attacks. In [299], Rani et al. presented an anomaly-based learning algorithm to protect UAV nodes against DoS and DDoS attacks. In [300], Lu et al. presented a reinforcement learning-based motor-temperature anomaly detection system for UAVs, which prevents drone's motors from operating at abnormal temperatures, using DS18B20 sensors for temperature recording and a raspberry-pi CPU for processing. This system offers the ability to avoid motor failure by landing the drone in case of overheating; however, it does not fully prevent the issue. Experimental results reveal the ability to safely control the drone based on the sensors' information. In [301], Condomines et al. presented a hybrid IDS based on spectral traffic analysis and a robust controller for anomaly estimation within UAV networks in a Flying Adhoc Network (FANET). This technique was targeting Distributed DoS attacks, and its effectiveness was tested on real-time traffic. The results showed an accurate detection of different anomaly types. However, further testing is still required to ensure its effectiveness.

  In [302], Sedjelmaci et al. presented an Intrusion Detection and Response Framework (IDRF) to secure a UAV network against data integrity and network availability attacks, and to secure a UAV-aided VANET against malicious threats [303]. The authors indicated that the proposed framework is unique as a hybrid detection technique for UAV networks [6]. In [304], Lauf et al. presented a decentralized anomaly-based detection technique using maxima and cross-correlation detection methods. In fact, Maxima Detection Systems (MDSs) ensure the characterization of either one or zero suspicious nodes, while Cross-Correlation Detection (CCD) methods detect multiple intrusions. However, their approach suffers from inaccuracies in relation to the false positive and false negative rates. Also, in [302], Sedjelmaci et al. presented a hierarchical intrusion detection and response scheme to enhance the security of UAV networks against devastating cyber-attacks such as false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks. This scheme operates at the UAV and ground station levels to detect malicious network anomalies. Simulation results revealed a high detection rate of 93.3%, and a low false positive rate of less than 3%, with a low communication overhead. In [305], Mitchell et al. presented a specification-based IDS to secure sensors and actuators embedded in a UAS. To assess the effectiveness of their solution, the IDS was tested on UAVs to investigate the impact of an attacker's behaviour. The results indicated that the solution effectively trades off the false positive rate for a high detection probability, to offer better security for UAS applications.

  Given that drone networks' gateways might be operating with some constraints (fog nodes), there is a need for a lightweight host-based anomaly detection technique that requires micivinimal computational resources. This can be achieved by using a simple machine learning technique or a statistical approach with minimum possible number of features. The structure of a resilient IDS should be based on a hybrid approach, where rule-based or signature-based approaches are used for known attacks and the anomaly-based approach for the detection of abnormal behavior. Such a system would depend on machine learning and human security experts.

6.2. Securing drones/UAV communications

Due to the increase in the number of drone/UAV footage interception, different solutions were presented to secure UAV communication. In [306], Zhang et al. addressed the issue of physical-layer security in UAV communication systems and presented an iterative algorithm based on the block coordinate descent and successive convex optimization methods. The simulation results showed a significant improvement in terms of the secrecy rate of UAV communication systems. In [307], Zhang et al. applied these algorithms to tackle the issues of broadcast, line-of-sight, and air-to-ground wireless channels challenges surrounding the Fifth Generation (5G) wireless networks. The simulation results revealed an improvement of secrecy rates for UAV-to-Ground (U2G) and Ground-to-UAV (G2U) communications. In [308], Cui et al. also addressed the broadcast nature of air-to-ground line-of-sight wireless channels challenges and tackled it based on the physical layer by leveraging the trajectory design of UAVs mobility. The authors presented an iterative sub-optimal algorithm by applying the block coordinate descent method, S-procedure, and successive convex optimization method. Simulation results revealed a significant improvement in their average worst-case secrecy rate.

In [309], Zhao et al. presented a caching UAV assisted secure transmission scheme in hyper-dense Small-cell Base Stations (SBSs) based on Interference Alignment to offload traffic via wireless backhaul and to improve the coverage and rate by generating jamming signals to disrupt any potential eavesdropping attempt. The simulation results revealed the effectiveness of their methods. In [310], Lee et al. investigated the UAV-aided secure communications with a cooperative jamming UAV, and presented an iterative algorithm which provides an efficient solution for the minimum secrecy rate maximization problem by jointly optimizing the transmit power, the UAVs trajectory and the user scheduling variables. Numerical results indicated

that the algorithm outperforms the baseline methods. In [311], Liu et al. examined the security issue in UAV-aided communication systems and presented a secure transmission scheme for a UAV wiretap channel using a multi-antenna source that transmits to a UAV's single-antenna, in the presence of a full-duplex active eavesdropper. The Multi-antenna source transmits artificial noise signals together with information signals to hinder the full-duplex eavesdropper ability to eavesdrop and jam.

In [312], Cai et al. investigated the joint optimization of UAV trajectories and user scheduling for a dual-UAV enabled secure communication system and presented a novel P-CCCP based algorithm for this purpose. The algorithm was further extended to cover the case of multiple jamming UAVs to further improve the secrecy rate. Simulation results revealed a better performance than other conventional UAV-aided algorithms. In [313], Li et al. studied secure communication with imperfect channel estimation, in the case of a smart UAV attacker under different modes (i.e keeping silent, eavesdropping, jamming, and spoofing). As a result, a non-cooperative game theory technique was used to present a Q-learning based power control algorithm, using a Nash Equilibrium (NE) strategy, to obtain an adaptive policy for the transmitter. Simulation results showed an effective decrease in the UAV attack rate and an increase in the system secrecy capacity.

In addition to modulation techniques, it is essential to encrypt the communications of drones and UAVs. In this context, different cryptographic solutions were recently presented, including message encryption and authentication. Since most drone standards have to ensure secure communication, the focus became on how to design a lightweight message authentication-encryption algorithm. Also, this can be done in a way to preserve the source authentication in addition to integrity and confidentiality of the transmitted data. The existing cryptographic algorithms to secure drone communications were discussed in [314,315]. These algorithms can possibly be applied to secure the communications of drones used for civilian applications. Moreover, a secure communication protocol (eCLSC-TKEM) between drones and smart objects was presented by Won et al. in [316]. The authors claimed that their system is 1.3, 1.5 and 2.8 times better than other protocols including the protocols in Seo's CLSC-TKEM [317], Sun's CL-AKA [318], and Yang's CL-AKA [319].

Additionally, in [320], Sharma et al. presented a highly secured Functional Encryption (FE) technique to secure a UAV assisted Heterogeneous Network (HetNet) in dense urban areas against malicious activities, and also to secure by encryption users' critical data; however, this solution requires further enhancements.

On the other hand, in [321], Chen et al. presented a Traceable and Privacy-Preserving Authentication (TPPA) scheme for UAV communication control systems. TPPA integrates Elliptic Curve Cryptography (ECC), digital signature, hashing, and other cryptography mechanisms for UAV applications. This ensures privacy, confidentiality, integrity, availability, anonymity, and non-repudiation, especially against DoS and spoofing attacks, with low computational and communication costs.

Operating over long distances on battery enabled devices, the security of drone communications requires lightweight cryptographic algorithms and protocols. Recently, new cryptographic algorithms with one round functions or few number of iterations were presented in [322]. Moreover, existing privacy-preserving authentication protocols can leverage such lightweight cryptographic algorithms for a minimal delay. Also, physical layer parameters can be used for multi-factor authentication.

6.3. Securing drones data

All the data captured by drones must be aggregated to minimize the traffic being continuously sent to the base station. However, aggregation of encrypted data imposes new challenges. Accordingly, in [4], He et al. presented a Homomorphic Encryption (HE) method, and a practical data aggregation scheme based on the additive HE presented in [323]. Unfortunately, existing HE solutions suffer from security and/or performance issues. Symmetric ciphers suffer from security issues, especially in terms of chosen plaintext/ciphertext attacks, while asymmetric ciphers suffer from high computational and resources overhead, in addition to the associated storage overhead.

6.4. Forensic solutions

Digital forensics techniques are being extensively used in the UAV/drone domain. In [324], Pilli et al. presented a generic framework for Network Forensics (NF) which involves the analysis of network data traveling through firewalls or intrusion detection systems. This allows a network-based investigation to detect and identify anomalies in the traffic. The goal of such a model is to trace back the source of the attack using a six-phased chain-of-custody. Another framework was presented in [325], and it uses a Digital Investigation Process (DIP) to promote a comprehensive multi-tier hierarchical digital investigation model. This framework includes two tiers:

1. **First-Tier:** involves *assessment and incident response phase,data collection and analysis phase*, and *presenting findings and incident closure phase*.
2. **Second-Tier:** includes an object-based sub-phase [326].

In [327], Bouafif et al. highlighted various drone forensics challenges and presented the results of their digital forensic analysis performed on a Parrot AR drone 2.0. The analysis included the ability to access the media file system from File Transfer Protocol (FTP) or serial connections to retrieve all required information by digital forensic investigators, including the controller's Android ID used to establish ownership. In [328], Barton et al. reported the extraction and interpretation of important artefacts found in the UAV's internal memory and the controlling application, and the analysis of digital media,

logs and files that identify the artefacts. Experiments were conducted on a DJI Phantom 3 Professional drone, and the results showed a successful number of data retrieval methods, and the finding of important useful artefacts using open source tools. In [329], Barton et al. covered the use of open source forensics tools and developed basic scripts that aid the forensics analysis of the DJI Phantom 3 Professional and AR Drone 2 in a polymathic workstyle, by aiming to reconstruct the actions that were taken by these drones, identifying the drones' operators, and extracting data from their associated mobile devices. This can be done by analyzing flight logs and identifying artefacts and capturing the drones' digital media.

In [330], Clark et al. presented an open source forensics tool, DRone Open source Parser (DROP), which parses proprietary data files extracted from the DJI Phantom III nonvolatile internal storage, and text files located on the mobile device controlling the drone. Results revealed that it is possible to identify GPS locations, battery, and flight time, along the ability to link a given drone to its controlling mobile device based on its serial number. Further results revealed that data can be forensically acquired by manually extracting the drone's Secure Digital (SD) card. In [331], Mantas et al. investigated the mostly used forensics platforms such as Ardupilot, the dataflash and telemetry logs, before presenting their own open source forensics tool, Gryphon, which focuses on the drone's flight data logs from the perspective of the ground control station, collects, examines and analyzes the forensic artefacts to construct the corresponding timeline of events so perpetrators can be brought to justice.

In [326], Jain et al. presented an event-based digital forensic investigation framework, as a result of an investigation process based on a physical crime scene [332]. this framework aids the hypothesis's testing and development through an event reconstruction based on the collected evidences following **the readiness and deployment phase, physical crime scene investigation phase, digital crime scene investigation phase**, and **presentation phase**.

Moreover, a UAV forensic investigation process was presented in [333], followed a step-by-step process based on three main initial phases.

- **Preparation Phase:** this is to identify the chain of command since the UAV will be the first equipment to be seized once crashed [333]. It allows a conventional forensic practice to be carried out to identify any DNA or fingerprints on the drone/UAV. Thus, a piece of digital evidence could be combined with traditional evidence such as witness statements. Then, an "offence analysis" [333] is carried out to identify the device in use, to determine the current date and time, and to identify the current UAV operator by tracking their address and seizing their device.
- **Examination Phase:** it is based on the identification of the drone's video/audio recording and image capturing capabilities [333]. This is done by identifying the data storage locations such as removable, fixed and flash memory cards, as well as identifying open communication ports for further traffic interception. This requires non-destructive methods, to protect the original data, using commercial or non-commercial forensic tools [334], or using a destructive extraction method.
- **Reporting and Analysis Phase:** it is based on an initial review of the extracted data since the first stored images are the suspect's own images including initial take off/landing spot, available personnel, surrounding location, area coordinates, etc. Thus, it is important to know how the recording function works to intercept the data and translate it into a human readable form.

Furthermore, a well-fit forensic model called "waterfall model" was presented in [326], in response to the significant differences among commercial models. This model includes multiple phases to allow a digital investigator to recheck all previous phases during an investigation process, including the **preparation and identification phase,weight measurement and customization check phase** [335], **fingerprints phase, memory card phase** [336], **geo-location phase** [336–338], and **Wi-Fi & Bluetooth phase** [339].

However, recently several anti-forensics techniques have been developed to prevent investigators from finding and/or collecting evidence, which necessitates the development of efficient countermeasures to recover valid evidence. Such anti-anti-forensics solutions should be designed in a way to preserve the main functionalities of drone systems while resisting anti-forensics methods.

In summary, this section reviewed the existing security solutions for securing drone systems, including cryptographic and non cryptographic solutions. The cryptographic solutions aim essentially at securing the drones communication and the communicated data, while the non-cryptographic solutions (IDS) aim at detecting and recovering from possible security attacks.

7. Anti-Drones counter-Measures

Since the number of incidents between drones and airplanes increased from 6 to 93 in 3 years (2014 to 2017) [340], it has become essential to address the security and privacy breaches at the highest national level. This includes adopting very strict approaches that limit the drone's ability to gather images and record videos of people and properties without a clearly authorized permission. In fact, since many people do not read the manual properly, they are incapable of reacting properly in case of a malfunction. In the UK, for example, if a drone weights more than 250 g, its users are supposed to take safety awareness tests and the police is given the authority to stop any drone when suspected of a criminal activity [341]. Also, the British government announced new rules to ban drones from flying within one kilometer of British airports to prevent any possible collisions with airplanes [342].

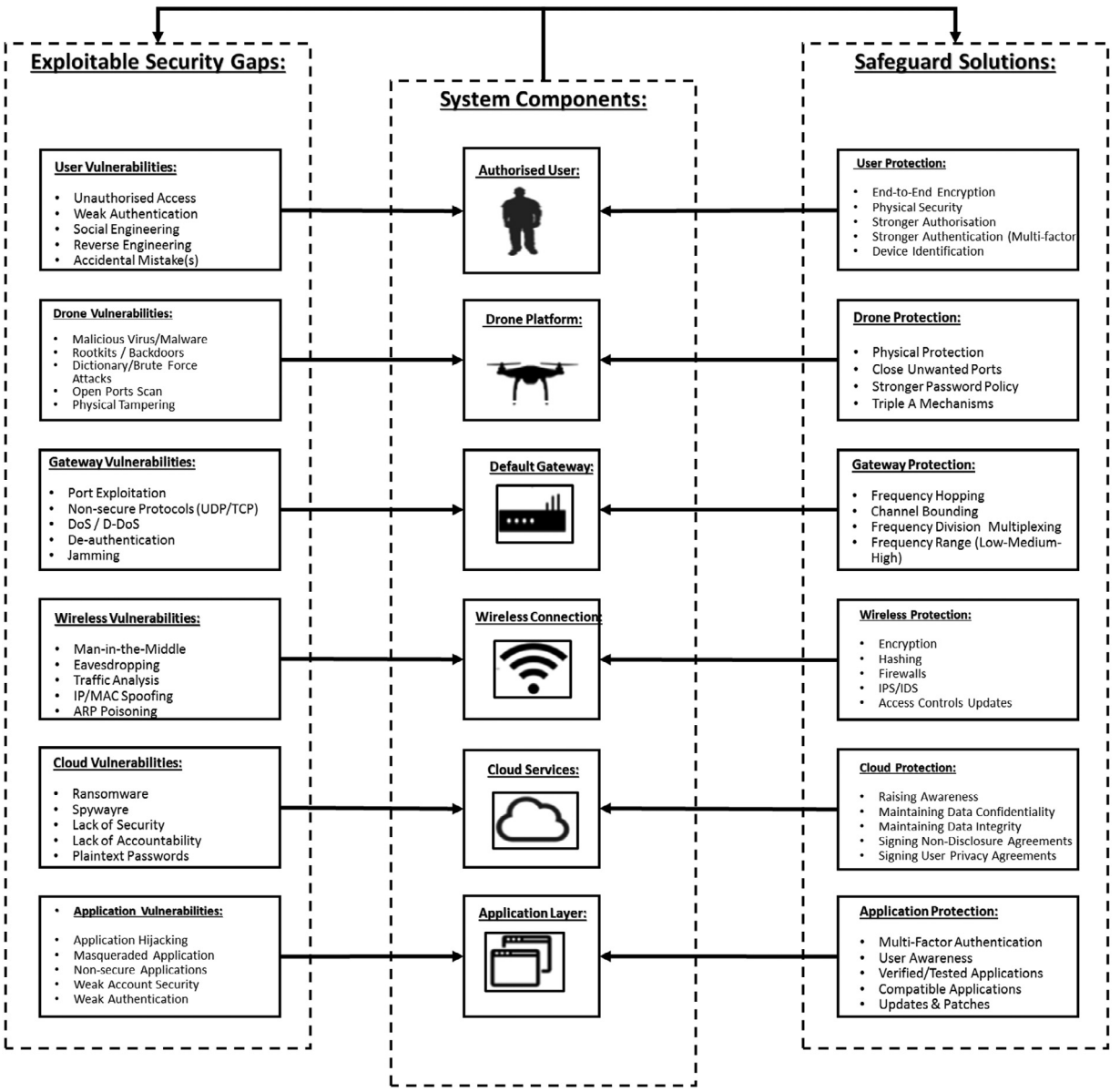


Fig. 5. Possible drone attacks and the corresponding countermeasures

In Fig. 5, we present a framework to secure the various components of a UAV system. There are different techniques to hack and/or hijack a drone, either using traditional techniques (discussed below) or using a new form called "hack and crack". On the other hand, due to the recent extensive use of armed drones in deadly conflicts such as in Yemen [246,343,344], Iraq and Syria by the different fighting factions [134,345,346], the adoption of non-lethal solutions to counter these threats is highly ineffective and unreliable. As such, the countermeasures are divided into civilian, government, and military countermeasures (see Fig. 6).

7.1. Civilian countermeasures

Civilian countermeasures are divided between physical and logical countermeasures.

7.1.1. Physical countermeasures

When drones became widely popular, many organizations spent time and resources searching for ways to prevent their use in restricted airspace and above their buildings. This issue emerged after a drone crashed last year in front of the White House.

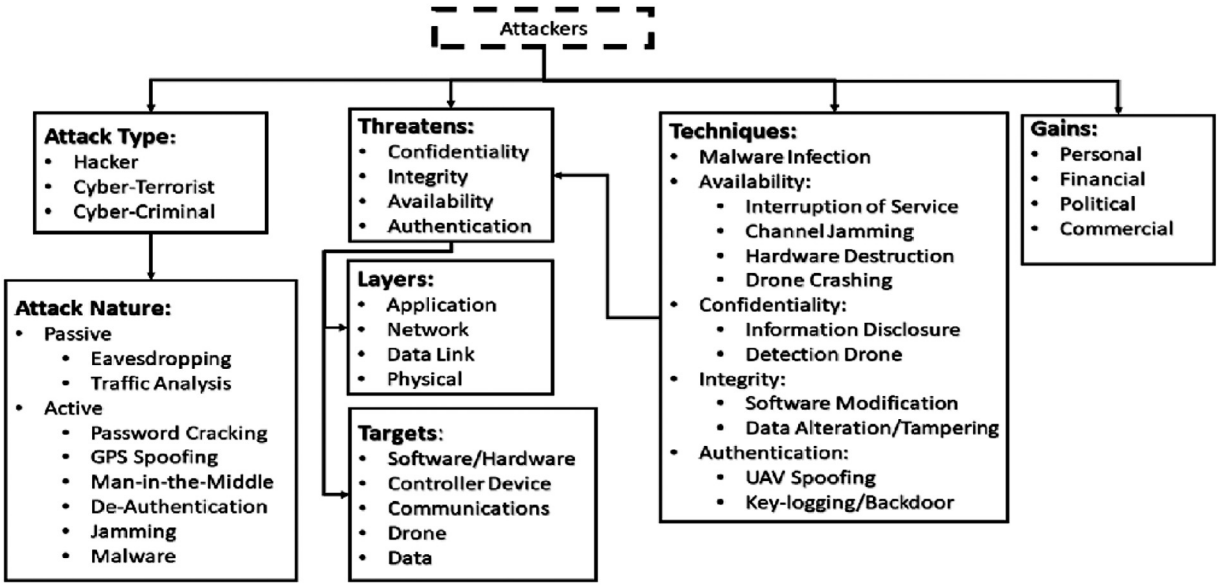


Fig. 6. Drones targets and impacts

- **Drone Catchers:** the Tokyo police and Michigan Tech University developed **drone catchers**, large drones equipped with nets, such as the "robotic falcon" [347].
- **Drone Defenders:** the US Company, Battelle, developed the **drone-defender (Dedrone)**, which is used to drop drones from the sky using radio waves.
- **Low Tech Methods:** low-tech methods were used by the police in Netherlands; these include training an **eagle** or a **hawk** to catch the drones with their talons [262]. However, such methods can cause serious harm to animals, especially in the case of large drones with very sharp rotaries.
- **Electrical Fence:** in October 2017, China was the only country to establish an electric fence connected to a UAS cloud to detect and prevent a UAS from entering prohibited areas, especially those beyond VLOS [348].

7.1.2. Logical countermeasures

These measures include the use of logical equipment rather than expensive physical equipment. For example, in [349], Hooper et al. conducted pen testing on a Parrot Bebop UAV and revealed how Wi-Fi-based Parrot UAVs are prone to zero-day vulnerabilities and different attacks such as Address Resolution Protocol (ARP) and Cache Poisoning attacks. Hence, the authors presented a Multi-layer security framework as a defence-in-depth mechanism to guard UAVs against zero-day vulnerabilities. In [350], Birnbaum et al. presented a prototype UAV monitoring system that captures flight data and performs real-time estimation and tracking of the airframe and controller parameters by comparing them to previously known parameters. This was done using the Recursive Least Squares Method (RLSM) that detects cyber-attacks and incipient hardware degradation and failures. Experimental results revealed that it is possible to automatically establish UAV flight parameters while achieving an efficient anomaly detection in flight to detect significant deviations. In [351], Abbaspour et al. presented a new active Fault Tolerant Control (FTC) UAV system design, using a neural network adaptive structure for Fault Detection and Isolation (FDI). This scheme ensures real-time detection and isolation of faults in the actuators without the need to reconfigure the controller or affecting its performance. However, other security solutions were presented to counter-UAVs, as presented next.

- **Wi-Fi Jamming:** This is the first method to apply when drones are using the frequency of 2.4 GHz. This jams all wireless communications within a specified coverage area [6]. However, the jamming ability is very limited and cannot be hidden for it can be easily detected and it jams other nearby frequencies.
- **Three-Way Handshake:** This process is based on a handshake between the router's AP and the newly integrated rogue device. It allows the attacker to de-authenticate or even jam the communication between the drone and the device controlling it. Moreover, such a handshake can be used in order to launch a password cracking attack, especially if the drone is secure.
- **Wi-Fi Aircrack:** In [4], a Wi-Fi attack (SkyJet) was presented; it enables an attacker to search for drones in its vicinity and hijack them, turning them into "zombie drones". SkyJet uses aircrack-ng to detect nearby wireless networks and clients before deactivating the drone's controller. This task is done while connecting the attacker to the drone, allowing full control over the victim's drone. This type of attacks is based on three main phases, as presented in [4].

  - *First Module:* a wireless sniffing tool, such as the "airodump", which aims at discovering WEP-enabled and WPA-2 enabled networks, as well as open networks.
  - *Second Module:* an injection tool, such as "airplay", used to increase the traffic.
  - *Third Module:* the "aircrack-ng", which allows the attacker to lead a de-authentication attack. Such an attack can disrupt a Wi-Fi connection protected by WPA2 encryption according to [4].
- **Replay:** this is a DoS-like attack, which intercepts the transmitted data and then, either delays it, or re-transmits it at a later time [4,352]. In fact, replaying the Address Resolution Protocol (ARP) request can also be used in an attempt to crack the encryption keys, especially if the connection between the drone and device is secure.
- **Buffer Overflow:** this is a DoS-like attack, which intercepts the network traffic and floods it with constant requests to disrupt the drone/device connection. This attack occurs when a JSON script makes a request to become the controller, from an attacking computer, to capture network traffic via Wireshark [8], in addition to embedded statistics from the /proc/stats directory. This is further explained in [352–354], with an example on how a DJI phantom 3 drone was exploited in [355].
- **Denial of Service (DoS):** this is performed either through de-authentication or Wi-Fi jamming using "Kali-Linux" as a platform to cause the UAV to crash [8]. The de-authentication process can be sent periodically or permanently using 1) the "airodump-ng" command to assess the drone's network security, 2) the "Aireplay-ng" command to disconnect any connected device, or 3) the "aircrack-ng" command to break any secure drone/device connection [356,357]. As for Wi-Fi jamming, Websploit Wi-Fi jammer can be used once the Extended Service Set Identifier (ESSID) of the device (MAC address of the drone's AP), and the Basic Service Set Identifier (BSSID) (channel number of drone/device communication) are known [216,358,359].
- **ARP Cache Poison:** this is a man-in-the-middle attack type and is launched to interrupt, halt or change the network traffic. To perform this attack, a computer is used to continuously execute a malicious script called "Scapy" via Python library until the drone disconnects from the connected device [360,361].
- **Injection and Modification:** also known as integrity attacks [302]. Such attacks are based on altering sensitive information of a legitimate aerial vehicle by injecting wrong data [5]. This allows the modification of content and possibly uploading infected data to ensure a backdoor to the ground-control system.
- **Fabrication:** this attack targets the drone's authenticity. It allows gaining access privilege into the aerial vehicle components to provide false information [6].
- **Civilian GPS Spoofing:** it is highly important to ensure that the GPS data is legitimate, otherwise, this leads to false estimation of the device's position. This could lead to mission failure and possibly loss of assets such as the recently claimed theft of a US RQ-170 Sentinel by Iranian forces [362]. Using Universal Software Radio Peripheral (USRP) [363], a GPS signal simulator was implemented to launch GPS spoofing attacks, which were deemed to be very effective in the Ukrainian conflict [143]. This was done by attaching a power amplifier and an antenna to a GPS signal simulator, while radiating the RF signal towards the target receiver. Then, simultaneously repeated periodic signals were sent, which led to the possibility of receivers being in tracking mode and prone to spoofing attacks [362]. As a result, the biggest challenge remains as how to encrypt civilian GPS since it is very costly and it requires complex hardware and software.
  In [7], the University of Texas managed to hijack a Hornet Mini-rotorcraft UAV by launching a GPS Spoofing attack, and exploiting the vulnerability of the drone that depends on civil GPS for navigation. The spoofer transmitted first weak counterfeit GPS signals towards the hovering UAV, and then, rapidly increased the counterfeit signal power, bringing the UAV under their control. This was done by simply inducing a false upward drift in the UAV's perceived location, fooling the UAV's flight controller into commanding a dive. Moreover, Humphreys [8] stated that a spoofer strategy requires predicted data navigation from the coupled receiver or an external source to produce fake GPS signals that are almost indistinguishable from the initial GPS signals. This can be achieved in two ways:
  Proximity Spoofing Attack: the spoofer is few meters away from the target receiver.
  Distant Spoofing Attack: the spoofer is at a non-negligible distance with a precise alignment of the counterfeit and authentic signals, which is only possible with a meter-level accurate suggested position.

Table 6 presents a classification of UAV attacks based of their class, and whether the target is just one or multiple security goals.

7.2. Government countermeasures

The national approach adopted by the British Government to enhance its cyber-security protection against cyber-attacks includes cyber-security boot camps and the national budget:

- **Cyber-security Boot Camp:** According to a BBC article, cyber-spies will learn how to hack drones and crack codes at a new government-backed cyber-security boot-camp. The students will gain all the required skills to fight cyber-attacks and to keep the UK safe. The boot-camp is a 10-week long course, and certified by UK spy agency GCHQ [364].
- **National Budget:** Another BBC article announced that the Cyber Retraining Academy is operated by the cyber-security training firm, Sans Institute, and funded as part of the government's £ 1.9bn **National Cyber Security Strategy (NCSS)**. The performance of students throughout the course was being tracked, and talented individuals were recruited. The fifty

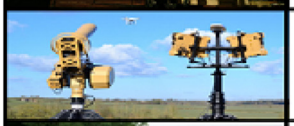
Presentation	Identification	Operational Distance	Target Size	Weapon Type	Lethal
	ATHENA	Several Kms	Undefined	Laser Beam	Yes
	Anti-UAV Zapper	Not Specified	Classified	Frequency Jam	No
	Rafael Drone Dome	3.5 Km	0.002 m2	Laser Beam	Yes
	CRAM	7 Km	Variable	Gatling Gun	Yes
	AUDS	10 Km	0.01 m2	Electro-Optical	No
	CLWS	35.4 Km	0.004 m2	Laser Beam	Yes

Fig. 7. Military anti-UAV/UAS techniques

successful candidates, who attended the academy in London in 2017, received a two year training condensed into 10 weeks [364].

7.3. Military countermeasures

Examples of military techniques to counter drone attacks include the use of old Soviet anti-aircraft weaponry (i.e ZSU-23-4 Shilka [365,366], and surface-to-air missiles (SAM S-300/S-400 missiles) [367,368]), to shoot down Turkish drones over Idlib and Syria [369,370]. Recent studies [371,372] revealed how terrorists are shifting towards a new asymmetric warfare called "drone warfare" [373]. For this reason, four main different military countermeasures were suggested and implemented to overcome the UAV security threats [374,375]. According to the Cable News Network (CNN), the Pentagon issued new guidelines allowing the military to bring down any drone flying near or over a US military base [376].

Next, we list a set of the most recent real-time highly accurate anti-drone countermeasures, and in Fig. 7, we highlight the latest generation of high-energy laser weapons targeting UAVs [377].

- **ATHENA:** or Advanced Test High Energy Asset, is an upgrade to the Area Defense Anti-Munitions (ADAM) system, which is a 30-KW laser weapon system that uses the 30-KW Accelerated Laser Demonstration Initiative (ALADIN) laser, which combines the power of three 10-KW fiber lasers into a single beam. ATHENA can also operate on 10 and 20 KW levels [378–380]. This system is funded and tested by Lockheed Martin and it can operate over thousands of meters.
- **Rafael Drone Dome:** is a counter-UAS operational mobile system [381] used to detect, track and eliminate hostile drones (even when maneuvering) as small as 0.002 m2, at a distance of 3.5 km, using a high power laser beam, enabling a soft and hard-kill. Testing results show its ability to successfully eliminate three drones in a timely manner [382–385].
- **Boeing Compact Laser Weapons System (CLWS):** is used to track and disable UAVs through the use of a laser weapon system to acquire, track, and identify potential targets, or even destroy them [386,387]. Its main advantages are based on the fact that it is portable and it can be assembled in almost 15 minutes. Moreover, it can destroy a target from 22 miles within 10-seconds, using an energy beam of 2, 5 or 10 KW.
- **Anti-UAV Defence System (AUDS):** is an anti-UAV system developed by UK defense companies to address the increasing UAV threats [388]. It is classified as a smart-sensor and "effector" package with the ability to remotely detect small UAVs, track and classify them before providing the option to disrupt their activities [389,390]. It was used around UK airports and it is now being deployed in New Zealand [11]. Among its characteristics, it contains an electronic-scanning radar aimed at detecting targets, an electro-optical video for target tracking and classification, along with a software known

as "intelligent directional RF inhibitor". Its detection range is up to 10 km, with a minimum target size of 0.01 m2. Moreover, it is able to operate in various weather conditions, and 24 hours a day.

- **Counter-Rocket and Mortar (CRAM):** is a missile-based counter rocket, artillery, and mortar defense system [391] developed as part of the US Army Enhanced Area Protection and Surviving (EAPS) technology, with an expansion including threats from unmanned aircraft systems or drones [392,393]. In fact, CRAM is the land version of Phalanx CIWS [394]. Among its characteristics is the use of a 20mm HEIT-SD (highly explosive incendiary tracer, self-destruct) [395,396], 30, 50 or 76mm Driven Ammunition Reduced Time (DART) of flight [397], cannon to launch command guided interceptors using a precise tracking radar interfero-meter as a sensor, a fire Control Computer (CC), along with an RF transceiver to launch the projectile into an engagement 'basket' [398]. Computations are then made on the ground, and the RF sends the information back to the CC.
- **Non-kinetic Methods:** other countermeasures include non-kinetic methods such as the use of radio waves to disrupt drone flights [372]. However, due to the rules of engagement being classified, it is hard to tell under what options and weapons the army might use them [399].
- **Anti-UAV Zappers:** were sent and used by the British forces on the frontline in Iraq and Syria to protect Western and American forces against drone attacks emanating from the Islamic State of Iraq and Syria (ISIS). By 2017, Zapper was responsible for downing more than 500 drones through radar jamming [400].
- **ADS-ZJU:** ADS-ZJU stands for Anti-Drone System at Zhejiang University; it was developed by Shi et al. in [11] and tested on a DJI Phantom 4 drone. The authors combined three detection and surveillance technologies including audio, video, and RF, and the architecture consists of four units:
  - **Heterogeneous Sensing Unit:** it uses various types of sensors to capture information to detect drones.
  - **Central Processing Unit:** it performs drone feature extraction, drone detection, and drone localization.
  - **Automatic Jamming Unit:** it relies on RF jamming against any drone flying over a sensitive area.
  - **Real-Time Display Unit:** it is based on a liquid crystal display that predicts both acoustic signals and real-time trajectory of a drone.

These solutions are summarized in Table 5.

7.4. Drones detection techniques

The rise of UAVs/drones, led to many detection techniques being developed and used as early warning signs. In fact, some of these techniques were presented and classified by Ganti et al. in [401] whilst also including their advantages, drawbacks and accuracy levels. Nonetheless, this paper presents the most known drone detection techniques as follows:

7.4.1. Audio detection

is an acoustic detection method, which captures the ambient sound through the use of a multi-directional microphone array that detects any sound from a range of 25 to 30 ft [401]. Then, the sound waves are filtered to analyze the target's frequency. This is possible since drones are noisy; their rotary includes at least 8 razors that buzz louder as it gets nearer. However, this method offers a high level of accuracy in quiet areas, and is not suitable in noisy environments.

7.4.2. Video detection

has been classified as a limited detection method [402]; the detection mechanism includes the ability to capture images of flying drones even at high distances (350 ft) with an acceptable resolution. However, the main problem is its inability to distinguish between birds and drones [401], which results into a high level of detection failure, despite the use of computer algorithms such as flight patterns. It was shown in [401] that seagulls' flight movement is similar to that of drones.

7.4.3. Motion detection

if combined with Speed Up Robust Features (SURF) algorithm, it can successfully detect drones while having other flying objects in its vicinity [401] (50–150 ft away), and it also draws the path of the drones.

7.4.4. Thermal detection

is more accurate at detecting fixed-wing drones up to 350 ft away. In [403], Stolkin et al. stated that turbo-fan or the turbo-jet engines are easier to detect due to the generation of hot gases from their exhausts. However, it seems like this method is not suitable nor reliable for plastic quad-copters with electric motors. Hence, in [401], Ganti et al. suggested that it is better to combine this method with other methods. Either way, its implementation cost is high with a low detection rate over a limited distance.

7.4.5. Radar detection

is very useful at detecting large aircrafts [404] over long distances (150-1500+ ft), but not small ones. This is due to the fact that smaller drones emit less noise and have less signal transmission.

Table 5
Analytical review of drone/UAV detection-prevention security solutions.

Technique	Equipment		Description							Use				Nature		Task			
Abbreviation	Software	Hardware	Deployment	Cost	Performance	Accuracy	Range	All -Weather	Limitation(s)	Civil	Military	National	International	Lethal	Non- Lethal	Detection	Jamming	Destruction	Capture
De-Drone	No	Yes	Mobile (Carry)	Varying	Acceptable	Acceptable	400 m	Yes	Heavy, Always Carried	Yes	Yes	Yes	Yes	X	✓	✓	✓	X	Optional
Drone-Catcher	No	Yes	Flyable	Varying	Acceptable	Acceptable	12.2 m	No	Unreliable	Yes	No	No	No	X	✓	X	X	X	✓
CLWS	Yes	Yes	Portable /Stationary	High	High	High	35.4 Km	Yes	High Cost	No	Yes	Yes	No	✓	X	✓	X	✓	X
AUDS	Yes	Yes	Mobile /Stationary	High	High	Very High	10 km	Yes	High Cost	Possible	Yes	Yes	Yes	X	✓	✓	✓	Optional	Optional
CRAM	Yes	Yes	Mobile /Stationary	High	High	Very High	3.5+ km	Yes	High Cost /Maintenance	No	Yes	Yes	No	✓	X	✓	X	✓	X
Non-kinetic Methods	Yes	Yes	Stationary	Variable	Untested	Unspecified	Varying	Unspecified	Classified /Theory	Yes	Yes	Yes	Yes	X	✓	✓	✓	Optional	Optional
Anti-UAV Zapper	Yes	Yes	Mobile /Stationary	Unspecified	Very High	Very High	Classified	Yes	Unknown	No	Yes	Yes	No	X	✓	✓	✓	Optional	Optional
ADS-ZJU	Yes	Yes	Stationary	Variable	Acceptable	Acceptable	150 m	No	Require Further Enhancements	Yes	No	Yes	No	X	✓	✓	✓	X	X
GPS Spoofing	Yes	Yes	Mobile /Stationary	Varying	Acceptable	Acceptable	1 m - 0.8 km	Possible	Limited Range	Yes	Yes	Yes	Yes	X	✓	✓	✓	Optional	Optional

Table 6
Analytical review of drone/UAV detection methods.

Method	Operational		Description			
Type	Range	Field	Characteristics	Accuracy	Advantages	Limitations
Audio-based	25–30 ft	Open fields	Multi-directional microphone array	Variable	Detects drones /UAVs buzzing sound waves	Short range, noise interference
Video-based	350 ft	Urban/rural areas	High distance image capture	Moderate/low	Good resolution image capture	High detection failure, non-distinguish between birds & drones
Motion-based	50–150 ft	Open fields	Motion & speed detection	Acceptable	Successful drone detection among flying Objects	Short range
Thermal-based	350 ft	Urban/rural areas, Open fields	Heat detection	High/low	Accurate at detecting fixed-wing drones	Inaccurate at detecting smaller quad-copters
Radar-based	150–1500+ ft	Urban/rural Areas, Open fields	Heat, motion & noise detection	High/moderate	Highly accurate at detecting/locating large/medium drones/UAVs	Inaccurate at detecting/locating small/tiny drones/UAVs
RF-based	200–1400 ft	Urban/rural area, open fields	RF signal detection/interception	High/moderate	Successful at detecting/intercepting signals & locating drones	Prone to signal interference, unable to detect higher/lower frequencies

7.4.6. RF Detection

RF detection is very effective for long-range drones since RF signals can be detected from a longer distance (between 200 ft [405] and up to 1400 ft). As such, in [406], Hansen et al. stated that it is highly difficult to detect a drone that escapes RF detection, especially when drones transmit an image to the Ground Control Station (GCS) using an RF signal. However, to ensure a successful detection rate, the transmitter's power and receiver's sensitivity must be first evaluated and maintained.

Table 6 lists the available drone/UAV detection methods.

In this section, we presented the possible drone/UAV and counter-drone/UAV security measures, in addition to prevention techniques, and solutions related to the security of drone/UAV communications and networks, which are essential for armed forces and search-and-rescue operations. Next, we discuss the limitations of the current solutions, in addition to recommendations for future research directions to secure UAS, UAVs and drone's systems, networks, data and communications.

8. Limitations and recommendations

8.1. Limitations

Many limitations are currently facing the adoption and usage of drones, which include serious security threats [407]. The main existing limitations in drones' security are:

- **Market Availability:** the availability of drones in all markets made them a suitable choice for terrorists and criminals to launch malicious activities. Further security screening and inspection requirements are needed, especially for the owners of advanced drone types.
- **Weak Designs:** manufacturers should take security as a key component in the development of any firmware, hardware and application. Therefore, security-by-design is the best practice to prevent most of the security attacks.
- **Weak Policies:** the adoption of authorization and authentication policies should be strict, preventing unauthorized entities from accessing a drone system, to prevent possible insider threats.
- **Non-Real-Time Isolation:** the need to implement mechanisms that instantly disconnect and/or turn off the drone, once a security threat is detected, is widely being adopted and used. This minimizes possible damages and avoids injuries and/or deaths. Equally important is the need to have a return-to-base command chip to be installed in each UAV/drone, in case of wandering outside the line-of-sight.
- **Limited Testing Phase:** drones must undergo thorough testing to evaluate the corresponding threat level when they fall into the wrong hands. Therefore, the applications that control the drones must be tested to prevent any security flaw that could be exploited by attackers. One way is to design automated drone penetration tests.
- **Limited Forensics Capabilities:** drones forensics are not currently a priority, even though they are essential to trace back and reconstruct any possible attack event. Therefore, efficient and lightweight forensics tools are required to help in detecting, locating, finding and preserving digital evidences, along with their corresponding sources [408,409].
- **Weak level of Protection:** drones protection systems should include three main phases for the detection, correction and protection, which is not currently the case.
- **Weak Authentication Scheme:** the literature review revealed how drones can be easily hijacked and intercepted by compromising the authentication process. Thus, an enhanced lightweight multi-factor authentication scheme is recommended to address this issue.
- **Weak or Missed Cryptographic Suites:** since the transmitted traffic is sometimes unencrypted, connection should be protected to ensure data confidentiality and authentication. Thus, using strong cryptographic suites is recommended to prevent data breaches.
- **Limited Frequency Range:** drones/UAVs are mostly prone to frequency attacks, which brings them down easily. The lack of frequency hopping in drones makes them prone to jamming and de-authentication attacks. The best solution includes the ability to switch between frequencies to prevent such attacks.

8.2. Suggestions & recommendations

After discussing the main security and privacy threats, the attacks and corresponding solutions, next we propose recommendations to enhance drone/UAV security:

- **Drone Licensing:** drone users must legally register them and obtain a permit to fly them.
- **Firmer Restrictions:** must be taken into consideration, especially against the illegal use of drones and UAVs, and the irresponsible use of drones near vital areas such as airports and military installations.
- **Enhanced Surveillance:** over the import of drones, especially counterfeit ones and keeping track of their purchase history, especially when drones have the ability to lift and carry weight at a high altitude with enhanced video feedback.
- **Further Education:** is required, especially for drone users to understand their threats, along with training on how to use them.
- **Firmer Laws:** must be adopted to prevent the unauthorised/unlicensed use of drones/UAVs, and illegal operators must be held accountable by law.

- **Restricted & Confined Areas:** drones and UAVs must avoid flying over restricted areas and must only be flown above certain confined and designated areas to prevent any near-encounter that would result into property damage, injuries or loss of life.
- **National/International Counter-Terrorism Efforts:** must be applied and maintained to limit the use of drones/UAVs in terrorist operations, and to track and shut down illegal drones/UAVs markets and trafficking.
- **Specialized Non-Lethal Security Measures:** should also be considered as an ideal solution to counter the UAV threats over no-fly civilian areas to prevent damage and injuries.
- **Enhanced Drone/UAV Detection Methods:** that offer a better alarming approach of any incoming drone/UAV, and to allow for enough time to neutralize its threat at a distance.
- **Define New Lightweight Host/Network IDS/IPS:** without an efficient IDS, drones can be seriously compromised and be used to lead cyber or physical attacks against individuals and properties. Therefore, developing a lightweight IDS that employs hybrid detection techniques (i.e signature-based, specification-based and anomaly-based detection methods) is recommended to make prompt decisions in a drone resource-constrained environment or real-time applications.
- **Lightweight Multi-factor Authentication Scheme:** using only one factor (cryptographic one) is not sufficient since any weakness in the identification/authentication schemes would compromise the drone to be used for malicious purposes, which can potentially lead to drastic effects. To address these challenges, lightweight cryptographic and non-cryptographic-based solutions should be combined to reduce the probability of illegal access.
- **Lightweight Dynamic cryptographic Algorithms:** designing lightweight dynamic cryptographic algorithms can secure drone communications, ensuring a higher level of confidentiality with low latency and resources overhead. This is the case of the approach in [410,411], which uses a single-round function by relying on common channel parameters as "you know" factor and the secret key as "you have" factor to produce a dynamic key since wireless channel parameters change in a random manner [322]. Therefore, the dynamic cryptographic approach strikes the right balance between security and performance levels.

9. Conclusion

The tremendous increase in the use of drones and UAVs led to a new aviation era of autonomous aerial vehicles in both the civilian and military domains, offering numerous benefits including economical, commercial, industrial, mainly due to their autonomous, flexible and easy-to-use nature, with low cost and energy consumption. However, their use led to the rise of many security, safety and privacy issues, which were manifested through various cyber attacks, threats and challenges, listed and explained in this paper. Also, we presented a holistic view of the drones/UAVs domains and provided detailed explanation and classification of their use in various domains and for different purposes, in addition to the different lethal/non-lethal security solutions as part of drones/UAVs countermeasures. Moreover, successful experiments to detect, intercept and hijack a drone through either de-authentication or jamming were highlighted, based on realistic scenarios that follow the traditional hacking cycle and hence, confirming the ease with which drones could be intercepted, especially in terms of UAV communication channels. In this context, different security suggestions and recommendations were proposed to ensure a safer and more secure use of drones and UAVs. Finally, due to the alarmingly increase in the use of drones by terrorists, further studies and experiments on how to prevent and counter the UAV threats, imposed by terrorists, will be performed and conducted as part of future work.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] K. Chan, U. Nirmal, W. Cheaw, Progress on drone technology and their applications: a comprehensive review, in: AIP Conference Proceedings, 2030, AIP Publishing, 2018, p. 020308.
[2] Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, K. Ren, Rise of mini-drones: applications and issues, in: Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, ACM, 2015, pp. 7–12.
[3] R. Altawy, A.M. Youssef, Security, privacy, and safety aspects of civilian drones: a survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2017) 7.
[4] D. He, S. Chan, M. Guizani, Drone-assisted public safety networks: the security aspect, IEEE Commun. Mag. 55 (8) (2017) 218–223.
[5] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, Taxonomy for description of cross-domain attacks on cps, in: Proceedings of the 2nd ACM international conference on High confidence networked systems, ACM, 2013, pp. 135–142.
[6] H. Sedjelmaci, S.M. Senouci, Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution, J. Supercomput. (2018) 1–17.
[7] T. Humphreys, Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing, Univer. Texas Austin (July 18, 2012) (2012).
[8] D.P. Shepard, J.A. Bhatti, T.E. Humphreys, A.A. Fansler, Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks, in: Proceedings of the ION GNSS Meeting, 3, 2012, pp. 3591–3605.
[9] İ. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, D. Matolak, Detection, localization, and tracking of unauthorized uas and jammers, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), IEEE, 2017, pp. 1–10.
[10] R.L. Sturdivant, E.K. Chong, Systems engineering baseline concept of a multispectral drone detection solution for airports, IEEE Access 5 (2017) 7123–7138.
[11] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, J. Chen, Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges, IEEE Commun. Mag. 56 (4) (2018) 68–74.

[12] B. Nassi, A. Shabtai, R. Masuoka, Y. Elovici, Sok-security and privacy in the age of drones: threats, challenges, solution mechanisms, and scientific gaps, arXiv Preprint arXiv:1903.05155 (2019).
[13] K.D. Atherton, The faa says there will be 7 million drones flying over america by 2020, Popular Sci. (2016).
[14] E. Vattapparamban, İ. Güvenç, A.İ. Yurekli, K. Akkaya, S. Uluağaç, Drones for smart cities: issues in cybersecurity, privacy, and public safety, in: Wireless Communications and Mobile computing Conference (IWCMC), 2016 International, IEEE, 2016, pp. 216–221.
[15] K. Dalamagkidis, K.P. Valavanis, L.A. Piegl, Aviation history and unmanned flight, in: On integrating unmanned aircraft systems into the national airspace system, Springer, 2012, pp. 11–42.
[16] M. Juul, Civil drones in the European union, Eur. Parliament. Res. Serv. (ed.). Eur. Union (2015).
[17] R. Stopforth, Drone licenses-neccesities and requirements, Il Ponte 73 (1) (2017) 149–156.
[18] V.S. Campos, European union policies and civil drones, in: Ethics and Civil Drones, Springer, Cham, 2018, pp. 35–41.
[19] A. Miah, Regulating drones, Drones: The Brilliant, the Bad and the Beautiful, Emerald Publishing Limited, 2020.
[20] S. Wright, Ethical and safety implications of the growing use of civilian drone, UK Parliament Website (Sci. Technol. Committee) (2020).
[21] Are drones dangerous or harmless fun? - bbc news, (https://www.bbc.com/news/uk-england-34269585). (Accessed on 07/09/2018).
[22] J.J. Cress, J.L. Sloan, M.E. Hutt, Implementation of unmanned aircraft systems by the us geological survey, Geocarto Int. 26 (2) (2011) 133–140.
[23] J. Park, S. Kim, K. Suh, A comparative analysis of the environmental benefits of drone-based delivery services in urban and rural areas, Sustainability 10 (3) (2018) 888.
[24] B. Canis, Unmanned aircraft systems (uas): commercial outlook for a new industry, 2015.
[25] C. Stöcker, R. Bennett, F. Nex, M. Gerke, J. Zevenbergen, Review of the current state of uav regulations, Remote Sens. (Basel) 9 (5) (2017) 459.
[26] T. Jones, International commercial drone regulation and drone delivery services, Technical Report, RAND, 2017.
[27] D.M. Marshall, R.K. Barnhart, S.B. Hottman, E. Shappee, M.T. Most, Introduction to unmanned aircraft systems, Crc Press, 2016.
[28] M. Chen, U. Challita, W. Saad, C. Yin, M. Debbah, Machine learning for wireless networks with artificial intelligence: a tutorial on neural networks, arXiv Preprint arXiv:1710.02913 (2017).
[29] J. Dinger, H. Hartenstein, Defending the sybil attack in p2p networks: taxonomy, challenges, and a proposal for self-registration, in: Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, IEEE, 2006, pp. 8–pp.
[30] H. Rowaihy, W. Enck, P. McDaniel, T. La Porta, Limiting sybil attacks in structured p2p networks, in: INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, IEEE, 2007, pp. 2596–2600.
[31] N. Naoumov, K. Ross, Exploiting p2p systems for ddos attacks, in: Proceedings of the 1st international conference on Scalable information systems, ACM, 2006, p. 47.
[32] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L.G. Giordano, A. Garcia-Rodriguez, J. Yuan, Survey on uav cellular communications: practical aspects, standardization advancements, regulation, and security challenges, arXiv Preprint arXiv:1809.01752 (2018).
[33] B. Uragun, Energy efficiency for unmanned aerial vehicles, in: Machine Learning and Applications and Workshops (ICMLA), 2011 10th International Conference on, 2, IEEE, 2011, pp. 316–320.
[34] P.J. Vincent, M. Tummala, J. McEachen, An energy-efficient approach for information transfer from distributed wireless sensor systems, in: System of Systems Engineering, 2006 IEEE/SMC International Conference on, IEEE, 2006, p. 6.
[35] Y. Singh, Wifi Espionage Using a Uav, 2016.
[36] J. Irizarry, M. Gheisari, B.N. Walker, Usability assessment of drone technology as safety inspection tools, J. Inf. Technol. Construct. (ITcon) 17 (12) (2012) 194–212.
[37] M.E. Abid, T. Austin, D. Fox, S.S. Hussain, Drones, uavs, and rpas: an analysis of a modern technology, Worcester Polytech. Inst., Worcester, Massachusetts (2014).
[38] P.H. Kopardekar, Unmanned aerial system (uas) traffic management (utm): Enabling low-altitude airspace and uas operations, 2014.
[39] A. Zeitlin, M. McLaughlin, Modeling for uas collision avoidance, AUVSI Unmann. Syst. North America, Orlando (2006).
[40] N.H. Motlagh, T. Taleb, O. Arouk, Low-altitude unmanned aerial vehicles-based internet of things services: comprehensive survey and future perspectives, IEEE Internet Things J. 3 (6) (2016) 899–922.
[41] F. Barfield, Autonomous collision avoidance: the technical requirements, in: National Aerospace and Electronics Conference, 2000. NAECON 2000. Proceedings of the IEEE 2000, IEEE, 2000, pp. 808–813.
[42] R. Sharma, D. Ghose, Collision avoidance between uav clusters using swarm intelligence techniques, Int. J. Syst. Sci. 40 (5) (2009) 521–538.
[43] L. Yang, J. Qi, J. Xiao, X. Yong, A literature review of uav 3d path planning, in: Intelligent Control and Automation (WCICA), 2014 11th World Congress on, IEEE, 2014, pp. 2376–2381.
[44] S. Ueno, T. Higuchi, Collision avoidance law using information amount, Numerical Analysis-Theory and Application, InTech, 2011.
[45] A.M. Brandt, M.B. Colton, Haptic collision avoidance for a remotely operated quadrotor uav in indoor environments, in: Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on, IEEE, 2010, pp. 2724–2731.
[46] J. Israelsen, M. Beall, D. Bareiss, D. Stuart, E. Keeney, J. van den Berg, Automatic collision avoidance for manually tele-operated unmanned aerial vehicles, in: Robotics and Automation (ICRA), 2014 IEEE International Conference on, IEEE, 2014, pp. 6638–6643.
[47] K. Tulum, U. Durak, S.K. Yder, Situation aware uav mission route planning, in: Aerospace conference, 2009 IEEE, IEEE, 2009, pp. 1–12.
[48] E. Yanmaz, R. Kuschnig, M. Quaritsch, C. Bettstetter, B. Rinner, On path planning strategies for networked unmanned aerial vehicles, in: Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, IEEE, 2011, pp. 212–216.
[49] L. Hernandez-Hernandez, A. Tsourdos, H.-S. Shin, A. Waldock, Multi-objective uav routing, in: Unmanned Aircraft Systems (ICUAS), 2014 International Conference on, IEEE, 2014, pp. 534–542.
[50] F. Baccelli, B. Błaszczyszyn, et al., Stochastic geometry and wireless networks: volume ii applications, Found. Trends® in Network. 4 (1–2) (2010) 1–312.
[51] H. Shakhatreh, A. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N.S. Othman, A. Khreishah, M. Guizani, Unmanned aerial vehicles: a survey on civil applications and key research challenges, arXiv Preprint arXiv:1805.00881 (2018).
[52] A. Rango, A. Laliberte, C. Steele, J.E. Herrick, B. Bestelmeyer, T. Schmugge, A. Roanhorse, V. Jenkins, Using unmanned aerial vehicles for rangelands: current applications and future potentials, Environ. Pract. 8 (3) (2006) 159–168.
[53] N. Jumaat, B. Ahmad, H.S. Dutsenwai, Land cover change mapping using high resolution satellites and unmanned aerial vehicle, in: IOP Conference Series: Earth and Environmental Science, 169, IOP Publishing, 2018, p. 012076.
[54] T. Sakano, Z.M. Fadlullah, T. Ngo, H. Nishiyama, M. Nakazawa, F. Adachi, N. Kato, A. Takahara, T. Kumagai, H. Kasahara, et al., Disaster-resilient networking: a new vision based on movable and deployable resource units, IEEE Netw. 27 (4) (2013) 40–46.
[55] J.-P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: limitations, issues and recommendations, Future Generat. Comput. Syst. (2019).
[56] C.A. Thiels, J.M. Aho, S.P. Zietlow, D.H. Jenkins, Use of unmanned aerial vehicles for medical product transport, Air Med. J. 34 (2) (2015) 104–108.
[57] M. Lipsitch, D.L. Swerdlow, L. Finelli, Defining the epidemiology of covid-19-studies needed, N. Engl. J. Med. (2020).
[58] F. Jiang, L. Deng, L. Zhang, Y. Cai, C.W. Cheung, Z. Xia, Review of the clinical characteristics of coronavirus disease 2019 (covid-19), J. Gen. Intern. Med. (2020) 1–5.
[59] M.N.K. Boulos, E.M. Geraghty, Geographical tracking and mapping of coronavirus disease covid-19/severe acute respiratory syndrome coronavirus 2 (sars-cov-2) epidemic and Associated Events around the World: How 21St Century Gis Technologies Are Supporting the Global Fight against Outbreaks and Epidemics, 2020.
[60] O. Alvear, N.R. Zema, E. Natalizio, C.T. Calafate, Using uav-based systems to monitor air pollution in areas with poor accessibility, J. Adv. Transp. 2017 (2017).

[61] T.F. Villa, F. Gonzalez, B. Miljievic, Z.D. Ristovski, L. Morawska, An overview of small unmanned aerial vehicles for air quality measurements: present applications and future prospectives, Sensors 16 (7) (2016) 1072.
[62] G. Rohi, G. Ofualagba, et al., Autonomous monitoring, analysis, and countering of air pollution using environmental drones, Heliyon 6 (1) (2020) e03252.
[63] P.K. Freeman, R.S. Freeland, Agricultural uavs in the us: potential, policy, and hype, Remote Sens. Appl. 2 (2015) 35–43.
[64] C. Malveaux, S.G. Hall, R. Price, Using drones in agriculture: unmanned aerial systems for agricultural remote sensing applications, in: 2014 Montreal, Quebec Canada July 13–July 16, 2014, American Society of Agricultural and Biological Engineers, 2014, p. 1.
[65] T. McKinnon, Agricultural drones: what farmers need to know, Boulder, Colorado (2016).
[66] K.R. Krishna, Agricultural drones: a peaceful pursuit, Taylor & Francis, 2018.
[67] V. Lakshmi, J. Corbett, How artificial intelligence improves agricultural productivity and sustainability: a global thematic analysis, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.
[68] J.C. van Gemert, C.R. Verschoor, P. Mettes, K. Epema, L.P. Koh, S. Wich, Nature conservation drones for automatic localization and counting of animals, in: European Conference on Computer Vision, Springer, 2014, pp. 255–270.
[69] B. Ivošević, Y.-G. Han, Y. Cho, O. Kwon, The use of conservation drones in ecology and wildlife research, J. Ecol. Environ. 38 (1) (2015) 113–118.
[70] A. Mukwazvure, T. Magadza, A survey on anti-poaching strategies, Int. J. Sci. Res. 3 (6) (2014) 1064–1166.
[71] A. Barnas, D. Chabot, A. Hodgson, D.W. Johnston, D.M. Bird, S.N. Ellis-Felege, A standardized protocol for reporting methods when using drones for wildlife research, J. Unmann. Vehicle Syst. (ja) (2020).
[72] A. Matos, E. Silva, N. Cruz, J.C. Alves, D. Almeida, M. Pinto, A. Martins, J. Almeida, D. Machado, Development of an unmanned capsule for large-scale maritime search and rescue, in: 2013 OCEANS-San Diego, IEEE, 2013, pp. 1–8.
[73] A. Matos, E. Silva, J. Almeida, A. Martins, H. Ferreira, B. Ferreira, J. Alves, A. Dias, S. Fioravanti, D. Bertin, et al., Unmanned maritime systems for search and rescue, Search Rescue Robotics; IntechOpen: London, UK (2017) 77–92.
[74] J.B. De Sousa, G.A. Gonçalves, Unmanned vehicles for environmental data collection, Clean Technol. Environ. Policy 13 (2) (2011) 369–380.
[75] V.V. Klemas, Coastal and environmental remote sensing from unmanned aerial vehicles: an overview, J. Coastal Res. 31 (5) (2015) 1260–1267.
[76] A. Hodgson, N. Kelly, D. Peel, Unmanned aerial vehicles (uavs) for surveying marine fauna: a dugong case study, PLoS ONE 8 (11) (2013) e79556.
[77] U.K. Verfuss, A.S. Aniceto, D.V. Harris, D. Gillespie, S. Fielding, G. Jiménez, P. Johnston, R.R. Sinclair, A. Sivertsen, S.A. Solbø, et al., A review of unmanned vehicles for the detection and monitoring of marine fauna, Mar. Pollut. Bull. 140 (2019) 17–29.
[78] L.K. Johnson, A.W. Dorn, S. Webb, S. Kreps, W. Krieger, E. Schwarz, S. Shpiro, P.F. Walsh, J.J. Wirtz, An ins special forum: intelligence and drones/eyes in the sky for peacekeeping: the emergence of uavs in un operations/the democratic deficit on drones/the german approach to drone warfare/pursuing peace: the strategic limits of drone warfare/seeing but unseen: intelligence drones in israel/drone paramilitary operations against suspected global terrorists: us and australian perspectives/the 'terminator conundrum' and the future of drone warfare, Intell. Natl. Secur. 32 (4) (2017) 411–440.
[79] J. Straub, Unmanned aerial systems: consideration of the use of force for law enforcement applications, Technol. Soc. 39 (2014) 100–109.
[80] R.L. Finn, D. Wright, Unmanned aircraft systems: surveillance, ethics and privacy in civil applications, Comput. Law Secur. Rev. 28 (2) (2012) 184–194.
[81] A. Rosenfeld, Are drivers ready for traffic enforcement drones? Accid. Anal. Prevent. 122 (2019) 199–206.
[82] P. Chamoso, A. González-Briones, F. De La Prieta, J.M. Corchado, Computer vision system for fire detection and report using uavs., in: RSFF, 2018, pp. 40–49.
[83] J. Koebler, North dakota man sentenced to jail in controversial drone-arrest case, US NEWS & WORLD REPORT, Jan 15 (2014).
[84] M. Hibbett, Audible killings: Capitalist motivation, character construction, and the effects of representation in true crime podcasts, 2018.
[85] C.M. Traylor, Serialized killing: usability and user experience in the true crime genre, 2019.
[86] S. Michaeli, Crowd Control: Israel's Use of Crowd Control Weapons in the West Bank, B'tselem, 2013.
[87] M. Crowley, Tear gassing by remote control: the development and promotion of remotely operated means of delivering or dispersing riot control agents, Remote Control Project (2015).
[88] A.A. Porter, Law enforcement's use of weaponized drones: today and tomorrow, Louis ULJ 61 (2016) 351.
[89] P. Asaro, Algorithms of violence: critical social perspectives on autonomous weapons, Soc. Res.: Int. Q. 86 (2) (2019) 537–555.
[90] S. Lee, Simulating the contact zone: corporate mediations of (less-lethal) violence in israel, palestine, and beyond, Jerusalem Q. (75) (2018) 24.
[91] K.L. Cook, The silent force multiplier: the history and role of uavs in warfare, in: 2007 IEEE Aerospace Conference, IEEE, 2007, pp. 1–7.
[92] R. Chait, A. Sciarretta, D. Shorts, Army science and technology analysis for stabilization and reconstruction operations, Technical Report, NATIONAL DEFENSE UNIV WASHINGTON DC CENTER FOR TECHNOLOGY AND NATIONAL, 2006.
[93] J. Wilson, Uav roundup, Aerosp. Am. (2013) 26–36.
[94] T. Galdi, Revolution in military affairs, CRS Report for Congress, 11, 1995.
[95] S. Long, S. Haskins, Uavs and win: a command, control, communications, computers, surveillance lance and reconnaissance winner, ARMY COMMUNICATOR 22 (1997) 34–41.
[96] R. Chait, A. Sciarretta, J. Lyons, C. Barry, D. Shorts, D. Long, A Further Look at Technologies and Capabilities for Stabilization and Reconstruction Operations, Technical Report, NATIONAL DEFENSE UNIV WASHINGTON DC CENTER FOR TECHNOLOGY AND NATIONAL, 2007.
[97] J. Eggers, M.H. Draper, Multi-uav control for tactical reconnaissance and close air support missions: operator perspectives and design challenges, in: Proc. NATO RTO Human Factors and Medicine Symp. HFM-135. NATO TRO, Neuilly-sur-Siene, CEDEX, Biarritz, France, 2006, pp. 2006–2011.
[98] J. Drew, Raytheon system to quicken air response: Darpa's persistent close air support program enters flight test phase, Inside the Air Force 25 (6) (2014) 1–13.
[99] B.R. Pirnie, A. Vick, A. Grissom, K.P. Mueller, D.T. Orletsky, Beyond close air support. forging a new air-ground partnership, Technical Report, RAND CORP SANTA MONICA CA, 2005.
[100] S.D. Wing, French intervention in mali: strategic alliances, long-term regional presence? Small wars Insurgencies 27 (1) (2016) 59–80.
[101] F. Heisbourg, A surprising little war: first lessons of mali, Survival (Lond) 55 (2) (2013) 7–18.
[102] B. Charbonneau, Intervention in mali: building peace between peacekeeping and counterterrorism, J. Contemp. Afric. Stud. 35 (4) (2017) 415–431.
[103] D.J. Francis, The regional impact of the armed conflict and french intervention in mali, Oslo: Norwegian Peacebuilding Resource Centre (2013).
[104] R. Rotte, Western drones and african security, Afric. Secur. Rev. 25 (1) (2016) 85–94.
[105] G.R. Olsen, Fighting terrorism in africa by proxy: the usa and the european union in somalia and mali, Eur. Secur. 23 (3) (2014) 290–306.
[106] D.M. Anderson, J. McKnight, Kenya at war: Al-shabaab and its enemies in eastern africa, Afr. Aff. (Lond) 114 (454) (2015) 1–27.
[107] D. Agbiboa, The ongoing campaign of terror in nigeria: boko haram versus the state, Stability: International Journal of Security and Development 2 (3) (2013).
[108] C. Griffin, Operation barkhane and boko haram: french counterterrorism and military cooperation in the sahel, Small Wars Insurgenci. 27 (5) (2016) 896–913.
[109] H. Solomon, Terrorism and Counter-Terrorism in Africa: Fighting Insurgency from Al Shabaab, Ansar Dine and Boko Haram, Springer, 2015.
[110] S.G. Jones, A.M. Liepman, N. Chandler, Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab, Rand Corporation, 2016.
[111] S. Burgess, Military intervention in africa: french and us approaches compared, Air Space Power J. 9 (2) (2018) 5–25.
[112] S.J. Hansen, Al-Shabaab in Somalia: The history and ideology of a Militant Islamist group, Oxford University Press, 2013.
[113] R.P. Churchill, Drone warfare: Ethical and psychological issues, in: Unmanned Aerial Vehicles: Breakthroughs in Research and Practice, IGI Global, 2019, pp. 452–468.
[114] D. Barrie, B. Barry, H. Boyd, M.-L.C. Chagnaud, N. Childs, B. Giegerich, C. Mölling, T. Schütz, Protecting Europe: Meeting the EU's Military Level of Ambition in the Context of brexit, International Institute for Strategic Studies, 2018.

[115] C. Marshall, R. Garrett, Simulation for c?isr: command, control, communications, computers, intelligence, surveillance, & reconnaissance, Phalanx 29 (1) (1996) 1–11.
[116] A. Callam, Drone wars: armed unmanned aerial vehicles, Int. Aff. Rev. 18 (3) (2010).
[117] P. Felgenhauer, After august 7: the escalation of the russia-georgia war, in: The Guns of August 2008, Routledge, 2015, pp. 186–204.
[118] The basic requirements for modern complexes of guided artillery armament as an element of conducting distribution-fire actions of tactical level, 19, 2018, pp. 15–20.
[119] A. Radin, L.E. Davis, E. Geist, E. Han, D. Massicot, M. Povlock, C. Reach, S. Boston, S. Charap, W. Mackenzie, et al., What will russian military capabilities look like in the future?, 2019.
[120] N. Jenzen-Jones, J. Ferguson, Raising red flags: An examination of arms & munitions in the ongoing conflict in Ukraine, 3, Armament Research Services Pty. Ltd., 2014.
[121] M.A.C. Fox, Battle of debal' tseve: the conventional line of effort in russia' s hybrid war in ukraine.
[122] A. Rossiter, Drone usage by militant groups: exploring variation in adoption, Defense Secur. Anal. 34 (2) (2018) 113–126.
[123] J. Wendle, The fighting drones of ukraine, Air Space Mag. (2018).
[124] O. Analytica, Turkey may recruit more syrian rebel fighters, Emerald Expert Briefings, (oxan-es).
[125] P. Escobar, Turkey at War with Syria.
[126] H. Gusterson, Drone: Remote Control Warfare, MIT Press, 2016.
[127] C. Hovle, A. Koch, Yemen drone strike: just the start? Jane's Defence Weekly 38 (20) (2002) 3.
[128] M. Zenko, Reforming US drone strike policies, Council on Foreign Relations, 2013.
[129] C. Cole, Drone wars briefing, Drone Wars UK: Oxford, UK (2012).
[130] J.F. Kreis, Unmanned aircraft in israeli air operations, Air Power History 37 (4) (1990) 46–50.
[131] K. Hartley, J. Belin, The Economics of the Global Defence Industry, Routledge, 2019.
[132] R. Sanders, An israeli military innovation: Uavs, Technical Report, INDUSTRIAL COLL OF THE ARMED FORCES WASHINGTON DC, 2003.
[133] M. Dobbing, C. Cole, Israel and the drone wars: examining israel' s production, use and proliferation of uavs, Drone Wars UK, Oxford (2014).
[134] D. Gettinger, Drones operating in syria and iraq, Center for the Study of the Drone at Bard College (2016).
[135] S. Blank, The russian military resurgence: Post-soviet decline and rebuilding, 1992 deliIns–2018, 2019.
[136] O. Analytica, Damascus may press on in idlib, at high human cost, Emerald Expert Briefing.(oxan-db).
[137] O. Analytica, A new accommodation over syria's idlib is probable, Emerald Expert Briefing.(oxan-db).
[138] O. Analytica, Syria's new idlib offensive may be incremental, Emerald Expert Briefings(oxan-es).
[139] O. Analytica, Idlib ceasefire shows syria's relegation below libya, Emerald Expert Briefings(oxan-es).
[140] O. Analytica, Moscow will limit ankara's military gains in syria, Emerald Expert Briefings(oxan-es).
[141] O. Analytica, Ceasefire may ultimately dislodge turkey from syria, Emerald Expert Briefings(oxan-db).
[142] O. Analytica, Risk of russia-turkey clash in syria may prompt pause, Emerald Expert Briefings(oxan-es).
[143] K. Hartmann, K. Giles, Uav exploitation: a new domain for cyber power, in: 2016 8th International Conference on Cyber Conflict (CyCon), IEEE, 2016, pp. 205–221.
[144] R. Lafta, M.A. Al-Nuaimi, G. Burnham, Injury and death during the isis occupation of mosul and its liberation: results from a 40-cluster household survey, PLoS Med. 15 (5) (2018) e1002567.
[145] G. Goebel, History of unmanned aerial vehicles, 2008.
[146] L. Kennett, The First Air War: 1914-1918, Simon and Schuster, 1999.
[147] J.M. Sullivan, Evolution or revolution? the rise of uavs, IEEE Technol. Soc. Mag. 25 (3) (2006) 43–49.
[148] D. MacManus, K. Dean, M. Jones, R.J. Rona, N. Greenberg, L. Hull, T. Fahy, S. Wessely, N.T. Fear, Violent offending by uk military personnel deployed to iraq and afghanistan: a data linkage cohort study, The Lancet 381 (9870) (2013) 907–917.
[149] M. Benjamin, Drone warfare: Killing by remote control, Verso Books, 2013.
[150] Mini drone for special forces military black hornet, (http://dronesonvideo.com/personal-drone-for-special-forces-soldiers-black-hornet/). (Accessed on 07/09/2018).
[151] S.K. Chaturvedi, R. Sekhar, S. Banerjee, H. Kamal, Comparative review study of military and civilian unmanned aerial vehicles (uavs), INCAS Bull. 11 (3) (2019) 183–198.
[152] A. EGOZI, The israeli new loitering weapon systems-answering a growing demand.
[153] A. Ghulam, C.P. Tomlinson, The fire shadow project: a big step towards rapid acquisition, RUSI Defence Syst. (2008) 77–80.
[154] D. Von Winterfeldt, T.M. O'Sullivan, Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? Decis. Anal. 3 (2) (2006) 63–75.
[155] T. Gibbons-Neff, Israeli-made kamikaze drone spotted in nagorno-karabakh conflict, Washington Post 5 (2016).
[156] D. Chornenky, A multi-sided platform for remote operation of shared drones: deriving strategic opportunities from regulatory trends, Massachusetts Institute of Technology, 2018 Ph.D. thesis.
[157] M.A. Hussain, K. kyung Sup, et al., Wsn research activities for military application, in: 2009 11th International Conference on Advanced Communication Technology, 1, IEEE, 2009, pp. 271–274.
[158] P.E. Hagen, N. Storkersen, K. Vestgard, P. Kartvedt, The hugin 1000 autonomous underwater vehicle for military applications, in: Oceans 2003. Celebrating the Past... Teaming Toward the Future (IEEE Cat. No. 03CH37492), 2, IEEE, 2003, pp. 1141–1145.
[159] A. Inzartsev, Underwater vehicles, BoD–Books on Demand, 2009.
[160] M. Eaglen, J. Rodeback, Submarine arms race in the Pacific: The Chinese challenge to US undersea supremacy, Heritage Foundation, 2010.
[161] J. Perlez, M. Rosenberg, P. Cook, China agrees to return seized drone, ending standoff, pentagon says, N.Y. Times 17 (2016).
[162] O.R. Cote, Assessing the Undersea Balance between the US and China, MIT Center for International Studies, 2011.
[163] S. Kawashima, Japan–us–china relations during the trump administration and the outlook for east asia, Asia-Pacific Rev. 24 (1) (2017) 23–36.
[164] T. Hardy, G. Barlow, Unmanned underwater vehicle (uuv) deployment and retrieval considerations for submarines, in: International Naval Engineering Conference and Exhibition 2008, 2008.
[165] G. Bane, J. Ferguson, The evolutionary development of the military autonomous underwater vehicle, in: Proceedings of the 1987 5th International Symposium on Unmanned Untethered Submersible Technology, 5, IEEE, 1987, pp. 60–88.
[166] I. Braverman, E.R. Johnson, Blue Legalities: The Life and Laws of the Sea, Duke University Press, 2020.
[167] D. Clegg, M. Peterson, User operational evaluation system of unmanned underwater vehicles for very shallow water mine countermeasures, in: Oceans 2003. Celebrating the Past... Teaming Toward the Future (IEEE Cat. No. 03CH37492), 3, IEEE, 2003, pp. 1417–1423.
[168] P. Chu, Smart underwater robot (sur) for naval operations and undersea mining.
[169] S.C. Truver, Taking mines seriously: mine warfare in china's near seas, Naval War College Rev. 65 (2) (2012) 30–66.
[170] R.F. Grimmett, Authorization for use of military force in response to the 9/11 attacks (pl 107-40): Legislative history, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2006.
[171] P. Lee, Submission of evidence to the all party parliamentary group drones: how are raf reaper (drone) operators affected by the conduct of recent and ongoing operations? Appgdrones. org. uk (2017).
[172] L.E. Davis, M. McNerney, M.D. Greenberg, Clarifying the Rules for Targeted Killing: An Analytical Framework for Policies Involving Long-Range Armed Drones, Technical Report, RAND CORP SANTA MONICA CA SANTA MONICA United States, 2016.
[173] J. Allen, Testing the effects of us airstrikes on insurgent initiated violence in yemen, 2019.
[174] L. Cutler, Drone security policy and targeted killing, in: President Obama's Counterterrorism Strategy in the War on Terror, Springer, 2017, pp. 37–63.

[175] M.J. Boyle, The costs and consequences of drone warfare, Int. Aff. 89 (1) (2013) 1–29.
[176] E. Boussios, Changing the rules of war: the controversies surrounding the united states' expanded use of drones, Contemp. Voices: St Andrews J. Int. Relat. 6 (1) (2015).
[177] A. Dworkin, Drones and targeted killing: Defining a European position, European Council on Foreign Relations (ECFR), 2013.
[178] J. Becker, S. Shane, Secret 'kill list'proves a test of obama's principles and will, N.Y. Times 29 (2012) 5.
[179] D. Byman, Do targeted killings work, Foreign Aff. 85 (2006) 95.
[180] P. Lee, The drone operator and identity: exploring the constitution of ethical subjectivity in drones discourses, Critical Approaches to Discourse Analysis across Disciplines: CADAAD 9 (2) (2017) 62–78.
[181] E.G. Boussios, The proliferation of drones: a new and deadly arms race, J. Appl. Security. Res. 9 (4) (2014) 387–392.
[182] D. Gettinger, A.H. Michel, Loitering munitions, Center Study Drone (2017).
[183] L.E. Davis, M.J. McNerney, J. Chow, T. Hamilton, S. Harting, D. Byman, Armed and dangerous? UAVs and US security, Technical Report, RAND Corp Santa Monica Ca, 2014.
[184] M. Hughes, J. Hess, An assessment of lone wolves using explosive-laden consumer drones in the united states, Global Secur. Intell. Stud. 2 (1) (2016) 6.
[185] A mini uav becomes a suicide drone | paris air show 2015 content from aviation week, (http://aviationweek.com/paris-air-show-2015/mini-uav-becomes-suicide-drone-0).(Accessed on 07/09/2018).
[186] M.R. Stolley, Unmanned Vanguard: Leveraging The Operational Effectiveness Of The Israeli Unmanned Aircraft System Program, Technical Report, Air Command And Staff College Maxwell Air Force Base United States, 2012.
[187] G. Dragon, Israel aerospace industries (iai) unveiled at the singapore airshow the newest members in its loitering munitions (lm) family. iai is the world's pioneer in Developing and Fielding Various Types of Lms: the Most Prominent So Far Being Harpy (an Autonomous.
[188] I. Nammer, Categorie: Isr.
[189] S. Wright, P. Lee, Should we fear the rise of the drone assassins? The Conversation (2017).
[190] , Venezuela 'drone attack': Six arrests made - bbc news, 2018. (https://www.bbc.com/news/world-latin-america-45077057)
[191] , Venezuela: Military figures arrested after drone 'attack' - bbc news, 2018. (https://www.bbc.com/news/world-latin-america-45190905
[192] Terrorism by joystick | pittsburgh post-gazette, (https://www.post-gazette.com/opinion/2018/08/07/Terrorism-by-joystick/stories/201808070022).
[193] F. Sauer, N. Schörnig, Killer drones: the 'silver bullet'of democratic warfare? Secur. Dialog. 43 (4) (2012) 363–380.
[194] K. Bergmann, et al., Mq-4c: northrop grumman gears up for'triton'full rate production, Asia-Pacif. Def. Reporter (2002) 45 (1) (2019) 50.
[195] D. Gettinger, Drone spending in the fiscal year 2017 defense budget, Center for the Study of the Drone at Bard College, 2016.
[196] P. Schulte, Future war: Ai, drones, terrorism and counterterror, Handbook of Terrorism and Counter Terrorism Post 9/11, Edward Elgar Publishing, 2019.
[197] T.M. McDonnell, Sow what you reap: using predator and reaper drones to carry out assassinations or targeted killings of suspected islamic terrorists, Geo. Wash. Int'l L. Rev. 44 (2012) 243.
[198] T. Cooper, Combat drone makes trans-atlantic history, 2018. (https://www.forces.net/news/combat-drone-makes-trans-atlantic-history)
[199] M. Bowden, The ploy: the inside story of how the interrogators of task force 145 cracked abu musab al-zarqawi's inner circle-without resorting to torture-and hunted down al-qaeda's man in iraq, Atlantic Monthly 299 (4) (2007).
[200] P. Chambers, Abu musab al zarqawi: the making and unmaking of an american monster (in baghdad), Alternatives 37 (1) (2012) 30–51.
[201] N. Meo, How israel killed ahmed jabari, its toughest enemy in gaza, The Telegraph 17 (2012).
[202] S. Shah, N. MANDHANA, S.S. HASAN, World news, Wall Street J. 9 (2014).
[203] A. Jakira, Israeli Deterrence And the 2nd Lebanon War, Technical Report, AIR WAR COLL MAXWELL AFB AL MAXWELL AFB United States, 2017.
[204] O. Analytica, Fearful gulf states will seek to placate tehran, Emerald Expert Briefings (2020). oxan-es
[205] O. Analytica, A new us-iran war will play out in iraq and beyond, Emerald Expert Briefings (2020). oxan-db
[206] J.A. Sluka, Death from above: uavs and losing hearts and minds, Mil. Rev. 91 (3) (2011) 70.
[207] R. Veltman, et al., Rationalising Drone Warfare The Biopolitics and Necropolitics of US, Israeli and UK Drone Warfare, 2019 Master's thesis.
[208] A. Mir, D. Moore, Drones, surveillance, and violence: theory and evidence from a us drone program, Int. Stud. Q. 63 (4) (2019) 846–862.
[209] M. Bonetto, P. Korshunov, G. Ramponi, T. Ebrahimi, Privacy in mini-drone based video surveillance, in: Automatic Face and Gesture Recognition (FG), 2015 11th IEEE International Conference and Workshops on, 4, IEEE, 2015, pp. 1–6.
[210] G. Horsman, Unmanned aerial vehicles: a preliminary analysis of forensic challenges, Digital Invest. 16 (2016) 1–11.
[211] F. Guérin, F. Guinand, J.-F. Brethé, H. Pelvillain, et al., Uav-ugv cooperation for objects transportation in an industrial area, in: Industrial Technology (ICIT), 2015 IEEE International Conference on, IEEE, 2015, pp. 547–552.
[212] U. Afzal, T. Mahmood, Using predictive analytics to forecast drone attacks in pakistan, in: Information & Communication Technologies (ICICT), 2013 5th International Conference on, IEEE, 2013, pp. 1–6.
[213] S.G. Vemi, C. Panchev, Vulnerability testing of wireless access points using unmanned aerial vehicles (uav), in: Proceedings of the European Conference on e-Learning, Academic Conferences and Publishing International, 2015, p. 245.
[214] S.S. Devekar, T.M. Pawar, Y.M. Lande, S. Deokule, Autonomous Drone Delivery System for Lightweight Packages.
[215] O. Westerlund, R. Asif, Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things, in: 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), IEEE, 2019, pp. 1–10.
[216] K. Wesson, T. Humphreys, Hacking drones, Sci. Am. 309 (5) (2013) 54–59.
[217] Analysis: with drone attacks, the era of joystick terrorism appears to have arrived | south china morning post, 2018, (https://www.scmp.com/news/world/article/2158380/analysis-drone-attacks-prove-era-joystick-terrorism-has-arrived-and-world).
[218] R.J. Ball, The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications, Technical Report, Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), 2017.
[219] J.G. Bunnell, From the Underground to the High Ground: The Insurgent Use of Airpower, Technical Report, Air War College Air University Maxwell AFB United States, 2011.
[220] R.J. Bunker, Terrorist and Insurgent Unmanned Aerial Vehicles: use, potentials, and military implications, Technical Report, ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE, 2015.
[221] A.S. Yayla, A. Speckhard, The potential threats posed by isis's use of weaponized air drones and how to fight back, 2017.
[222] B. Solomon, Witnessing an isis drone attack, New York Times (2017). (https://www.nytimes.com/video/world/middleeast/100000005040770/isisdrone-attack-mosul.html)
[223] A. Sims, The rising drone threat from terrorists, Georgetown J. Int. Affair. 19 (2018) 97–107.
[224] A. Almohammad, A. Speckhard, Isis drones: evolution, leadership, bases, operations and logistics, Int. Center Study Violent Extremism 5 (2017).
[225] B. Serkan, Daesh's drone strategy technology and the rise of innovative terrorism, 2017, SETA Found. Polit. Econ. Soc. Res..
[226] T.H. Tønnessen, Islamic state and technology–a literature review, Perspectives on terrorism 11 (6) (2017) 101–111.
[227] M. Pomerleau, How $650 drones are creating problems in iraq and syria, C4ISRNET-Media for the Intelligence Age Military (2018).
[228] K. El Damanhoury, C. Winkler, W. Kaczkowski, A. Dicker, Examining the military–media nexus in isis's provincial photography campaign, Dyn. Asymmetr. Conf. 11 (2) (2018) 89–108.
[229] A. Harper, Drones Level the Battlefield for Extremists, 2018.
[230] J.A. Lee Ludvigsen, The portrayal of drones in terrorist propaganda: a discourse analysis of al qaeda in the arabian peninsula's inspire, Dyn. Asymmetric Confl. 11 (1) (2018) 26–49.

[231] M. McKown, The new drone state: suggestions for legislatures seeking to limit drone surveillance by government and nongovernment controllers, U. Fla. JL & Pub. Pol'y 26 (2015) 71.
[232] K.W. Smith, Drone technology: benefits, risks, and legal considerations, Seattle J. Envtl. L. 5 (2015) i.
[233] M. Hoenig, Hezbollah and the use of drones as a weapon of terrorism, Public Interest Rep. 67 (2) (2014).
[234] M. Knights, A. Mello, Defeat by annihilation: mobility and attrition in the islamic state's defense of mosul, CTC Sentinel 10 (43) (2017).
[235] D.H. Dunn, Drones: disembodied aerial warfare and the unarticulated threat, Int. Aff. 89 (5) (2013) 1237–1246.
[236] D. Rassler, The Islamic State and Drones: Supply, Scale, and Future Threats, Combating Terrorism Center at West Point, 2018.
[237] J. Warrick, Use of weaponized drones by isis spurs terrorism fears, Washington Post 12 (2017).
[238] H. Yokohama, J. Sunde, S.T. Ellis-Steinborner, Z. Ayubi, Vehicle borne improvised explosive device (vbied) characterisation and estimation of its effects in terms of human injury, Int. J. Protect. Struct. 6 (4) (2015) 607–627.
[239] M. Davis, Buda's Wagon: A brief history of the car bomb, Verso Books, 2017.
[240] N. Waters, Types of islamic state drone bombs and where to find them, Bellingcat. May 24 (2017).
[241] T. Gibbons-Neff, Houthi forces appear to be using iranian-made drones to ram saudi air defenses in yemen, report says, Washington Post 22 (2017).
[242] B. Hubbard, P. Karasz, S. Reed, Two major saudi oil installations hit by drone strike, and us blames iran, The New York Times (Sept. 14, 2019) (2019). available at https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html(last updated Sept. 15, 2019)
[243] D. Criekemans, Simulation exercise: Iran versus saudi arabia. geopolitical struggle in the middle east, 2019.
[244] F. Rezaei, Iran and Israel: Taking on the "zionist enemy", in: Iran's Foreign Policy After the Nuclear Agreement, Springer, 2019, pp. 215–242.
[245] M. Knights, The houthi war machine: from guerrilla war to state capture, Combatt. Terror. Center Sentinel 11 (8) (2018) 15–23.
[246] J.M. Sharp, I.A. Brudnick, Yemen: civil war and regional intervention, 2015.
[247] S. Center, Where coalitions come to die.
[248] L. Nevola, B. Shiban, The role of "coup forces," saleh, and the houthis, in: Global, Regional, and Local Dynamics in the Yemen Crisis, Springer, 2020, pp. 233–251.
[249] D. Rassler, Remotely piloted innovation: Terrorism, drones and supportive technology, Technical Report, Combating Terrorism Center at West Point West Point United States, 2016.
[250] Y. Katz, Idf encrypting drones after hezbollah accessed footage, Jerusalem Post (2010).
[251] S. Gorman, Y.J. Dreazen, A. Cole, Insurgents hack us drones, Wall Street J. 17 (2009).
[252] W. Wan, P. Finn, Global race on to match us drone capabilities, Washington Post 4 (2011).
[253] S.P. McBride, Pirating the ultimate killer app: hacking military unmanned aerial vehicles, Inf. Secur. Manag. Handbook 6 (2012) 301.
[254] T. Gibbons-Neff, Isis drones are attacking us troops and disrupting airstrikes in raqqa, officials say, Washington Post 14 (2017).
[255] C. Scher, D. Saah, Extent and characteristics of damage from wildfires caused by incendiary kites during protests of the gaza-israel barrier fence (march 2018 to present), AGU Fall Meeting Abstracts, 2018.
[256] L. Gleeson, et al., Palestinians still defying apartheid, Green Left Weekly (1189) (2018) 13.
[257] J. Zych, The use of weaponized kites and balloons in the israeli–palestinian conflict, Secur. Defence Q. (2019).
[258] H.M.-E. Khen, From knives to kites: developments and dilemmas around the use of force in the israeli–palestinian conflict since protective edge, J. Int. Humanitar. Legal Stud. 10 (2) (2019) 303–336.
[259] A. Cavoukian, Privacy and drones: Unmanned aerial vehicles, Information and Privacy Commissioner of Ontario, Canada Ontario, 2012.
[260] M.A. Kafi, Y. Challal, D. Djenouri, M. Doudou, A. Bouabdallah, N. Badache, A study of wireless sensor networks for urban traffic monitoring: applications and architectures, Procedia Comput. Sci. 19 (2013) 617–626.
[261] K. Mansfield, T. Eveleigh, T.H. Holzer, S. Sarkani, Unmanned aerial vehicle smart device ground control station cyber security threat model, in: Technologies for Homeland Security (HST), 2013 IEEE International Conference on, IEEE, 2013, pp. 722–728.
[262] A. Jones, G.L. Kovacich, Global Information Warfare: The New Digital Battlefield, Auerbach Publications, 2015.
[263] B. Hudson, Drone attacks are essentially terrorism by joystick - the washington post, 2018. (https://www.washingtonpost.com/opinions/drone-attacks-are-essentially-terrorism-by-joystick/2018/08/05/f93ec18a-98d5-11e8-843b-36e177f3081c_story.html?noredirect=on&utm_term=.792978a5071d)
[264] P. Boucher, Domesticating the drone: the demilitarisation of unmanned aircraft for civil markets, Sci. Eng. Ethic. 21 (6) (2015) 1393–1412.
[265] C. Letterman, D. Schanzer, W. Pitts, K. Ladd, J. Holloway, S. Mitchell, S.C. Kaydos-Daniels, Unmanned aircraft and the human element: Public perceptions and first responder concerns, Technical Report, Institution for Homeland Security Solutions, 2013.
[266] H. Du, M.A. Heldeweg, Responsible design of drones and drone services: Legal perspective synthetic report, 2017.
[267] K. Wackwitz, H. Boedecker, Safety risk assessment for uav operation, Drone Industry Insights, Safe Airspace Integration Project, Part One, Hamburg, Germany (2015).
[268] E.B. Carr, Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace, Natl. Centre Policy Anal. (NCPA). Retriev. September 23 (2013) 2014.
[269] N. Syed, M. Berry, Journo-drones: a flight over the legal landscape, Comm. LAw. 30 (2014) 1–27.
[270] R.L. Finn, D. Wright, M. Friedewald, Seven types of privacy, in: European data protection: coming of age, Springer, 2013, pp. 3–32.
[271] R. Clarke, The regulation of civilian drones' impacts on behavioural privacy, Comput. Law Secur. Rev. 30 (3) (2014) 286–305.
[272] O. Salman, I. Elhajj, A. Chehab, A. Kayssi, Iot survey: an sdn and fog computing perspective, Comput. Netw. 143 (2018) 221–246.
[273] O. Salman, I. Elhajj, A. Chehab, A. Kayssi, Software defined iot security framework, in: 2017 Fourth International Conference on Software Defined Systems (SDS), IEEE, 2017, pp. 75–80.
[274] M.F.B.A. Rahman, Smart cctvs for secure cities: Potentials and challenges, 2017.
[275] Y. Zeng, R. Zhang, T.J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges, arXiv preprint arXiv:1602.03602 (2016).
[276] D. Rudinskas, Z. Goraj, J. Stankūnas, Security analysis of uav radio communication system, Aviation 13 (4) (2009) 116–121.
[277] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, Unmanned aircraft capture and control via gps spoofing, J. Field Rob. 31 (4) (2014) 617–636.
[278] S.-H. Seo, B.-H. Lee, S.-H. Im, G.-I. Jee, Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal, J. Positioni. Navigat. Timing 4 (2) (2015) 57–65.
[279] A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge, Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, in: Infotech@ Aerospace 2012, 2012, p. 2438.
[280] N. Shashok, Analysis of vulnerabilities in modern unmanned aircraft systems, 2017.
[281] X. Lin, R. Wiren, S. Euler, A. Sadam, H.-L. Maattanen, S.D. Muruganathan, S. Gao, Y.-P.E. Wang, J. Kauppi, Z. Zou, et al., Mobile networks connected drones: field trials, simulations, and design insights, arXiv Preprint arXiv:1801.10508 (2018).
[282] A. Abdallah, M.Z. Ali, J. Mišić, V.B. Mišić, Efficient security scheme for disaster surveillance uav communication networks, Information 10 (2) (2019) 43.
[283] D. Kovar, Uavs, Iot, and Cybersecurity, 2016.
[284] P. Ramon Soria, R. Bevec, B. Arrue, A. Ude, A. Ollero, Extracting objects for aerial manipulation on uavs using low cost stereo sensors, Sensors 16 (5) (2016) 700.
[285] R. Tomislav, V. Andrija, I. Jurica, W. Bo, Challenges and solutions for urban uav operations, in: International Scientific Conference "Science and Traffic Development"(ZIRP 2018), 2018.
[286] M. Alwateer, S.W. Loke, A. Zuchowicz, Drone services: issues in drones for location-based services from human-drone interaction to information processing, J. Locat. Based Serv. 13 (2) (2019) 94–127.

[287] S.J. Kim, G.J. Lim, J. Cho, Drone flight scheduling under uncertainty on battery duration and air temperature, Comput. Ind. Eng. 117 (2018) 291–302.
[288] C.-M. Tseng, C.-K. Chau, K. Elbassioni, M. Khonji, Autonomous recharging and flight mission planning for battery-operated autonomous drones, arXiv preprint arXiv:1703.10049 (2017).
[289] B.P. Commission, et al., The security impact of drones: challenges and opportunities for the uk, Univer. Birmingham, October (2014).
[290] R.A. Clothier, R.A. Walker, N. Fulton, D.A. Campbell, A casualty risk analysis for unmanned aerial system (uas) operations over inhabited areas, 2007.
[291] M. Dinucci, Missili usa in romania e polonia: l'europa sul fronte nucleare.
[292] M. Erdelj, E. Natalizio, Drones, smartphones and sensors to face natural disasters., in: DroNet@ MobiSys, 2018, pp. 75–86.
[293] P. Velagapudi, S. Owens, P. Scerri, M. Lewis, K. Sycara, Environmental factors affecting situation awareness in unmanned aerial vehicles, in: AIAA Infotech@ Aerospace Conference and AIAA Unmanned... Unlimited Conference, 2009, p. 2057.
[294] M. Strohmeier, V. Lenders, I. Martinovic, Intrusion detection for airborne communication using phy-layer information, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2015, pp. 67–77.
[295] R. Mitchell, R. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. Syst. Man Cybernet. 44 (5) (2014) 593–604.
[296] R. Mitchell, R. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. Syst. Man Cybernet. 44 (5) (2013) 593–604.
[297] T. Kacem, D. Wijesekera, P. Costa, A. Barreto, An ads-b intrusion detection system, in: Trustcom/BigDataSE/ISPA, 2016 IEEE, IEEE, 2016, pp. 544–551.
[298] S.G. Casals, P. Owezarski, G. Descargues, Generic and autonomous system for airborne networks cyber-threat detection, in: Digital Avionics Systems Conference (DASC), 2013 IEEE/AIAA 32nd, IEEE, 2013, pp. 4A4–1.
[299] C. Rani, H. Modares, R. Sriram, D. Mikulski, F.L. Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks, J. Defense Model. Simul. 13 (3) (2016) 331–342.
[300] H. Lu, Y. Li, S. Mu, D. Wang, H. Kim, S. Serikawa, Motor anomaly detection for unmanned aerial vehicles using reinforcement learning, IEEE Internet Things J. 5 (4) (2017) 2315–2322.
[301] J.-P. Condomines, R. Zhang, N. Larrieu, Network intrusion detection system for uav ad-hoc communication: from methodology design to real test validation, Ad Hoc Netw. 90 (2019) 101759.
[302] H. Sedjelmaci, S.M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks, IEEE Trans. Syst. Man Cybernet. 48 (9) (2017) 1594–1606.
[303] H. Sedjelmaci, S.M. Senouci, N. Ansari, Intrusion detection and ejection framework against lethal attacks in uav-aided networks: a bayesian game-theoretic methodology, IEEE Trans. Intell. Transp. Syst. 18 (5) (2017) 1143–1153.
[304] A.P. Lauf, R.A. Peters, W.H. Robinson, A distributed intrusion detection system for resource-constrained devices in ad-hoc networks, Ad Hoc Netw. 8 (3) (2010) 253–266.
[305] R. Mitchell, I.-R. Chen, Specification based intrusion detection for unmanned aircraft systems, in: Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications, ACM, 2012, pp. 31–36.
[306] G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing uav communications via trajectory optimization, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.
[307] G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing uav communications via joint trajectory and power control, IEEE Trans. Wireless Commun. 18 (2) (2019) 1376–1389.
[308] M. Cui, G. Zhang, Q. Wu, D.W.K. Ng, Robust trajectory and transmit power design for secure uav communications, IEEE Trans. Veh. Technol. 67 (9) (2018) 9042–9046.
[309] N. Zhao, F. Cheng, F.R. Yu, J. Tang, Y. Chen, G. Gui, H. Sari, Caching uav assisted secure transmission in hyper-dense networks based on interference alignment, IEEE Trans. Commun. 66 (5) (2018) 2281–2294.
[310] H. Lee, S. Eom, J. Park, I. Lee, Uav-aided secure communications with cooperative jamming, IEEE Trans. Veh. Technol. 67 (10) (2018) 9385–9392.
[311] C. Liu, T.Q. Quek, J. Lee, Secure uav communication in the presence of active eavesdropper, in: 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2017, pp. 1–6.
[312] Y. Cai, F. Cui, Q. Shi, M. Zhao, G.Y. Li, Dual-uav-enabled secure communications: joint trajectory design and user scheduling, IEEE J. Sel. Areas Commun. 36 (9) (2018) 1972–1985.
[313] C. Li, Y. Xu, J. Xia, J. Zhao, Protecting secure communication under uav smart attack with imperfect channel estimation, IEEE Access 6 (2018) 76395–76401.
[314] Y. Lee, E. Kim, Y. Kim, D. Seol, Effective message authentication method for performing a swarm flight of drones, Emergency 3 (4) (2015) 95–97.
[315] Y.J. Kim, K.-U. Kyung, Secured radio communication based on fusion of cryptography algorithms, in: Consumer Electronics (ICCE), 2015 IEEE International Conference on, IEEE, 2015, pp. 388–389.
[316] J. Won, S.-H. Seo, E. Bertino, A secure communication protocol for drones and smart objects, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ACM, 2015, pp. 249–260.
[317] S. Seo, E. Bertino, Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing, CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 10 (2013) 2013.
[318] H. Sun, Q. Wen, H. Zhang, Z. Jin, A novel pairing-free certificateless authenticated key agreement protocol with provable security, Front. Comput. Sci. 7 (4) (2013) 544–557.
[319] G. Yang, C.-H. Tan, Strongly secure certificateless key exchange without pairing, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 71–79.
[320] D. Sharma, A. Rashid, S. Gupta, S.K. Gupta, A functional encryption technique in uav integrated hetnet: a proposed model, Int. J. Simul.–Syst. Sci. Technol. 20 (2019).
[321] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, C.-M. Wu, A traceable and privacy-preserving authentication for uav communication control system, Electronics (Basel) 9 (1) (2020) 62.
[322] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, M.M. Mansour, One round cipher algorithm for multimedia iot devices, Multimed. Tools Appl. 77 (14) (2018) 18383–18413.
[323] K.A. Shim, C.M. Park, A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 26 (8) (2015) 2128–2139, doi:10.1109/TPDS.2014.2346764.
[324] E.S. Pilli, R. Joshi, R. Niyogi, A generic framework for network forensics, Int. J. Comput. Appl. 1 (11) (2010).
[325] N.L. Beebe, J.G. Clark, A hierarchical, objectives-based framework for the digital investigations process, Digital Invest. 2 (2) (2005) 147–167.
[326] U. Jain, M. Rogers, E.T. Matson, Drone forensic framework: Sensor and data identification and verification, in: Sensors Applications Symposium (SAS), 2017 IEEE, IEEE, 2017, pp. 1–6.
[327] H. Bouafif, F. Kamoun, F. Iqbal, A. Marrington, Drone forensics: Challenges and new insights, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–6.
[328] T.E.A. Barton, M.H.B. Azhar, Open source forensics for a multi-platform drone system, in: International Conference on Digital Forensics and Cyber Crime, Springer, 2017, pp. 83–96.
[329] T.E.A. Barton, M.H.B. Azhar, Forensic analysis of popular uav systems, in: Emerging Security Technologies (EST), 2017 Seventh International Conference on, IEEE, 2017, pp. 91–96.
[330] D.R. Clark, C. Meffert, I. Baggili, F. Breitinger, Drop (drone open source parser) your drone: forensic analysis of the dji phantom iii, Digital Invest. 22 (2017) S3–S14.
[331] E. Mantas, C. Patsakis, Gryphon: Drone forensics in dataflash and telemetry logs, in: International Workshop on Security, Springer, 2019, pp. 377–390.

[332] B. Carrier, E.H. Spafford, An event-based digital forensic investigation framework, in: Digital forensic research workshop, 2004, pp. 11–13.
[333] A. Roder, K.-K.R. Choo, N.-A. Le-Khac, Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study, arXiv preprint arXiv:1804.08649 (2018).
[334] J. Brunty, Validation of forensic tools and software: a quick guide for the digital forensic examiner, Forensic Mag. (2011).
[335] A. Krishnan, Killer robots: legality and ethicality of autonomous weapons, Routledge, 2016.
[336] C. Strawn, Expanding the potential for gps evidence acquisition, Small Scale Digital Device Forensics J. 3 (1) (2009) 1–12.
[337] A. Zulu, S. John, A review of control algorithms for autonomous quadrotors, arXiv preprint arXiv:1602.02622 (2016).
[338] K.M. Smalling, K.W. Eure, A short tutorial on inertial navigation system and global positioning system integration (2015).
[339] H. Achi, A. Hellany, M. Nagrial, Digital forensics of wireless systems and devices technical and legal challenges, in: High-Capacity Optical Networks and Enabling Technologies (HONET), 2009 6th International Symposium on, IEEE, 2009, pp. 43–46.
[340] G. Wild, J. Murray, G. Baxter, Exploring civil drone accidents and incidents to help prevent potential air disasters, Aerospace 3 (3) (2016) 22.
[341] K. McElrath, C. O'Neill, Experiences with mephedrone pre-and post-legislative controls: perceptions of safety and sources of supply, Int. J. Drug Policy 22 (2) (2011) 120–127.
[342] Uk Set to Ban Drones from Flying within 1Km of Airports | Financial Times, (https://www.ft.com/content/64d8ef9e-63fa-11e8-90c2-9563a0613e56). (Accessed on 07/09/2018).
[343] M. Zweiri, Iran and political dynamism in the arab world: the case of yemen, Digest Middle East Stud. 25 (1) (2016) 4–18.
[344] P. Brookes, The growing iranian unmanned combat aerial vehicle threat needs us action, Heritage Found. Backgrounder (3437) (2019).
[345] A. Sanchez, C. McKibben, Worst case scenario: the criminal use of drones, Counc. Hemispheric Affairs. Feb. 2 (2015).
[346] B.G. Williams, Counter Jihad: America's Military Experience in Afghanistan, Iraq, and Syria, University of Pennsylvania Press, 2016.
[347] M. Goodrich, Drone catcher:" robotic falcon" can capture, retrieve renegade drones, Michigan Tech News 7 (2016).
[348] E. Capello, M. Dentis, L.N. Mascarello, S. Primatesta, Regulation analysis and new concept for a cloud-based uav supervision system in urban environment, in: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), IEEE, 2017, pp. 90–95.
[349] M. Hooper, Y. Tian, R. Zhou, B. Cao, A.P. Lauf, L. Watkins, W.H. Robinson, W. Alexis, Securing commercial wifi-based uavs from common security attacks, in: MILCOM 2016-2016 IEEE Military Communications Conference, IEEE, 2016, pp. 1213–1218.
[350] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, C. Stracquodaine, Unmanned aerial vehicle security using recursive parameter estimation, J. Intell. Robot. Syst. 84 (1–4) (2016) 107–120.
[351] A. Abbaspour, K.K. Yen, P. Forouzannezhad, A. Sargolzaei, A neural adaptive approach for active fault-tolerant control design in uav, IEEE Trans. Syst. Man Cybernetics (2018).
[352] C.A.T. Bonilla, O.J.S. Parra, J.H.D. Forero, Common security attacks on drones, Int. J. Appl. Eng. Res. 13 (7) (2018) 4982–4988.
[353] J. Daubert, D. Boopalan, M. Mühlhäuser, E. Vasilomanolakis, Honeydrone: A medium-interaction unmanned aerial vehicle honeypot, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–6.
[354] J. Lindley, P. Coulton, Game of drones, in: Proceedings of the 2015 annual symposium on computer-human interaction in play, 2015, pp. 613–618.
[355] F. Trujano, B. Chan, G. Beams, R. Rivera, Security analysis of dji phantom 3 standard, Massachusett. Inst. Technol. (2016).
[356] L. Watkins, J. Ramos, G. Snow, J. Vallejo, W.H. Robinson, A.D. Rubin, J. Ciocco, F. Jedrzejewski, J. Liu, C. Li, Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems, in: Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, 2018, pp. 1–6.
[357] G. Fournier, P.A. de Kerdrel, P. Cotret, V.V.T. Tong, Dronejack: Kiss your drones goodbye!, 2017.
[358] K. Sharma, S. Bhatt, Jamming Attack–a Survey, 2018.
[359] G. Najera-Gutierrez, J.A. Ansari, Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, Packt Publishing Ltd, 2018.
[360] R. French, P. Ranganathan, Cyber attacks and defense framework for unmanned aerial systems (uas) environment.
[361] M. Booker, Effects of Hacking an Unmanned Aerial Vehicle Connected to the Cloud, The Ohio State University, 2018 Ph.D. thesis.
[362] K. Hartmann, C. Steup, The vulnerability of uavs to cyber attacks-an approach to the risk assessment, in: 2013 5th international conference on cyber conflict (CYCON 2013), IEEE, 2013, pp. 1–23.
[363] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, S. Capkun, On the requirements for successful gps spoofing attacks, in: Proceedings of the 18th ACM conference on Computer and communications security, ACM, 2011, pp. 75–86.
[364] M. Mohan, Cybersecurity in drones, Utica College, 2016 Ph.D. thesis.
[365] C. Kopp, Russian/Soviet point defence weapons, Technical Report, Air Power Australia, 2008.
[366] S.J. Zaloga, Zsu-23-4 shilka and soviet air defense gun vehicles, 1992.
[367] A. Priego, Russia's a2/ad policy as a balancing strategy vs nato enlargement, in: Security and Defence in Europe, Springer, 2020, pp. 203–216.
[368] M. Guardia, Self-Propelled Anti-Aircraft Guns of the Soviet Union, Bloomsbury Publishing, 2015.
[369] O. Analytica, Erdogan-putin relations will outweigh syria frictions, Emerald Expert Briefings(oxan-db).
[370] S. Köstem, Russian-turkish cooperation in syria: geopolitical alignment with limits, Cambridge Rev. Int. Affair. (2020) 1–23.
[371] G. LASCONJARIAS, H. MAGED, Fear the drones: Remotely piloted systems and non-state actors in Syria and Iraq, 2019.
[372] D.J. Praisler, Counter-UAV Solutions for the Joint Force, Technical Report, AIR WAR COLLEGE, AIR UNIVERSITY MAXWELL United States, 2017.
[373] A. Harutyunyan, Rapid development of uavs: Transforming the Warfare and Defence.
[374] G. Ding, Q. Wu, L. Zhang, Y. Lin, T.A. Tsiftsis, Y.-D. Yao, An amateur drone surveillance system based on the cognitive internet of things, IEEE Commun. Mag. 56 (1) (2018) 29–35.
[375] M. Kratky, J. Farlik, Countering uavs–the mover of research in military technology, Def. Sci. J. 68 (5) (2018) 460–466.
[376] A.H. Michel, Counter-drone systems, Center for the Study of the Drone at Bard College, 2018.
[377] M. Peck, High-energy laser weapons target uavs, C4ISRNET-webpage [Online]. Accessed 21 (2016) 2016.
[378] A. Extance, Military technology: laser weapons get real, Nature News 521 (7553) (2015) 408.
[379] C. Carter, Understanding c-uas purpose and process, Counter Unmanned Aircraft Syst. Technol. Oper. (2020).
[380] M.G. Tham, C.E. Wong, M.K.K.K. Ming, Technologies in hybrid warfare: challenges, Editor. Board, 12.
[381] G. Slocombe, et al., Uas: developments with small unmanned aerial systems, Asia-Pacif. Defence Rep. (2002) 45 (1) (2019) 36.
[382] A. Egozi, Rafael unveils /guillemotleftdrone dome/guillemotright anti-uav system, FlightGlobal 12 (2016).
[383] K. Atherton, Israeli contractor rafael shows off anti-drone laser in korea, Aust. Popular Sci. 21 (2015).
[384] O. Analytica, Tighter restrictions on drones promise limited gain, Emerald Expert Briefings(oxan-db).
[385] A. IAI's, Successes of israel's defence industry.
[386] J.P. Geis II, et al., Defeating small civilian unmanned aerial systems to maintain air superiority, Air Space Power J. 31 (2) (2017) 102.
[387] L.F. Hauck III, J.P. Geis II, et al., Air mines: countering the drone threat to aircraft, Air Space Power J. 31 (1) (2017) 26.
[388] A. Marrone, J.-P. Maulny, D. Fattibene, A.A. Stabile, Boosting defense cooperation in europe: an analysis of key military capabilities, Istituto Affari Internazionali, Institut de Relations Internationales et Strategiques, Hellenic Foundation for European and Foreign Policy, Swedish Defence Research Agency, Polish Institute of International Affairs, Royal United Services Institute (2018).
[389] A. Shelley, A framework for counter-unmanned aircraft system regulation in new zealand, Policy Q. 14 (3) (2018) 74–80.
[390] M. Król, W. Koperski, J. Błaszczyk, R. Woźniak, P.M. Błaszczyk, San: an integrated unmanned air vehicles interdictor system concept, Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa 8 (2017).
[391] C.D.H. Kiel, U.C.M. Ziv, U. Ret, A vision for directed energy and electric weapons in the current and future navy, Paper and presentation from ASNE, Arlington, VA (2007).

[392] B. Smith, R. Nourse, J. Baumann, G. Sanders, Extended area protection system (eaps) program overview, in: 2006 IEEE Aerospace Conference, IEEE, 2006, pp. 8–pp.
[393] M. Luciano, Extended area protection and survivability (eaps) ato 2016, Armaments Systems Forum [dok. elektr.], 2018. https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2016/armament/18295_Luciano.pdf[dost ep: 20.07.]
[394] R. Staton, R. Pawlak, Laser weapon system (LAWS) adjunct to the close-in weapon system (CIWS), Technical Report, NAVAL SURFACE WARFARE CENTER DAHLGREN DIV VA, 2012.
[395] J.D. Moretti, J.J. Sabatini, G. Chen, Armor piercing incendiary projectile, 2017. US Patent 9,702,678
[396] I. Siperco, Shield of david: the promise of israeli national missile defense, Middle East Policy 17 (2) (2010) 127.
[397] L. Seligman, Alternative to bae's 57 mm: Oto melara pitching 76 mm gun as option for navy's future frigate, Inside the Navy 28 (8) (2015) 1–12.
[398] M.M. Chen, Structural Design and Analysis of Initial Extended Area Protection and Survivability (EAPS) Projectile Configurations, Technical Report, ARMY RESEARCH LAB ABERDEEN PROVING GROUND MD WEAPONS AND MATERIALS RESEARCH DIRECTORATE, 2006.
[399] P. Green, Encyclopedia of Weird War Stories: Supernatural and Science Fiction Elements in Novels, Pulps, Comics, Film, Television, Games and Other Media, McFarland, 2017.
[400] S.S. Nikolić, An innovative response to commercial uav menace: anti-uav falconry, Vojno Delo 69 (4) (2017) 146–167.
[401] S.R. Ganti, Y. Kim, Implementation of detection and tracking mechanism for small uas, in: Unmanned Aircraft Systems (ICUAS), 2016 International Conference on, IEEE, 2016, pp. 1254–1260.
[402] E. Páll, K. Mathe, L. Tamas, L. Busoniu, Railway track following with the ar. drone using vanishing point detection, in: Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on, IEEE, 2014, pp. 1–6.
[403] R. Stolkin, D. Rees, M. Talha, I. Florescu, Bayesian fusion of thermal and visible spectra camera data for region based tracking with rapid background adaptation, in: Multisensor Fusion and Integration for Intelligent Systems (MFI), 2012 IEEE Conference on, IEEE, 2012, pp. 192–199.
[404] C.J. Li, H. Ling, Synthetic aperture radar imaging using a small consumer drone, in: Antennas and Propagation & USNC/URSI National Radio Science Meeting, 2015 IEEE International Symposium on, IEEE, 2015, pp. 685–686.
[405] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, T. Vu, Investigating cost-effective rf-based detection of drones, in: Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, ACM, 2016, pp. 17–22.
[406] S.T. Hansen, A.S. Ergun, B.T. Khuri-Yakub, Improved modeling and design of microphones using radio frequency detection with capacitive micromachined ultrasonic transducers, in: Ultrasonics Symposium, 2001 IEEE, 2, IEEE, 2001, pp. 961–964.
[407] G. Choudhary, V. Sharma, T. Gupta, I. You, Internet of drones (iod): threats, vulnerability, and security perspectives, arXiv Preprint arXiv:1808.00203 (2018).
[408] H. Noura, O. Salman, A. Chehab, R. Couturier, Preserving data security in distributed fog computing, Ad Hoc Netw. 94 (2019) 101937.
[409] H.N. Noura, O. Salman, A. Chehab, R. Couturier, Distlog: a distributed logging scheme for iot forensics, Ad Hoc Netw. 98 (2020) 102061.
[410] H. Noura, R. Melki, A. Chehab, M.M. Mansour, S. Martin, Efficient and secure physical encryption scheme for low-power wireless m2m devices, in: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, 2018, pp. 1267–1272.
[411] R. Melki, H.N. Noura, M.M. Mansour, A. Chehab, An efficient ofdm-based encryption scheme using a dynamic key approach, IEEE Internet Things J. (2018).