Countermeasures for Aerial Drones

Garik Markarian | Andrew Staniforth

Countermeasures for Aerial Drones

For a complete listing of titles in the
Artech House Radar Library,
turn to the back of this book.

Countermeasures for Aerial Drones

Garik Markarian
Andrew Staniforth

ARTECH HOUSE
BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library.

Cover design by Andy Meaden, meadencreative.com

ISBN 13: 978-1-63081-801-2

685 Canton Street
Norwood, MA 02062

10 9 8 7 6 5 4 3 2 1

To Liliya, Sophie, Maya, and Eddie
—Garik Markarian

To Corrie, Joseph, and Oliver
—Andrew Staniforth

Contents

Preface

The future of flight is currently being dominated by the proliferation of unmanned aerial vehicle (UAV) technology. It appears that the very same safety, efficiency, and cost benefits that appealed to the military application of UAV technology also makes drones attractive for a wide range of commercial and civil government functions.

However, along with the advantages and benefits, the increasing nefarious, criminal, and terrorist uses of drones raise important questions on the effective responses to rogue drone attacks and how this once-disruptive technology has now become decidedly dangerous. It is clear to see why drones offer a new tactic for operators with hostile intent, as they can be operated anonymously and remotely, they present little or no risk to their operators of detection or prosecution, they can be acquired cheaply and easily, their operation can be mastered simply and safely, and they can be used in isolation or in large numbers as swarms to devastating effect. The illegal use of drones is now a pressing security concern across the world as terrorists, activists, and criminals are adopting drone technology and developing new, creative, and sophisticated ways in which to commit crime and terrorism.

All in authority who have professional responsibility for the protection of valuable data and the maintenance of privacy, safety, security, and well-being of citizens and colleagues now need to prepare and equip their organizations against all manner of rogue drone hazards. However, combatting the threat of drones is largely ineffective without fully understanding the complexity of the UAV threat, which forms an integral part of the *Countermeasures for Aerial Drones.* Building upon joint research and innovation with leading law enforcement agencies and specialists in the defense and security drone detection domain, the primary purpose of this handbook recognizes that the formulation of a coherent counter-drone response includes understanding

not only the threat and risks posed by drones and knowledge of related regulatory frameworks, but also the procurement and deployment of the appropriate equipment, combined with the effective integration of that equipment and practical response measures embedded into the very culture and concept of an organization's existing security operation.

This handbook is organized into four parts. Part I examines the diverse drone threat landscape with a specific focus upon the criminal and terrorist uses of UAVs, as well as exploring new and emerging cybersecurity threat vectors from drones. Part II focuses upon the development of UAV technology and provides an in-depth overview of existing drones, their classifications, and major components. This part also analyzes the UAVs from the point of countermeasures, identifying strengths and weaknesses of various UAVs and recommending the most efficient countermeasures. Part III explores counter-UAV technology and systems. In this part, we describe the comprehensive approach to counter-UAV systems and describe both detection and neutralization components. We explain in detail the various detection sensors and present practical examples of the best systems that are currently available on the market. We emphasize the importance of artificial intelligence (AI) while designing command and control platforms and present a generalized counter-UAV (C-UAV) neutralization chain, suitable for various operational scenarios. Part IV examines and explains strategies to counter-UAVs, including explanations of regulatory frameworks and analysis of counter-UAV training and research programs designed to push drone and drone-detection technological development beyond the current state of the art.

Taken together, the individual parts of this handbook provide a coherent and comprehensive analysis of counter-UAV challenges, priorities, technologies, emerging trends, and best practices. Moreover, this handbook is enriched by the inclusion of case studies with unique industry insights, providing the knowledge required to ensure the design, development, and delivery of effective counter-drone policy, practice, and procedures. Given the growing concerns of drone threats, positive steps must now be taken to identify the most effective solutions to safeguard against hostile UAV incursions. This handbook provides all professionals, policymakers, and practitioners with expert guidance and advice on how organizations are able to effectively respond to the diverse range of threats from rogue drones that are becoming increasingly sophisticated and aggressive.

Acknowledgments

No technical book is the sole creation of its authors, and this particular book is no exception. It gives us a great pleasure to acknowledge the assistance and support of many people without whom this book would not have been possible, including:

- All colleagues at Rinicom Ltd., specifically Dr. Sean Sonander, Denis Kolev, Hassan Girach, James Barnes, Soren Sudby, and Natasha McCrone;
- All colleagues at Saher-UK and Saher-Europe, and specifically directors Dave Fortune, Andrew Brown, and Meredydd Hughes, CBE QPM.

The U.K. National Aerospace Technology Programme (NATEP) sponsored the Detection, Evaluation, Neutralisation and Identification (DENI) project that created the strong scientific foundation and research evidence base for this book.

We thank all our customers and partners who have shared information and insights about their systems and provided valuable comments and suggestions to this book.

Finally, we would also like to extend our thanks to Artech House for their professional support, guidance, and patience during the preparation of this book.

CHAPTER

1

Contents

The Drone Threat Landscape

1.1 Introduction

Social and technical innovations continue to occur at an ever-increasing speed, causing fast and drastic changes to society. These changes, driven by the possibilities offered by new and emerging technologies, affect citizens, governments, and all public and private industry sectors. Unmanned aerial vehicles (UAVs), or drones, are democratizing the sky and enabling new participants in aviation, quickly evolving beyond their military origin to become powerful business tools [1]. Drones have earned their status as a contemporary disruptive technology, proving to be an innovative development that has significantly altered the way that consumers, industries, and businesses across the world operate [2]. As a disruptive technology, drones have swept away systems and traditional operating practices because they have a diverse range of attributes that are recognizably superior. Drones are becoming an increasingly familiar aspect of life and work across the world today, playing a growing role in areas ranging from emergency services to construction to oil

and gas. However, the sudden and dramatic rise of the use of commercial drones from hobby enthusiasts to a ubiquitous business tool remains in its infancy. During a time when all organizations and governments across the world are under pressure to be more efficient, environmentally friendly, innovative, and ambitious in how they deliver services, drones offer a unique lens on the world below. Gathering data quickly and accurately from hard-to-reach places, they can create a unique record in near real time. This can make a crucial difference in managing costs, controlling risks, increasing safety, and influencing outcomes.

The proliferation of UAVs represents a disruptive technological innovation that continues to develop at exponential speed and on a global scale. Drones already have proven their ability to increase crop yields, make dangerous jobs safer, and act as a lifeline for remote populations. Autonomously piloted systems have the potential to revolutionize how people and goods are transported and to support entirely new and disbursed economic societies with profound implications. At the same time, this new technology is being hijacked by those with hostile intentions, adopting and adapting the use of drones for their own nefarious purposes, thereby creating a new counter-drone and drone-detection industry to prevent harm. Unfortunately, in the wrong hands, drones have the capacity to damage, destroy, disrupt, and, when used as a terrorist tactic, have the capability to conduct deadly and determined attacks. This chapter shall therefore examine the rise of drone use, identifying the current threats and future risks posed by UAVs to public safety and national security on a global scale.

1.2 The Future of Flight

It is clear to see why drones offer a new and exciting opportunity across all sectors as they can be operated remotely; they present little or no risk to their operators; they can be acquired easily; their operation can be mastered simply and safely; and their environmental impact on reducing emissions and carbon footprints when compared to other traditional forms of transport is impressive. However, the major factor critical to the success of the proliferation of drones remains the cost-effectiveness of commercial UAVs. As the average unit price of drones has decreased with their proliferation and reliability, drone use has accelerated to be successfully deployed as a crucial link in supply chain logistics for the pharmaceutical industry, enabling the delivery of fresh blood plasma and essential drugs to remote regions inaccessible to other forms of transport. UAVs have also proven their value as reconnaissance and delivery agents in the health-care and emergency services sectors, supporting fire and rescue operations. In agriculture, drones are being used to chart patterns and success rates for irrigation and

to monitor the health of growing crops via infrared and other technologies. However, the greatest impact upon the day-to-day operation of business will be the increasing use of drones for parcel delivery.

Industry forecasters suggest that delivery drones could become business as usual by 2030 [3], with large retail and logistics companies investing in delivery drones with the aim of achieving increased efficiency, lower costs, and increased customer satisfaction. Amazon is continuing to invest in its drone delivery system Prime Air, a future delivery system designed to safely get packages under 2.5 kg to customers in 30 minutes or less using small UAVs. Prime Air has great potential to enhance the services of Amazon, which already supports millions of customers by providing rapid parcel delivery. With safety as a key priority, Prime Air vehicles are being built with multiple redundancies, as well as sophisticated "sense and avoid" technology [4]. Through ongoing testing at development centers in the United States, the United Kingdom, Austria, France, and Israel, the drones are being assessed in multiple international locations and are gathering data to continue improving the safety and reliability of systems and operations [4]. Amazon intends to deploy Prime Air when and where it has the regulatory support needed to safely realize the vision of effectively incorporating small drones into the airspace and is also working with regulators and industry to design an unmanned air traffic management (UTM) system that will recognize who is flying what drone, where they are flying, and whether they are adhering to operating requirements [4].

The scope of delivery drones could also be beyond dropping off parcels in the "last mile" of client logistics. Drones will be ubiquitous in warehousing being able to autonomously conduct real-time stock checks by scanning inventory applications [3]. This will integrate seamlessly with other ground-based autonomous warehouse robotics in an end-to-end management and movement of inventory driven by artificial intelligence (AI) with no human touch. Delivery drones could also integrate with other advances in technology, for example, a driverless vehicle, loaded with parcels by robotics at the warehouse that automatically dispatches multiple delivery drones when it nears the most efficient point to complete its deliveries. Such a vehicle would serve as a base station for the drones providing charging and payload swapping as required. This scenario may still require several years of development, as current technical and regulatory challenges remain, such as flying pilotless fully automated drones and beyond visual line of site (BVLOS), but the drone delivery and wider logistics and supply chain are set to be revolutionized by the increasing use of UAVs [3].

Aside from drones as delivery vehicles, one particular service may end up being their chief contribution: by acting as mitigating forces against the impacts of climate change. Drones are now capable of everything from

fighting dwindling bee populations and reducing carbon emissions to tracking changes in the wildlife population and gathering water samples [5]. Perhaps the most prominent way in which drones can help to fight climate change is by assisting with data collection. Drones can travel to places where humans cannot easily go, thereby reducing research costs and increasing the accuracy of data collection. Researchers have already used drones to measure surface reflectivity, logging how much solar energy a landscape reflects and absorbs [6]. This measurement is crucial for understanding climate change and can help forest planners to determine in which locations to plant trees to get the most climate benefit. Satellites typically gathered this information in the past, but drones have the advantage of being more agile. Drones are also ideal for collecting information on air quality, monitoring wildlife population and activities, and calculating deforestation rates. Gathering data in this way also improves researcher safety, as helicopter and small plane crashes are the leading cause of on-the-job deaths for wildlife biologists [7].

Drones have also proved their efficiency at supporting the delivery of public health security operations. During the height of the coronavirus pandemic in 2020, to enforce new emergency powers to prevent public gatherings and promote social distancing measures, police forces across the world utilized the use of specially modified drones. Learning from police strategies in other jurisdictions to effectively manage public lockdowns, quarantine, and curfews, the U.K. police forces used their existing fleet of drones as part of a new tactical menu of options. Northamptonshire Police Chief Constable Nick Adderley said he planned to increase the force's number of drones from two to eight as using drones would be a "cost-effective way" to pass on information to the public and protect his first responders from contracting the virus [8].

The drones were equipped with speakers in order for them to transmit messages to the public, providing health warning updates and enforcing new emergency police powers. The decision to consider the use of drones to prevent the spread of Covid-19 in the United Kingdom followed the use of police drones in China, Spain, Belgium, and France. Local police in Italy were also permitted to use drones to monitor the movements of citizens, the Italian Civil Aviation Authority (ENAC) confirming their approval after receiving requests for additional support from local police units that were struggling to monitor the movement of citizens on lockdown by traditional police use of closed-circuit television (CCTV), roadblocks, checkpoints, and increased high-visibility patrols [9]. The Chula Vista Police Department in California also used drones equipped with cameras and loudspeakers to monitor the Coronavirus shutdown, doubling its fleet of drones with new specifications to include night-vision cameras. Spencer Gore, chief

executive of the U.S.-based drone company Impossible Aerospace, said he was "working like crazy" to help equip law enforcement agencies across the United States with drones to support Covid-19 police operations [10]. The police use of drones to enforce emergency government powers to prevent the spread of Covid-19 was another unprecedented measure to protect the public during the pandemic in which the versatility of drones was used to maintain public safety and save lives.

As the use of UAVs continues to increase, the size and type of UAVs is set to expand rapidly. The proliferation of UAVs includes the development of "Uber-style" drones to autonomously transport people within cities, developments that are amplifying the size, scale, and payloads of UAVs. The continued development of drone capacity and capability has created a market with huge potential, serving to further accelerate and amplify innovations of drone and drone-related technologies and systems. The rapid increase in the use of drones across all sectors has served to shape industry estimates of future growth of the drone market. In 2015, predictions that annual global revenues from commercial drone sales were expected to reach $500 million during 2020 were quickly surpassed [11]. New and revised industry estimates of global drone sales predict that the value will exceed $12 billion in 2021 [12]. Research focusing upon the consumer and commercial applications, regulations, and opportunities for 2020 found that a low price point had significantly reduced the barrier to entry in many sectors. In the United States, the projected growth of the market for commercial drones is set to rise from $850 million in 2020 to $1 billion in 2022, with the energy sector alone expected to grow to around $30 million by 2022 [13]. The largest share of the drone market in the United States is expected to be across all government departments, predicted to reach $420 million by 2022 [13]. In the United Kingdom, industry estimates predict that, by 2030, 76,000 drones will be flying across U.K. skies, being part of a projected drone technology industry with the potential to increase U.K. Gross Domestic Product (GDP) by £42 billion (or 2%) over the next 10 years [3]. The U.K. government's Counter-Unmanned Aircraft Strategy, published in 2019, reinforced this anticipated growth, stating that drones have the potential to bring great benefits to the United Kingdom, acknowledging that increasing levels of drone autonomy will increase their use across all sectors [14].

The predicted rise of domestic drone markets in the United States and the United Kingdom are also anticipated throughout European member states, as well as other nations across the globe. The future of flight is currently being dominated by the proliferation of drone technology and all industry estimates, even factoring the artificial inflation parameters for such predictions, provide strong evidence that drones are headed for new heights in the business world. Some industry forecasters also suggest that drones'

full economic potential is likely to be multiple times the number estimated, as their ripple effects reverberate through the economy as they continue to deliver savings and increase efficiencies when accessing new sectors [15]. It appears that the very same safety, efficiency, and cost benefits that appealed to the military also make drones attractive for a wide range of business and civil government functions. However, the rapid growth of the drone industry has so far outpaced the development of rules and systems to govern their use, resulting in a growing threat landscape that presents a major public safety and nation security concern. The increasing use of UAVs by amateur enthusiasts and professionally qualified UAV pilots has resulted in a growing catalog of incidents ranging in seriousness from minor occurrences causing public nuisance to major threats to national security. The inappropriate use of drones, encompassing causing antisocial harassment, alarm, and distress to individuals, includes the misuse of drones by persistent paparazzi invading the privacy of individuals. The inappropriate use of drones by pilots either losing control of their UAVs or not adhering to regulations, both of which provide evidence of inappropriate assessment of risk to others, has resulted in unnecessary injuries to pedestrians and entirely avoidable damage to vehicles and property. The increasing use of drones has also resulted in police officers in many nations across the world having to attend incidents and accidents involving drones and, more concerning, having to investigate a fourfold rise in crimes involving drones purchased online or direct from stores [16]. These investigations have included allegations that drones are being used by pedophiles hovering over children's playgrounds and burglars scoping out people's properties [16]. Law enforcement officers have taken it upon themselves to categorize the full range of incidents that they encounter from the misuse of drones, indicating that all of the drone-related reports that they investigate are either a direct result of the pilot's clueless, careless, or criminal actions.

An example of the misuse of drones with far-reaching unintended consequences occurred at the White House, Washington, D.C., at 3 a.m. on January 26, 2015, when an inebriated off-duty government intelligence officer flew a friend's quadcopter drone from an apartment located near the official residence of the U.S. President and lost control and sight of it [17]. The National Geospatial-Intelligence Agency officer texted his friends, worried that the drone may have landed on the White House grounds and then went to sleep [18]. It was not until the next morning, when he woke and learned from friends that a drone had been found at the White House, that he contacted his employer and cooperated with the Secret Service, who immediately began an investigation into the incident. In the process of what officials described as nothing more than a drunken misadventure, the employee managed to pilot his friend's drone under the radar of White

House defenses, causing substantial embarrassment to the security posture of the White House complex [17]. Shortly after the incident, the drone manufacturer released a firmware update for the model to prevent it from flying within a 25-km radius of the White House [19]. The rogue drone pilot did not face any criminal charges, as the investigation showed that, before the crash, the drone was in uncontrolled flight, so the prosecutor's office did not bring charges against the pilot [20]. The White House rogue drone incursion reflects the vast majority of drone incidents that occur in the absence of malicious or criminal intent but major security concerns are raised when drones are used with hostile intentions.

1.3 Aircraft Alert

Aviation facilities, particularly large airports, are attractive targets for terrorists and those involved in serious and organized crime because of their high-profile and iconic nature. An attack, or malicious and disruptive incursion using a drone, can have serious safety, security, and economic consequences. On July 22, 2014, the pilot of an Airbus A320 reported seeing a helicopter-style drone as the jet was 700 feet off the ground on its approach to the runway at London's Heathrow airport [21]. The U.K. Civil Aviation Authority (CAA) confirmed that an unidentified drone came close to hitting the commercial plane, which can carry 180 passengers, categorizing the incident as a "serious risk of collision," the highest rating that the CAA can attribute [21]. Investigators were unable to identify the drone, which did not appear on air traffic control radar and disappeared after the encounter. The near-miss was followed by a series of drone-related incidents being reported across the world, including three separate incidents in the United Arab Emirates in 2016, resulting in the temporary closures of Dubai and Sharjah International [22]. The shutdowns were serious events, costing hundreds of millions of dirhams per hour, disrupting dozens of flights and inconveniencing thousands of passengers as drone sightings were reported within restricted zones [22]. Reports of illegal use of UAVs at airports continue to increase but it is not just civil aviation that is under siege from rogue drone incursions.

In September 2017, the National Transportation Safety Board (NTSB) in the United States announced that it was investigating a collision between a recreational drone and an Army UH-60 helicopter that occurred in New York [23]. The NTSB, an independent federal agency responsible for investigating and determining the probable cause for transportation-related accidents, revealed that a drone had collided with the helicopter [24]. The Army helicopter sustained damage to its main rotor blade, window frame, and transmission deck. A motor and arm from a small drone, identified as

a DJI Phantom 4, were recovered from the helicopter [23]. Investigators were able to identify and subsequently interview the drone operator who provided flight data logs for the incident flight. Within a couple of weeks of the military helicopter collision in October 2017, another serious drone incident was reported, involving a UAV crashing into a commercial airplane in Canada, the first time that such an incident had occurred in the country [24]. A commercial plane operated by charter airline Skyjet was approaching Quebec City's Jean Lesage International Airport when a drone struck one of its wings [24]. There were six passengers and two crew members aboard the plane at the time of the incident [25]. Despite Canadian authorities having announced new safety measures making it illegal to fly recreational drones within 5.5 km of an airport and restricting the height of a drone's flight to 90m, the drone struck the passenger plane flying much higher than legally allowed, hovering some 450m above the ground [26]. The drone collision in Canada was part of a pattern of rogue drone incursions at major airports in 2017 and 2018 that suggested that a single pilot, operating a single drone, was responsible for the isolated incident. This threat analysis of rogue drone incursions would be dramatically changed by the events at London's Gatwick airport.

At 9 p.m. on December 19, 2018, authorities at Gatwick Airport suspended flights in and out of the airport after reports of two drones flying near the airfield were received [27]. Some planes arriving were diverted to other airports until 3 a.m. on December 20 when the airport was deemed safe to reopen, but within just 45 minutes, at 3:45 a.m., the runway was forced to close again after further reports of drone sightings were received [27]. Later that morning, Sussex Police revealed the flying of drones close to the airfield was a deliberate act to disrupt the airport but provided reassurance that there was no indication to suggest that the disruption was related to terrorism. As the airport remained closed in the afternoon of December 20, Gatwick Airport's chief operating officer Chris Woodroofe declared that the 110,000 passengers due to travel that day would witness cancellations and disruptions to their travel plans [27]. That same afternoon, the U.K. Ministry of Defence police revealed that they were in "ongoing discussions" with the Army about assisting with the operation to find the drones and to protect the airport so that it could be safely reopened. Later that same day, at around 6 p.m., Mr. Woodroofe revealed that the airport would remain closed for the rest of the evening after further drone activity had been reported "within the last hour." At 9:30 p.m. that same day, with the airport remaining closed, Detective Chief Superintendent Jason Tingley of Sussex Police provided information that there had been more than 50 sightings of the drone device in the past 24 hours, revealing that shooting down

the drone was a "tactical option" being considered by police [28]. At 6:60 a.m. the following morning, on Friday, December 21, Gatwick Airport was reopened, being available to a limited number of flights scheduled for departure and arrival [27].

The mayhem at Gatwick Airport was finally brought to an end when police requested the services of the military. The British Army used a cutting-edge Israeli anti-drone system to defeat the UAV threat that had ruined Christmas for thousands of passengers and cost the airline industry tens of millions of pounds [29]. The series of drone sightings above its runway forced Britain's second-largest airport to shut three times in 3 days, leaving 140,000 passengers stranded [29]. It was the airport's biggest disruption since the Icelandic volcanic ash cloud of 2010 and, embarrassingly for U.K. airport and security authorities, the most disruptive incident ever caused by a drone at a major international airport. The formal request for military aid to support civil power provided evidence that airport security and police tools and tactics to neutralize the threat and identify the perpetrators had proved ineffective. While technology used by the police helped the operation by tracking drones, it appears that the rogue drone over the skies of Gatwick airport was extremely advanced, rendering the technology used by police completely useless. To neutralize the drone threat, military teams used advanced battlefield techniques deployed against the Islamic State (IS) in conflicts overseas [30]. For members of the traveling public, the police response was frustrating, appearing to be outwitted by the deliberate actions of a drone pilot. With passenger safety remaining the number one priority to airport authorities, closing airspace when there was suspected unauthorized drone activity was essential. Assistant Chief Constable Dave Miller, head of operations command at Sussex Police, said [31]: "This was a serious and deliberate criminal act designed to endanger airport operations and the safety of the travelling public. A drone strike can cause significant damage to an aircraft in flight and it is important to emphasise that public safety was always at the forefront of our response. No aircraft was damaged or passenger injured. This was an unprecedented set of circumstances for all agencies involved at a time when the police and the government were at the early stages of assessing domestic counter drone technology. Equipment was quickly installed using both military and private assets to bring it to a conclusion and allow the airport to reopen." During the incident, local residents Paul Gait, aged 47, and Elaine Kirk, aged 54, were arrested on suspicion of causing the disruption, but, having been detained for 36 hours, they were released without charge, stating that they felt "violated" after their home was searched and their identities exposed [32]. Their statement came as Sussex Police faced growing criticism from government ministers, who

accused them of "messing up" the handling of the Gatwick drone incident, with Chris Grayling, the Transport Secretary, suggesting that "mistakes" had been made by Sussex Police. The main criticism from government ministers surrounded their statement during the incident that there existed the "possibility" that there might never have been a drone, despite later confirming that there had been 67 sightings of the drone, or drones, by credible witnesses [33]. Giles York, the Chief Constable of Sussex Police, defended the decision to hold Mr. Gait for an extended period, despite his employer saying he was at work during the rogue drone flights stating [33]: "I'm really sorry for what has been experienced and the feeling of violation around it."

Following an intensive 9-month police and airline authority investigation, and despite the drone activity happening in "groupings" on 12 separate occasions over 3 days, with sightings varying in length from between 7 and 45 minutes, no suspects have been brought to justice [25]. The chaos at Gatwick was compounded by conflicting reports of multiple sightings, further complicated by the police use of drones, which added to the complexity of confirming sightings at the time they were reported, and during the protracted post-incident investigation. The incident, being viewed across the world, caused major security embarrassment and a loss in confidence in the traveling public of the United Kingdom's measures to protect critical infrastructures from rogue drone activity. The incidents of rogue drone incursions, when combined with the ineffective response by authorities to prevent the threat and bring the perpetrators to justice, regrettably signaled to would-be terrorist plotters and other hostile actors, the effective ways in which to target and paralyze transport hubs and critical infrastructures.

The drone disruption to London's Gatwick Airport over the 2018 Christmas period was a wake-up call for the global aviation industry of the significant impact of malicious drone use. Hundreds of thousands of people had their travel disrupted, with tens of millions of pounds of economic damage [20]. The rogue drone sightings disrupted flights in and out of Gatwick Airport for 33 hours costing airlines an estimated £50 million [34]. The total cost was extrapolated from the budget airline easyJet's announcement that it lost £15 million in revenue and customer welfare costs during the shutdown [35]. EasyJet revealed that 82,000 customers were affected and more than 400 flights were canceled, costing easyJet £10 million in customer welfare costs and £5 million in lost revenues [35]. The budget airline added that the drone incident and subsequent disruption included the cancelation of over 1,000 flights [35]. The drone attack also cost Gatwick Airport £1.4 million. Announcing 2018 annual profits of £208 million, the chief executive of Gatwick, Stewart Wingate, stated [36]: "I fully stand by the decisions taken back then to close the airport when we came under a sustained

attack." While early estimates of the costs ran into tens of millions, the financial brunt of the incident has been borne by airlines, although Gatwick has since spent an extra £4 million on anti-drone technology, with the chief executive claiming that [36]: "We have installed some of the most sophisticated counter-drone equipment of any airport in western Europe."

The chaos at one of the world's busiest airports, being a major international transit hub, had far-reaching financial implications beyond the aviation industry. Responding and investigating the drone sightings led to policing costs of £459,000 [37]. Sussex Police said that its total costs were £419,000, including £332,000 on overtime and bank holiday pay, £52,000 on basing police officers on the site, £12,000 on mutual aid from other forces in Cambridge and Essex, £14,000 on accommodation and subsistence, £4,000 on equipment, and £5,000 on transport [25]. Surrey Police, the neighboring police force to Sussex that provided support to the investigation, also spent £40,000 in police officer overtime [25]. Crawley Member of Parliament Henry Smith, who warned Parliament in 2017 that drones could bring major disruption if steps were not taken at Gatwick Airport, said the figure was "shocking," stating [37]: "Eighteen months before the Gatwick drone incident I warned in Parliament this might well bring major disruption. This is obviously a significant cost to the taxpayers, both locally in Sussex and Surrey, as well as nationally." Following a 9-month investigation, Sussex Police admitted that without new information they had run out of realistic lines of inquiry. The overall police investigation cost a total of £790,000 [25]. Sussex Police received reports of 129 separate sightings of drone activity, with 109 of them coming from "credible witnesses," including a pilot, airport workers, and airport police [25]. The force said the investigation had involved 1,200 door-to-door inquiries along with the searching of 25 potential drone take-off and landing zones around the airport [25]. Following a lengthy legal battle, Sussex Police, which used 12 firearms officers to enter the home and arrest Mr. Gait, who was later found to have been wrongly accused of causing the chaos at Gatwick, paid £55,000 in damages, and a further £145,000 to cover legal costs [38]. The out-of-court settlement to Mr. Gait finally vindicated his involvement in the incident and added a further £200,000 to the cost to the public purse of responding to the rogue drone incursions at a major international airport.

The 3-day lockdown of London's critical aviation infrastructure highlighted that tackling a malicious drone presents a significant operational challenge. The decision to close airport operations is not taken lightly, and the initial response and post-incident investigation include mounting costs. While all in authority understood the prolonged drone incident at Gatwick to be malicious, Robert Garbett, the chairman of the British Standards

Institution Committee for U.K. Drone Standards, which advises airports on drone defense and security, said that closing the airport was a "massive overreaction" [39]. He said that the issue was not about drones but "preparedness," stating [39]: "It's not really about drones, it's about the preparedness of airports in the UK, which in the past has really not been there. They've got to take a risk-based approach." The actions of the perpetrators of the recent drone chaos at Gatwick Airport highlight a series of major vulnerabilities in the detection and neutralization of UAV threats at airports and also at other sites of critical importance to our nation's infrastructure. The shutdown at Gatwick also exposed fault lines in the multi-agency threat and risk assessment prioritization processes at airports. Assessing the risk from rogue drone incursions at airports or other physical locations, infrastructures, or premises requires the adoption of risk assessment methodologies, including identifying potential hazards and anything that may cause harm, leading to analyzing the risk and potential harm that could be done [40]. This should then be followed by action to manage and mitigate the identified risk, recording the decisions that have been taken, and regularly reviewing the assessment to ensure that it remains fit for purpose [40].

1.4 Political Protest

In a liberal, pluralist, and democratic society, a wide range of political views are acceptable and desirable, even views that may offend others, are aggressively pursued, or are highly unpopular. A sophisticated democracy allows space for these views as all citizens should tolerate and respect each other's position, learning to live side by side and accepting one another's differences. It is this tolerance and acceptance that is not only essential in a democracy but also to a successful and progressive multicultural society. However, it is important to understand that political views that are at the extreme ends of the political spectrum can cause serious issues within society as people who hold such views cannot often tolerate others. Tensions within communities can be raised when the rights and freedoms of others are not tolerated by individuals and groups with extreme views who act and behave in a manner outside of legal frameworks with the intention of forcing their beliefs on others through violence, intimidation, or provocation, causing harassment, alarm, and distress to fellow citizens.

1.4.1 Climate Change Direct Action

The United Nations report that climate change is the defining crisis of our time that it is happening even more quickly than we feared [41]. The

protection of our planet has become a global social movement centered upon the primary concern for the conservation and improvement of the natural environment. An important part of responding to the climate emergency is addressing energy supply and consumption, underpinned by reducing carbon emissions and lowering the burning of fossil fuels. As the search for greener and more sustainable environmentally friendly energy sources continues, existing power plants remain a primary target for environmental groups that are harnessing the capability of drones to carry out dangerous direct action.

In 2014, France's state-run power firm Électricité de France (EDF) announced that unidentified drones had flown over seven nuclear powers plants during October, leading it to file a complaint with the police. EDF revealed that the unmanned aircraft did not harm the safety or the operation of the power plants, stating that the first drone was spotted on October 5 above a plant in deconstruction in eastern Creys-Malville [42]. More drone activity followed at other nuclear power sites across the country between October 13 and 20, usually at night or early in the morning [42]. Greenpeace, whose activists have in the past staged protests at nuclear plants in France, denied any involvement in the mysterious pilotless flight activity. However, the environmental group expressed concern at the apparent evidence of "a large-scale operation," noting that drone activity was detected at four sites on the same day, October 19, at Bugey in the east, Gravelines and Chooz in the north, and Nogent-sur-Seine in north-central France [42]. As an independent movement, Greenpeace does not accept any funding from governments, corporations, or political parties, which means that it is free to confront governments and corporations that it deems responsible for the destruction of the natural world and push for real change [43]. Greenpeace advances the environmental cause by investigating, documenting, and exposing the causes of environmental destruction, bringing about change by lobbying, consumer pressure, mobilizing members of the general public, and taking direct action to promote solutions for a green and peaceful future [43]. Responding to the suite of sightings at nuclear plants, Yannick Rousselet, head of Greenpeace's anti-nuclear campaign, stated [42]: "We are very worried about the occurrence and the repetition of these suspicious overflights." The French nuclear safety authority (ASN) did not comment on the claims, saying only [42]: "We don't discuss matters outside our field of expertise."

France, the world's most nuclear-dependent country, operates 58 reactors and has been a leading international cheerleader for atomic energy. However, in a deal with the Greens before the 2012 parliamentary and presidential elections, President François Hollande's Socialist party promised to

cut reliance on nuclear energy from more than 75% to 50% by shutting 24 reactors by 2025 [42]. To maintain pressure upon the French government, Greenpeace has repeatedly tried to highlight alleged security weaknesses at French nuclear sites. In May 2012, a Greenpeace activist flew a paraglider over the Le Bugey plant and landed on the site, a drone being used to film the stunt [44]. In October 2017, Greenpeace activists set off fireworks inside a nuclear plant in eastern France after breaking into the facility to underline its vulnerability to attack. Greenpeace said the fireworks were set off at the foot of a spent fuel pool (SFP), where nuclear plants store highly radioactive fuel rods that are removed from reactors after their use [45]. EDF immediately refuted the report, saying in a statement that its nuclear plants were: "Safe, properly monitored and very well protected," and that it was [45] "constantly evaluating their resistance to criminal acts or terrorism." A French court later sentenced two Greenpeace activists to a minimum of 2 months in jail for breaking into the nuclear power plant in Cattenom, near the border with Luxembourg [46]. Six other protesters were handed 5-month suspended sentences and Greenpeace France was fined 20,000 euros [46]. Prosecutor Christelle Dumont stated that [46]: "Greenpeace crossed a red line. Any debate about nuclear safety must be in accordance with the law."

The arrest and conviction of Greenpeace activists did very little to dissuade the movement in France to scale back its direct action campaign against the EDF nuclear power plants. The punishments received by activists seemed only to amplify the efforts of Greenpeace, leading to the creative use of drones to deliver their direct actions. In July 2018, a Superman-shaped drone crashed into the EDF's Bugey nuclear plant in Bugey, near Lyon. Greenpeace said that it had flown the drone, piloted by one of its activists, into the no-fly zone around utility EDF's Bugey nuclear plant and then crashed it against the wall of the plant's spent-fuel pool building to demonstrate its vulnerability to outside attack [47]. Greenpeace stated that action demonstrated [48]: "The extreme vulnerability of French nuclear structures, designed in the 70s and not equipped for external attacks." The timing of the incident caused substantial embarrassment to EDF as the French parliament had been investigating nuclear security breaches for months following a Greenpeace report from October 2017 that detailed the vulnerability of EDF's nuclear reactors. While the presence of the Superman drone had no impact on the security of the installations, the vulnerability of attack from the air was evident [48]. The persistent direct action campaign by Greenpeace activists has been sustained through harnessing the innovations of drones. Environmental protestors have successfully utilized the deployment of drones to draw attention to their cause, operating under the radar of law enforcement and intelligence agencies and defeating all

measures put in place by authorities to protect critical infrastructure from hostile attack. The effective misuse of drones by environmental protestors has provided activists pursuing other single-issue causes to adopt hostile drone operations.

1.4.2 Drone Disorder

Soccer club supporter rivalries across the world are renowned for resulting in violence, intimidation, and large-scale public disorder both in and outside of the stadiums. Some of these incidents of soccer hooligan violence have led to tragedy and large-scale loss of life, resulting in new and improved measures to physically separate rival fans, underpinned by the close monitoring of their activities through the use of covert surveillance and intelligence gathering tactics once the preserve of national intelligence agencies. Joint police and soccer authority operations to safeguard the safety and security of fans and supporters are increasingly complex given the underground and clandestine activities of rival soccer hooligan firms that provoke and antagonize each other, leading to physical clashes as part of an organized and orchestrated culture of violence. For police commanders in control of operations to keep thousands of soccer supporters safe before, during, and after a match, the burden of responsibility weighs heavy on their shoulders, knowing that just a tiny spark of provocation can ignite violence leading to pitch invasions, crowd surges, and large-scale disorder, serving to threaten the safety and security of fans and supporters inside the stadium.

During a Europa League soccer match at Luxembourg's Joy Barthel stadium, a drone carrying the flag of a region disputed by Azerbaijan and Armenia flew onto the pitch, raising the security concerns amongst police commanders on many fronts. The game, between Luxembourg's F91 Dudelange and Azerbaijan's FK Qarabag, was halted for 15 minutes as the drone incensed Qarabag players, who tried to hit it with the ball as it flew over the center circle [49]. The drone was spotted carrying the flag of Nagorno-Karabakh, a disputed territory resulting in an ethnic conflict between Armenia and Azerbaijan in the 1990s. The disputed region of Nagorno-Karabakh and seven surrounding districts, which are controlled by the self-declared Republic of Artsakh, but are internationally recognized as part of Azerbaijan, led to thousands being killed on both sides during the conflict, as well as hundreds of thousands of people being displaced by the war which ended with a truce in 1994, although sporadic violence continues [50]. The soccer club FK Qarabag originates from Agdam, a now-ghost town in Nagorno-Karabakh, but moved to be based in Azerbaijan's capital of Baku in 1993 during the conflict in the region [50]. F91 Dudelange

tweeted an apology to fans over the drone incident after the game, stating [50]: "We had nothing to do with this provocation."

The rogue drone incursion at the soccer stadium was a timely reminder of the poor levels of counter-drone capabilities at sporting venues where thousands of people gather in close proximity. Following the incident, police commanders and stadium officials shared their concerns of the incident, which not only could have sparked a large-scale disorder in and around the stadium at the time, but could have also raised international diplomatic relations leading to a resurgence in violence and the renewal of a major conflict in the disputed region. Moreover, the drone incursion provided evidence of the vulnerabilities of open stadiums to future drone attacks from political activities and violent extremist and terrorist groups.

The attraction of flying a drone over tens of thousands of people attending a sports stadium to draw attention to a particular political cause or single issue appears to be a tactic for activists who are drawn by the publicity that each rogue drone incident attracts. In May 2018, authorities in the United States announced that a Sacramento resident, Tracy Michael Mapes, aged 56, had been officially charged with violating two separate Temporary Flight Restriction (TFR) areas during U.S. National Football League (NFL) football matches on November 26, 2017 [51]. Mapes was accused of flying his drone over a San Francisco 49ers game at the Levi's Stadium and dropping anti-media leaflets into the crowd. He was also accused of the same violation during a Raiders NFL game at Oakland Stadium later that same day. According to police, his drone released leaflets containing content about free speech and personal views on television being corrupt [51]. Most of the leaflets did not make it into the stadium or crowd at the 49ers game due to high winds and rain. No one was injured in the incident during which stadium surveillance cameras were able to identify the drone operator and record his license plate number as he drove away from Levi's Stadium in Santa Clara. Detectives alerted their counterparts in Oakland ahead of the Raiders game [51]. Mapes released leaflets into Oakland Coliseum and, once again, no one was affected. Officers located his vehicle as he was leaving, cited him with misdemeanor charges, and released him [51].

Despite clear evidence pointing to the danger rogue drones can pose to both athletes and fans, many professional sports clubs and venue administrators appear to continue to take little action. Lucas Le Bell, CEO and cofounder of CerbAir, who provide anti-drone solutions protecting a major French soccer club as well as prominent music festivals and political gatherings from malevolent drone intrusions states [52]: "By not putting in place appropriate airspace security above their venues, some clubs and stadiums are taking an enormous gamble." Besides the immediate physical security risks from rogue drone incursions at sporting venues, the pirate

broadcasting of sporting events by online live-streaming via drones is on the rise, proving costly to horse racing and track administrators who lose control over how races are covered and the profits that come with that control [52]. Other sporting events run a similar risk with pirated broadcasts of meetings and matches that have the potential to threaten viewership numbers and advertising revenues placing pressure upon owners of sporting venues and stadiums to invest in drone detection systems to protect their commercial interests and economic investments.

1.5 Hostile Reconnaissance and Rogue Drone Surveillance

The technical advancement of UAVs capable of carrying increasingly sophisticated imaging equipment and significant payloads is now readily available on the civilian market. The broad accessibility of drones, combined with their ever-expanding capabilities, has created new exploitation opportunities for hostile actors. A range of terrorist, insurgent, criminal, corporate, and activist threat groups have already demonstrated the ability to use civilian drones for conducting hostile reconnaissance, the term given to the information gathering activities by those individuals or groups with malicious intent [53]. Hostile reconnaissance forms a vital part of the attack planning process as actors seek to obtain a detailed profile of an identified target. Hostile reconnaissance covers a broad range of intended objectives, from identifying a specific piece of information not readily available from other open source intelligence gathering opportunities to a complex feasibility study of security measures in place at an identified target premises.

Identifying hostile reconnaissance remains integral to security operations as it very often provides the first early sign confirming the presence of a hostile threat. For rogue actors, hostile reconnaissance operations represent sensitive covert activity, being shrouded in secrecy and with the intention of capturing the information that they require to formulate attack plans while remaining anonymous. The use of drones as a tool to facilitate hostile reconnaissance with their increasing technical camera and video capacity and capability makes them highly desirable for such operations. Military forces deployed in hostile environments and conflict zones have been aware for many years of the threat posed by terrorist and insurgent groups conducting hostile reconnaissance missions, using drones to identify their positions, strength of resources, and security operations, but the use of drones as a method of gathering information has also come to the attention of civil authorities and law enforcement agencies. The National Police Chiefs Council (NPCC) in the United Kingdom has previously raised serious concerns that drones could be used to obtain information through hostile

reconnaissance to conduct all manners of operations by various actors with malicious and hostile intent [54].

The best defense against the hostile use of drones is to employ a hierarchy of measures to counter the threat that encompasses regulatory, passive, and active countermeasures [55]. The combination of these countermeasures, augmented by a counter-drone strategy as an integral component of broader security operations, will support the prevention and detection of the rogue drone hostile reconnaissance threat. However, all security postures will fail if the threat from hostile reconnaissance is not fully understood. Therefore, this chapter will examine hostile reconnaissance as an intelligence-gathering tactic, identifying current threats from the use of drones and highlighting the important consideration of countermeasures to reduce the threat and minimize the risk from future rogue drone hostile reconnaissance operations.

1.5.1 Theatres of Conflict

There are many examples of individuals using drones for reconnaissance purposes beyond authorized and accepted use, but the most serious cases have been captured in theatres of conflict where insurgent groups have demonstrated their effective adoption of UAVs for surveillance purposes. The extremist militant group Islamic State (IS) was shown to be using DJI Phantom UAV platforms in Fallujah, Iraq, from early 2014 [55]. The Phantom drone is a series produced and commercially sold online by DJI whose platforms empower them to capture images that were once out of reach [56]. DJI offers flying and camera stabilization systems that redefine camera placement and motion providing high-end professional imagery [56]. While the early insurgent demonstrations of commercially available drones appeared to be for propaganda purposes only, there is evidence that these platforms have provided actionable intelligence and target acquisition capabilities to the IS. There are some indications that the IS used hobbyist drones to gain situational awareness ahead of the campaign to capture the Tabqa military airfield in northern Syria in August 2014 [55]. Surrounding the airbase in Raqqa Province from all sides, the IS trapped 800 to 1,000 Syrian troops and airmen who had used the base to attack mainstream opposition groups in the north of the country [57]. Despite the Syrian government launching airstrikes on the IS positions, the group's fighters managed to enter the grounds of the air base and seized the critical infrastructure after many of the troops inside withdrew [58]. More than 340 IS fighters were estimated to have been killed in the offensive, in addition to 170 government soldiers, making the battle the deadliest between the jihadist movement and the Syrian government at that time of the conflict [58]. The

attack on the Tabqa airbase in eastern Syria came as the IS continued to move back towards areas it controlled north of Aleppo, using weapons the group looted from abandoned Iraqi military bases, stunning regional powers with its rapid advances [57].

In March 2015, U.S. military forces launched an airstrike against an IS militant who had been flying a UAV over Fallujah [55]. In April 2015, the IS released a video showing UAVs being used for reconnaissance and battlefield coordination during its assault on the Baiji oil refinery complex in Iraq [55]. The struggle between Iraqi government forces and Shia militia against the IS for control of the country's largest oil refinery represented a critical juncture in the conflict [59]. Although the Baiji oil refinery complex had changed hands several times, the offensive in April 2015 by the IS threatened to displace Iraqi troops and their allies and the importance of retaking the refinery would deprive the IS of a major source of revenue [59]. Islamist insurgents battled Iraqi forces for control of the oil refinery, which produced 310,000 barrels per day [60]. During the course of the fighting, 17 gas storage tanks were set ablaze [60]. Dramatic satellite images showing the oil facility with black smoke billowing from the site's buildings, the plumes of smoke so large they could be seen from space [61]. Workers who had been inside the complex, which spread for miles close to the Tigris River, were evacuated after a temporary ceasefire [61]. After months of battles and rapidly shifting lines of control, pro-government forces pushed the IS out of Baiji city and its refinery in late October 2015 [62].

During the height of armed engagement during the conflict in Iraq, it became clear to American and Iraqi commanders that the IS were using drones to help them on the battlefield. In March 2015, General MacFarland and American military commanders in Baghdad received an intelligence report that the IS had posted a surveillance video online that had been taken by a small drone [63]. The video footage showed a newly created series of bases in northern Iraq where American and Iraqi forces were stationed. Just days after the video was uploaded, a Katyusha rocket landed in the middle of an outpost of more than 100 American Marines, killing one who was rushing to get others to shelter in a nearby bunker [63]. The strike was so accurate that military officials described it as a "golden shot" to pierce the defenses put in place, and there was speculation that a drone was used in the targeting [63].

The use of drones in theatres of conflict is now a permanent feature of terrorist and insurgent activity, with military forces deploying sophisticated drone-detection systems to mitigate the risk from hostile drone surveillance. The success of drone operations has rapidly spread between terrorist and insurgent groups across the world. Insurgent groups have many of the same capabilities and intentions as terrorist organizations and the use of

drones have the potential to become a significant component of insurgents' armories [55]. Obtaining aerial reconnaissance to support attack planning capabilities marks a step change for many insurgent groups who continue to develop their use of drones. The IS first used drones to film suicide car bomb attacks, which militants posted online for propaganda purposes [63]. Modern terrorism and insurgency has rapidly evolved becoming increasingly nonphysical, with vulnerable "home-grown" citizens being recruited, radicalized, trained, and tasked online, influenced by dramatic propaganda media content glorifying their operations captured by drones and disseminated in the virtual and ungoverned domain of cyberspace. It would be unwise to underestimate how the Internet has rapidly changed, and continues to change, the very nature of terrorism and insurgency, whose operatives understand the power of online communications, especially those professionally edited with footage from their operations captured by drones.

1.5.2 Drone Surveillance

The image capture capabilities of drones make them a perfect tool for covert and overt surveillance. One would think that drones hovering at a window of a company during a board meeting would attract some attention, but it is not inconceivable that a drone can attach itself to the side of any building and remaining motionless where it would become inconspicuous to those inside [64]. Drones equipped with cameras are by far the most common risk to business and concerns of drone-enabled industrial espionage are growing. There are many security professionals who believe that drones pose no risk to their secret and sensitive commercial operations, but drones equipped with the latest camera technologies and video analytics capabilities are able to capture activity at business meetings. The risk includes revealing all presentation information, breaching security measures designed to protect new prototypes, patents, or prelaunch of products and services. This presents a real drone business espionage problem as UAV surveillance can also monitor business executives and detail the logistics of product movement. The presence of large-scale industrial environments makes concealing a small drone in a factory, warehouse, or distribution center notably easy [64]. Businesses have many locations that provide valued and viable targets for drone surveillance missions including testing tracks for vehicle prototypes and research laboratories [65]. Drones that operate in the airspace above a manufacturing or production plant also present a risk for stock theft or sabotage, raising concerns among security experts that state-sponsored drone surveillance operations presents a threat to a nation's economic well-being.

There have been isolated examples of drones being used to obtain commercially sensitive information, such as drones flying over the filming of *Game of Thrones* in Ireland, Apple's new campus site being built in Cupertino in the United States, and the BAE Systems facility in northern England that builds submarines for the Royal Navy [55]. Organizations that are aware of an attack may consider it unwise to disclose that they have been a victim due to fear of loss of confidence in their security posture and damage to their reputation. Moreover, many organizations, given the reluctance by some security professionals to recognize that drone espionage is a clear and present danger, may not know if they have been attacked and had valuable information and intellectual property stolen. The broad range of threat scenarios whereby drones are integrated into corporate espionage operations, including the threat of cyber offensives and drone-enabled spear phishing campaigns, suggests the threat of industrial espionage is an emerging threat vector which requires a dedicated response.

The threat of drone-enabled industrial espionage is not limited to the sensitive operations of organizations in the defense sector or high-tech companies developing the next generation of computer software; even the sports industry has been the target of rogue drone surveillance. Horse racing in particular over recent years has been subject to all manner of UAV-related threats, with crime gangs piloting them over courses to give gambling punters an unfair advantage while placing bets before footage is screened to bookmakers. The drone surveillance at horse racing events serves to undermine bookmakers and broadcasters and, by extension, threatens the future of the sport given the levels of revenue and sponsorship received from media and gambling industries. However, the criminal use of drones is not the only threat posed by UAVs to horse-racing events. During the 2019 U.K. Grand National at Aintree, one of the largest horse-racing events in the world, organizers recruited the services of a specialist drone surveillance team to keep watch amid fears UAVs may put at risk the safety of very important people (VIPs) arriving by helicopter [66]. The Jockey Club, owners of the Aintree racecourse, hired the drone spotters after fears were expressed for the safety of helicopters ferrying trainers and wealthy racegoers to courses as many VIPs, including members of the British Royal Family, opt for a 90-minute helicopter flight from London directly into the racecourse [66]. To mitigate the threat posed by drones to the Grand National event, the U.K. Civil Aviation Authority (CAA) imposed airspace restrictions prohibiting the use of UAVs below 2,000 ft [66].

While rogue drone surveillance at large sporting events presents a threat to their continued commercial success, it is the impact of the use of UAVs on the privacy of individual citizens that represents a key concern to the public. The hostile use of drones to capture imagery of private citizens

remains a lively social, political, and legal debate. The extent of the invasion of privacy by the use of drones is best evidenced through paparazzi drones, used by photographers and videographers, being supported by media organizations and fueled by consumer demand for the latest celebrity news. Drones have become Hollywood's most-feared gate-crashers with long-lens cameras and video recorders hovering over the private retreats of famous film stars and celebrities with their lenses peering through open windows into bedrooms. The paparazzi using drones, the so-called "Dronerazzi," has fast become a nuisance in the celebrity world, with reporters using drone technology for advanced monitoring and surveillance, learning of celebrity whereabouts and capturing invasive footage and snaps that otherwise would have been impossible [67]. Robert Izzard, a veteran bodyguard who has protected many of Hollywood's biggest stars, revealed the serious security concerns of celebrities, stating [68]: "Even if a paparazzo doesn't intend to publish a drone's photos of a star, they can still legally fly a drone over their house and learn what time they wake up, when they walk their dog, when they take their kids to school, and use that information to follow them and take photos. That's an incredible intrusion of privacy, and deeply disturbing. What's to stop deranged stalkers doing the same thing, even if they don't intend to publish any photos, just so they know where a celebrity is at any time of day?" Despite their many positive attributes, drones have a dark side, proving themselves to be disruptive and sinister surveillance tools in the hands of pilots with malicious intent whose activities threaten the very social acceptance and continued proliferation of UAV technology.

1.6 Adoption of Drones for Organized Crime

On a global level, many preexisting crimes are developing into significant international threats by taking advantage of advances in technology and the borderless nature of our interconnected world [69]. Serious and organized crime features a great variety of criminal activities, which are increasing in complexity and scale. Criminals quickly adopt and integrate new technologies into their modus operandi or build brand-new business models around them [70]. The use of new technologies by organized crime groups has an impact on criminal activities across the spectrum of serious and organized crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as the adoption and integration of new tools to accelerate and amplify criminal operations, which include the introduction of UAVs. According to Europol, Europe's leading law enforcement agency, organized crime groups involved in drug trafficking will likely invest in drone technology

for trafficking purposes in order to avoid checks at border crossing points, ports, and airports [70]. However, the potential user cases of drones for the commission of all manner of crime types are almost limitless. From human trafficking gangs monitoring border patrols to transporting contraband and pedophile rings sharing images captured from school playgrounds, drone technology is facilitating new ways to commit traditional crimes more effectively. As UAV technology continues to develop and prices continue to diminish, the criminal adoption of drones will increasingly present complex challenges for police first responders, critical incident commanders, and post-incident digital investigation specialists [69]. The proliferation of the criminal use of drones is set to have an impact upon the full operating landscape of the law enforcement community.

1.6.1 Drone Drug Trafficking

The global drug trafficking market is worth an estimated $652 billion and represents approximately one-third of the total retail value of all transnational crimes [71]. Cannabis is responsible for the largest share of drug trafficking, followed in order by cocaine, opiates, and amphetamine-type stimulants [71]. Amphetamine-type stimulants and cannabis are produced all over the world, while the production of cocaine and opiates is concentrated in South America and Afghanistan. Drug trafficking organizations, guerrilla groups, and terrorist organizations are all involved in drug trafficking. In recent years, organized crime groups in West Africa have increased their control of the drug market in the region, and the volume of heroin trafficked from Afghanistan through East Africa continues to escalate [71]. Drug markets remain the largest criminal markets across Europe. According to Europol, more than one-third of the criminal groups active in Europe are involved in the production, trafficking, or distribution of various types of drugs. The trade in drugs generates multibillion euro profits for the groups involved, a retail drug market estimated to be worth at least €24 billion a year [70]. The immense profits generated from the trade in drugs fund various other criminal activities allowing organized crime groups to thrive and develop their criminal enterprises at the expense of the health, prosperity, and security of citizens. Organized crime groups involved in drug trafficking heavily rely on corruption to facilitate their trafficking activities. They also make use of fraudulent documents such as fake imports or company registration certificates to import illicit drugs among legal goods to procure preprecursors and purchase equipment used as part of production processes [70]. The prohibitions on drugs have created perverse economic incentives that make combating drug producers and distributors extremely difficult. The high black-market price for illegal drugs has generated huge profits for

the groups that produce and sell them, income that is invested in buying state-of-the-art weapons, hiring gangs to defend their trade, paying off public officials, and making drugs easily available.

Europe remains confronted by a rapidly evolving drug market. The increased potency and purity of illicit drugs, the record numbers of seizures, and the increased production in the EU all indicate that the availability of illicit substances is growing [72]. Paraskevi Michou, the Director-General for Migration and Home Affairs at the European Commission, has stated [72]: "Organised crime benefits significantly from the drug trade but, more worryingly, these criminals have shown determination and ruthlessness in trying to grow their market share." The violence and intimidation used by Europe's organized crime groups trafficking illegal drugs is severe but is dwarfed by the death and destruction in Mexico. In fear of losing ground on the war on drugs, U.S. President Trump and his military leaders in 2020 announced a new operation to combat Mexican drug cartels and other Central and South American narcotics organizations. U.S. Joint Chiefs of Staff General Mark Milley stated that [73]: "We will defend our country regardless of the cost." U.S. law enforcement agencies are challenged on many fronts in their efforts to combat the South American drug cartels that have embraced technical innovation and acquired access to sophisticated equipment, allowing them to maximize the production output of individual illegal drug cultivation sites. Large-scale laboratories manufacturing synthetic drugs now feature advanced chemical equipment and, given their appetite to reduce operating costs and maximize profits, transnational crime organizations have invested in drone technology to transport narcotics, a tactic of drug trafficking that is becoming increasingly prevalent.

In April 2015, 28 pounds of heroin strapped to a drone made it across the U.S.-Mexico border near Calexico, making it the first cross-border seizure by U.S. law enforcement involving the new smuggle-by-air tactic. U.S. Attorney Laura Duffy stated [74]: "With border security tight, drug traffickers have thought of every conceivable method to move their drugs over, under and through the border. We have found their tunnels, their Cessna's, their jet skis, their pangas, and now we have found their drones." Two men pleaded guilty to retrieving the drone delivered drugs near state Route 98 in Imperial County, a pickup that was captured on border patrol cameras resulting in police officers stopping the suspect vehicle where they found a duffel bag full of drugs in the trunk that later tested positive for heroin. Responding to the guilty plea of the suspects, Ronnie Martinez, assistant special agent in charge for Homeland Security Investigations in El Centro, stated [74]: "The use of drones to smuggle drugs across the U.S.-Mexico border is an emerging threat, which fortunately, has not proven to be a lucrative

criminal enterprise in the Imperial Valley as various law enforcement agencies along the border have banned together to wipe out the smugglers." Despite the best efforts of U.S. law enforcement agencies to prevent the smuggling of drugs by drone through U.S.-Mexico borders, which has included the creation of specialized units to detect and combat all aerial drug smuggling, the use of drone as mules to transport illegal drugs continues to rise. In January 2015, a drone hauling methamphetamine crashed in a parking lot of a Tijuana shopping center in Mexico, located 2 miles from the U.S. border. Mexican law enforcement revealed that the drone was loaded with 7 pounds of drugs and was likely being ferried from neighborhood to neighborhood [74]. In August 2017, border patrol agents intercepted a drone-borne drug shipment when an agent in San Diego County heard the buzzing of a remote-controlled aircraft coming over the border fence and contacted his fellow agents, who then found and arrested a 25-year-old man carrying 13 pounds of methamphetamine that he had removed from the drone [75].

Recognizing the growing threat of drug-carrying drones, Paul Knierim, the Drug Enforcement Agency (DEA) deputy chief of operations, told a Senate Judiciary Committee Subcommittee on Border Security and Immigration in 2019 that [75]: "Mexican Transnational Crime Organisations (TCOs) exploit various aerial methods to transport illicit drugs across the southwest border. These methods include the use of ultralight aircraft and unmanned aerial systems and drones to conduct air drops. Ultralights are primarily used to transport marijuana shipments, depositing the drugs in close proximity to the southwest border. Currently, unmanned aerial systems can only convey small multi-kilogram amounts of illicit drugs at a time and are therefore not commonly used, though there is potential for increased growth and use. Mexican TCOs also use drones to monitor the activity of U.S. law enforcement along the southwest border to identify cross-border vulnerabilities." The testimony of the DEA deputy chief of operations followed the address to the nation on the crisis at the border by President Trump, who acknowledged the scale of drug trafficking from Mexico, stating [76]: "Our southern border is a pipeline for vast quantities of illegal drugs, including meth, heroin, cocaine, and fentanyl. Every week, 300 of our citizens are killed by heroin alone, 90 percent of which floods across from our southern border. More Americans will die from drugs this year than were killed in the entire Vietnam War."

The use of drones to smuggle drugs did not come as a strategic surprise to U.S. law enforcement authorities as Mexican cartels have used this tactic to transport narcotics to other South American nations since 2010 [77]. By 2012, drone use along the border was highly prevalent, evidenced by the

United States' interception of 150 drones carrying an estimated 2 metric tons of drugs, primarily marijuana, cocaine, and heroin [77]. In November 2016, Colombian police seized 130 kg of cocaine and a drone used by narcotraffickers in the Bahía Solano sector of Chocó, allegedly used to send cocaine shipments to Panama [78]. The seizure was carried out in the area called Playa Huaca, where authorities were able to seize parts of a drone that had the capacity to transport 10 kg of cocaine to Panama. The discovery of the drone provided the first instance in which commercial UAVs have been identified as a viable trafficking method in the country, being capable of traveling up to 100 km in a single trip [78]. Authorities indicated that the use of drones to traffic narcotics was likely developed by the Clan del Golfo, the largest criminal gang in Colombia dedicated to drug trafficking, representing a significant shift in tactics for transnational criminal organizations operating in Colombia [77].

1.6.2 Contraband Drones

The trafficking of drugs across borders using drones by organized crime groups is not the only threat that UAVs pose to the supply of illegal drugs. In 2016, Daniel Kelly, aged 27, formerly of Lewisham, southeast London, used a drone to fly contraband into prisons, becoming the first person in the United Kingdom to be jailed for the crime [79]. Police officers from Kent Constabulary revealed that Kelly had used the remote-control drone to smuggle items, including tobacco and the psychoactive drug Spice, into two prisons in Kent and one prison in Hertfordshire. Jailed for 14 months at Maidstone Crown Court in Kent after admitting conspiracy to project an article into prison, Kelly was arrested after a police patrol spotted a car parked near Her Majesty's Prison (HMP) Swaleside on the Isle of Sheppey in Kent, where he was seen running and climbing into the front passenger seat before the car sped off, later being found at a holiday park in nearby Leysdown [79]. The drone used in crime was discovered in the car and seized by police officers; the drone was originally white but had been spray-painted black with its lights taped over. The police investigation also revealed that there were two unsuccessful attempts to fly the drone into HMP Wandsworth in southwest London. Investigating officer Detective Constable Mark Silk stated [79]: "Psychoactive substances and tobacco have an inflated value in prison and this can lead to offences being committed within. This places both inmates and prison staff at risk."

The arrest and conviction of the first person to smuggle drugs into a U.K. prison by use of a drone failed to prevent a surge in similar offences. In 2017, eight members of a criminal gang that used drones to airlift £500,000 worth of drugs into prisons were given jail terms ranging from 3 to 10

years [80]. Over a 2-year period, drone pilots, drivers, and lookouts had conspired with prisoners to smuggle drugs into seven jails, including HMP Birmingham and HMP Liverpool [80]. Remote-controlled drones, equipped with a fishing line and hooks, were flown to cell windows where inmates, in contact with the pilot, used tools such as extendable broom handles to retrieve smuggled items [81]. During the investigation, 11 drones, including some that had crashed, were seized during police inquiries into flights that also targeted HMP Wymott in Lancashire, HMP Hewell in Worcestershire, HMP Risley in Cheshire, and HMP Oakwood and HMP Featherstone in Staffordshire [80]. Craig Hickinbottom, aged 35, was a prison inmate at HMP Featherstone in Staffordshire, and later HMP Hewell in Worcestershire, who directed the large-scale and persistent operation from behind bars and was sentenced to 7 years' imprisonment after admitting four counts of conspiring to bring contraband into prison and conspiracy to supply psychoactive substances [81]. Drone pilot Mervyn Foster received a sentence of 6 years and 8 months for his part in the enterprise [81]. Passing sentence, Judge Roderick Henderson said [81]: "Prisons are difficult enough places to run. They contain people who are dangerous and vulnerable. Supplying things into prison that should not be there—drugs, phones, tools and the like—threatens proper management and creates real risks of violence and loss of control and discipline. To do that is desperately serious."

At a later trial of a further 13 conspirators connected to the drone-enabled supply of drugs in prisons, Judge Simon Drew, QC, said [80]: "Each of you falls to be sentenced for your part in conveying controlled drugs, mobile phones and sim cards into prisons up and down the country. The method you chose to do this was both carefully planned and executed. Each of you played a part in a wider conspiracy which resulted in approximately 100 separate deliveries. This was a sophisticated commercial operation and due to the high value placed on drugs and mobile phones in prisons, designed to make those of you who ran the operation hundreds of thousands of pounds in profit." The prosecution case also provided evidence that the increase of illegal drugs and the unauthorized mobile phone use in prisons had caused heightened levels of violence, an increase in self-harm and deaths, and allowing witness intimidation and illegal financial transactions [80]. The convictions of the criminal gang exposed the reality of the illegal use of drones for transporting drugs into prisons, but the phenomenon was not just restricted to the United Kingdom, as similar incidents have been recorded in Canada, Brazil, and several European member states. The proliferation of drone use to smuggle drugs into prisons provides further evidence that law enforcement agencies in many jurisdictions across the world had to respond to an increasing number of incidents where criminal offenses were being facilitated by the illegal use of drones.

1.7 Terrorist Threat from Drones

In a world of startling change, the first duty of government remains protecting the safety and security of its citizens. Today, many nations across the world are both more secure and more vulnerable than ever before: more secure, in the sense that they do not currently face, as nations have so often in the past, a conventional threat of attack on their territory by a hostile power, but more vulnerable, because their nations are increasingly open societies, in a world that is more networked than ever before. As a direct result, nations across the world face a different and more complex range of threats from myriad sources: terrorism, cyberattack, unconventional attacks using chemical, nuclear, or biological weapons, as well as large-scale accidents, natural climate change hazards, and pandemics. Any of these can result in grave damage to citizens and a country's economic well-being, as well as impact upon their international relations with other states. New threats can emerge from states, but also from non-state actors: terrorists (home-grown or overseas), insurgents, or criminals, as well as the security of energy supplies, which increasingly depends on fossil fuels located in some of the most unstable parts of the planet. Governments know, for example, that international terrorist groups are determined to exploit their increasing levels of openness to attack, plot against, and kill innocent citizens to or inflict mass disruption to services to destabilize a nation's economy to progress their political, ideological, or religious motivations.

Given the persistent severity of the terrorist threat, governments across the world no longer accept that they should simply prepare to respond to the types of terrorist attacks already encountered. All in authority now recognize that this reactive posture will not preserve their national security, and so an increasingly proactive and creative approach has been implemented, dedicated to identifying new and emerging terrorist threat vectors, founded upon the security principles of preparedness and assessing risk and managing the consequence of past, present, and future terrorist events. This new proactive posture now forms an essential part of tackling international contemporary terrorism. One such emerging threat is the adoption of drones as a tactical attack planning option for terrorists to cause mass disruption, damage economic stability, and threaten security. The adoption of drones for terrorist purposes is a significant security concern for governments across the world. Reinforcing the concern of this new threat, in August 2019, the European Union Security Commissioner Julian King warned that drones could be used for acts of terrorism, stating that [82]: "Drones are becoming more and more powerful and smarter which makes them more and more attractive for legitimate use, but also for hostile acts." The warning followed the publication of a leaked secret report in December 2018 from France's Anti-Terrorism Unit (UCLAT) to the country's Special Committee

on Terrorism. The report [82] warned of: "a possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents." The terrorist use of UAVs has already materialized in theaters of conflict with devastating impact, confirmed by Assistant Commissioner Neil Basu, the head of the Counter Terrorism Command at the Metropolitan Police, stating [82] that drones "have been used on the battlefield and what's used on the battlefield will eventually be adapted to be used on domestic soil." Moreover, Catherine De Bolle, the executive director of Europol, has stated that a major security concern for Europe and other nations across the world remains the return of Foreign Terrorist Fighters (FTF) from theaters of conflict with combat and technical expertise [83]. Europol also reveals that terrorist attacks across Europe have shown a recurrent targeting of public spaces, and, as terrorist organizations innovate their techniques, Europol and Interpol have stated that the response needs to be as equally innovative to mitigate emerging homeland security threats, which includes those posed by the terrorist use of UAVs. While the threat landscape from UAVs is diverse, the greatest concern among the international security community is the expectation that terrorists and terrorist groups will flirt with new technologies in an attempt to harness the power of drones to attack crowded public spaces [84].

1.7.1 Terror Tactics

Terrorists and their organizations target and train which tactic they wish to deploy. There are many factors that influence this decision, which includes the nature of the intended target, the abilities of its operatives, and the hostile environment in which they operate. Whatever target is chosen, the terrorists are spoiled by an abundance of methods at their disposal to bring about a successful conclusion and are very often only limited by their creativity. Over time, either by trial and error or by accident rather than design, terrorist organizations develop a preferred method of operating, a tactic that they have come to trust and have refined through experimentation and learning from operational experience. The threat from contemporary international terrorism embraces a variety of tactics where no single technique can be solely attributed to a specific terrorist group. It would be unwise to believe that a particular terrorist group operates in a certain way as terrorists are continually seeking new and innovate ways in which to deliver death, disruption, and destruction. Contemporary terrorist attack plans continue to evolve, seemingly sharing the aim of wanting a lot of people watching and a lot of people dead [85]. To accomplish these objectives, and to outbid rivals for the spotlight, entities like the IS seek to use more lethal methods of attack and to execute people in shock-inducing ways [86]. For

a number of terrorists operating in today's media-saturated environment, novelty is sought out as a form of distinction and surprise. Using new attack methods is seen as a way to create more casualties as well as generate increasing levels of media coverage, attracting international attention to their particular cause. One of the novel platforms with which terrorists have been experimenting to diversify and bolster their capabilities is the use of drones. The terrorist interest in drones is nothing new, as the following series of examples bring the utility, attractiveness, and future potential of UAVs as a platform for terrorists into focus.

On March 20, 1995, the Japanese cult Aum Shinrikyo (Supreme Truth), motivated by an apocalyptic ideology, placed containers of the toxic Sarin gas on five trains of the Tokyo underground network [87]. The trains were destined to stop at the Kasumigaseki Station, which serviced many government offices [88]. Twelve people were killed in the attack and 5,500 commuting citizens were wounded [88]. The police counterterror post-incident investigation of the incident focused upon the attack-planning activities of the terror group, informed by intelligence gained from the arrest of more than 400 cult members [89]. Police detectives discovered that the attack had been meticulously planned, but the final execution of the operation was hurriedly brought forward as members of the cult believed that the authorities had become aware of their activities [88]. Police officers also found that the Sarin gas used in the attack was not pure, and its distribution in polythene bags was largely ineffective, as they had been punctured [88]. Officials also believed that minor adjustments to their terror-attack plans would have resulted in many more deaths. Police detectives also found that, 2 years earlier, in 1993, in preparation for an assassination plot against a rival leader, the Japanese terror group had begun experimenting with a new way to deliver the deadly Sarin gas [86]. The new delivery mechanism under development was a remote-control helicopter, with Aum Shinrikyo's goal being to attach an aerosol dispersion device to the remote-control helicopter so it could be used in the attack [86]. The attack was finally delivered by using a truck option instead because the helicopters crashed during testing [86]. Although the group never used the helicopter component during the final operation, it provides insights to the commitment and creativity of the terrorist group's intention to deliver mass murder by utilizing the capacity and capability of UAVs. This case is the first known instance of a terrorist group attempting to use an unmanned aerial system (UAS), and the first known attempt by a terror group to weaponize such a device. Chizuo Matsumoto, the half-blind guru who led the Aum Supreme Truth cult under the name Shoko Asahara, was arrested in the wake of the Sarin gas attack. He was later sentenced to death for multiple crimes and was executed on July 6, 2018 [89].

In 1997, 2.5 years after Japan's Sarin terror attack, a small group of elite Israeli naval commandos from unit Shayetet 13 were finalizing their preparations for a sensitive operation that they were about to conduct in Lebanon [90]. Speculation about their mission suggests that they were to assassinate a senior Shia Muslim cleric of the Hezbollah movement [91]. After disembarking from their entry craft on Lebanon's coast, located south of Sidon between the towns of Loubieh and Ansariya, the Israeli commandos made their way to the mission's objective when they were intercepted and ambushed by local fighters loyal to the Shia militant group Hezbollah [86]. The fighters were prepared for the Israeli commando incursion, as Hezbollah had developed the ability to gain access to and observe Israeli UAS feeds, which at the time were not sufficiently encrypted [86]. Twenty years after the event, the Israeli Defense Forces finally confirmed that Hezbollah had been able to intercept intelligence while being transmitted from Israeli military drones hovering overhead the target site area days before the attack, providing advance knowledge of the naval commando operation, which resulted in the death of 12 Israeli naval commandos [91]. The successful interception of drone communications provided evidence of the increasingly sophisticated capabilities of the military wing of Hezbollah, committed to the armed resistance for the state of Israel with the aim to seize all Palestinian territories and Jerusalem from Israel. Translated as the "Party of God," Hezbollah remains one of the most infamous terrorist organizations operating in the world today [92]. Proscribed as a terrorist organization in many nations across the world, membership and engagement with its activities are outlawed. Established in 1982 in Lebanon and originally the militant wing of a religious group, the Shia was designed to provide a proactive arm in the protest against social and political deprivation and has expressed its objectives of wishing to remove foreign influences from Lebanon to create an independent and Islamic Lebanon [88].

The interest shown by terrorist groups operating across the world in adopting and intercepting UAS to bolster their operational capabilities suggests that their development for terrorist purposes was already on the radar of attack planners before the tragic events of September 11, 2001, in the United States. In the aftermath of 9/11, a group of friends residing in Virginia, the United States, conspired to provide material support to the Pakistani terrorist group Lashkar-e-Taiba (LeT). Arrested by the Federal Bureau of Investigation (FBI) in 2003, the "Virginia Jihad Network" was charged with several terrorism-related offenses for activities that included the acquisition of sensitive technology to assist and enhance the performance of UAS on behalf of LeT. The UAS dimension of the Virginia Jihad Network primarily involved three individuals, including U.S. residents Ali Asad Chandia and Seifullah Chapman, and Mohammed Ajmal Khan, an LeT operative based

in the United Kingdom. On 9/11, Chapman was firing weapons and performing military drills at a training camp in Pakistan run by LeT. After 9/11, Chapman returned to the United States, staying in touch with contacts he had made in Pakistan [93]. Chandia, a school teacher from Maryland, had also made a trip to Pakistan, spending 3 months in the country between 2001 and 2002 where he met and allied with Khan [94]. Described as the global quartermaster for LeT, Khan used millions of pounds raised by supporters in the United Kingdom to purchase Kevlar body armor, firearms, and high-tech surveillance equipment, which were funneled to rebels in Afghanistan and Pakistan [95]. While Khan was the driving force behind the acquisition of the sensitive technology and was the individual who communicated with U.S. companies to acquire it, Chapman paid for some of the products, and Chandia supported Khan's efforts to acquire and ship the material overseas [86]. Early on in the process, Khan disclosed to his fellow accomplices that he was purchasing the material for LeT, a terrorist organization originally located in the Lahore region of Pakistan and seeking independence for Kashmir by creating an Islamic state. At the time that the Virginia Jihad Network was in contact with LeT, it was believed to be the largest and most active militant group located in Lahore. LeT, translated from Arabic as the "Army of the Righteous" or the "Army of the Pure," was formed in 1990 to support the military activities of other terrorist groups in Pakistan and Afghanistan, conducting a series of attacks on Indian armed forces in Jammu and Kashmir [96]. LeT was distinguished from other terrorist groups operating to liberate Kashmir for two reasons: first, because its operations conducted against security forces are well-planned and executed, and second, for its ruthless and bloody involvement in numerous massacres of innocent and unarmed non-Muslim villagers [96].

To support LeT terrorist missions, in December 2002, Khan purchased an MP-1000SYS airplane control module from Vesta Technologies [97]. According to the testimony of Cindy Reish, the general manager of Vesta Technologies, provided at the trail of the terrorist cell, and being supported by evidential documents regarding the transaction maintained by Vesta Technologies, the MP-1000SYS was a stability and control computer that can be programmed to fly an airplane with a 10 to 12-ft wingspan using Global Positioning System (GPS) coordinates [97]. The unit controls altitude, speed, and navigation to programmed waypoints and can also be programmed to turn a video camera on and off when the airplane reaches certain locations [97]. The court heard that the majority of Vesta's customers for this technology were universities and government, including NASA and the military, and that common applications of the technology were for use with model airplanes equipped with video devices to monitor forest fires, property boundaries, gas lines, or livestock in remote or inaccessible

areas. From this evidence, the court found that the procurement of the model airplane autopilot module equipment was for LeT's military use in Kashmir [97]. The counterterror operation mounted against the Virginia Jihad Network resulted in the successful conviction of nine terrorist cell members and was an important development in measures to counter the proliferation of drone-related equipment to theaters of conflict by the U.S. government. The investigation also illustrated that LeT had been interested in acquiring drones and technology designed to boost their performance since at least 2002 and that the group leveraged a network of U.S. residents to acquire this type of advanced technology directly from U.S. companies. LeT's attempt to acquire UAS-affiliated technology was not a surprise to the global intelligence agency community, as it had previously published an article in July 2000 that claimed that it was already using UAS and had the capability to manufacture them [86].

Despite disrupting the acquisition of drone-related technology, U.S. security forces were unable to prevent the terrorist threat posed by the use of drones in the theater of conflict. The IS first used drones to film suicide car bomb attacks that militants posted online as part of their propaganda campaigns to raise awareness to their cause and to recruit and radicalize others to their ranks [98]. As their use of drone technology advanced, American and Iraqi military commanders revealed that IS drones were employed to support direct action on the battlefield [63]. Throughout the summer of 2016, American troops in Iraq and Syria reported seeing small drones hovering near their bases and around the front lines in northern Iraq [63]. The commercially available drones were being deployed for surveillance and reconnaissance by the IS, which also called on their followers to implant small store-bought drones with grenades or other explosives, directing recruits to use them to launch attacks on crowded places at the Rio Olympic Games [63]. While no such attacks occurred during the Olympics, security forces countering the threat from the IS were alerted to the potential risk from deadly and determined drone strikes. When Kurdish forces fighting the IS in northern Iraq shot down a small drone the size of a model airplane in 2016, they believed that it was like the dozens of drones that the terrorist organization had been flying for reconnaissance in the area [63]. Seizing the drone and transporting it back to their outpost for further examination, the captured drone was thought to be able to provide intelligence on IS drone operations. But as they were taking it apart, the small improvised explosive device (IED) contained inside detonated, killing two Kurdish fighters in what is believed to be the first time that the IS has successfully used a drone with explosives to kill troops on the battlefield. The drone IED attack was followed by further IS drone operations, prompting American commanders in Iraq to issue a warning to forces fighting the group to treat

any type of small flying aircraft as a potential explosive device. For some American military analysts and drone experts, the incidents confirmed their view that military authorities were slow to anticipate the terrorist adaption of drones as weapons.

Based on the experiences of coalition military leaders in Iraq and Syria, it was right to believe that drones would continue to present a security challenge in theaters of conflict, as well as an attack planning option for domestic terrorist groups. On August 4, 2018, as Venezuelan President Nicolás Maduro addressed a military parade in Caracas on Avenida Bolivar, one of the capital's main thoroughfares, the sound of an explosion suddenly scattered civilians and soldiers alike [99]. State news cameras and social media at the event captured fragmented images of mass confusion—smoke rising above the city, a formation of soldiers scattering, and bodyguards leaping to shield the president [100]. Only later would the story be pieced together: two small drones flying over the event had exploded. Neither was close enough to deliver lethal damage, although seven members of the Venezuelan National Guard were injured [100]. In the aftermath of the attack, dozens of people were arrested as Venezuelan officials launched an investigation to work out who had orchestrated the apparent assassination, with the police and security force operation identifying the group, which included defectors from the Venezuelan military whose was aim to kill President Maduro [100]. The plan was believed to have been foiled by the presidential security guards who caused the drones to explode prematurely by activating the cell phone signal blockers that protect the president, causing the blasts. The failed assassination attempt was alarmingly ambitious. The attack instantly made protecting heads of state even more complex, so varied are government leaders' schedules and public appearances. Not only did the assassination attack plan provide evidence that drones could be preprogramed to swoop in from almost any direction, but they could also be used by anyone with the means to buy them. The attack also showed that threats from the sky were no longer the exclusive domain of nation-states, with weaponized drones now being firmly in the hands of nonstate actors.

1.8 Adaption of Drones for Cyberattack

The development of the internet and digital technologies represents a major opportunity for nations across the world, transforming businesses and providing new tools for everyday communication. It has been estimated that 60% of the global population in 2020 were using the Internet, a 1,500% increase in population use since 2000 [101]. The use of the internet has been rapidly accelerating over recent years, amplified by the development

of increasingly mobile telecommunications, with 3.5 billion people across the world now having use of a smart cell phone [102]. The improvements to internet coverage and access across the world has resulted in more people spending increasing amounts of time online, undertaking a greater range of online transactions and social networking communications. In terms of business, consumers worldwide spent $3.46 trillion online in 2019, up from $2.93 trillion in 2018, maintaining the expected 18% year-on-year growth in online global retail spending forecasted for the next 5 years [103]. With an estimated 2.89 billion people using the online social networking services of Facebook, including WhatsApp, Instagram, and Messenger, each month, internet activities have now become central to the very way in which many people live their lives in modern societies [104].

While the internet has positively enriched societal communications and economic opportunities, these technological advancements have changed, and continue to change, the very nature of crime, serving to breed a new sophisticated and technically capable criminal. The nature of some traditional crime types has been transformed by the use of computers and information communications technology in terms of their scale and reach, with threats and risks extending to many aspects of citizens' social lives. New forms of criminal activity have also been developed, targeting the integrity of computers and computer networks. Threats exist not just to individuals and businesses, but also to national security and critical infrastructures. Furthermore, the borderless nature of the phenomenon of cybercrime means that a nation's security or an individual's privacy can be targeted from jurisdictions across the world, making law enforcement particularly challenging. The new features of crime brought about as a result of the development of cyberspace have created a new police and security discipline of cybercrime, and the purpose of this section is to examine how UAVs are now being adapted to support all manner of cyberattacks.

1.8.1 Cyber Threats Take Flight

A growing concern among cyber security policymakers is the adoption of the illegal use of UAVs, which is now a pressing security threat across the world as terrorists, activists, and criminals are adopting drone technology and developing ways in which to commit crime and terrorism. As drones continue to evolve from novelty items to a ubiquitous business tool, resourceful cybercriminals performing network intrusions may also see an opportunity to leverage drones' proximity to homes, businesses, critical infrastructures, and defense sector premises to turn the machines into a jumping-off point to illegally access networks and systems, thus creating a new category of the infection vector of cybercrime.

The use of drones as rogue Wi-Fi access points may be one of the most simplistic yet effective tactics for targeting individuals. Cyber researchers suggest that drones equipped with a device like a Wi-Fi Pineapple can be placed in proximity to a target's premises and can be used to harvest credentials, perform man-in-the middle attacks, and conduct network reconnaissance [105]. Even users connected to legitimate company access points could conceivably be forced to connect to the drone's Wi-Fi if the target's network does not prevent forced deauthentications. This threat is further amplified by the growing culture of Bring Your Own Device (BYOD) with organizations flooded by employees who are encouraged to make use of their personal devices to access enterprise systems and data providing further connections for cyber drone hackers [106]. To commit their cyber intrusions, drones may park themselves on the roof of a building or other concealed location, including those that are in enclosed areas that are otherwise off-limits to foot and vehicle traffic, which describes many defense sector installations. Conventional security measures, including all physical protection and biometric entry systems, are rendered useless against drone-based network attacks that are not unprecedented, but, to date, this is a tactic that has predominantly remained in the realm of controlled research environments. Security researchers have demonstrated drone-based attacks that range from the simplistic to the complex and esoteric. Drones hovering outside office windows have hijacked a Bluetooth Mouse to silently install malware on a computer, and a drone-mounted video recorder was used to receive communications from a malware-infected computer that emitted light pulses through a window [105]. Drones equipped with specially fitted hardware and software may also be used to install malicious malware on systems or disrupt systems' operations, particularly devices that are vulnerable to the exploitation of wireless protocols such as Bluetooth [105].

Drone-enabled network attacks may never reach the scale of traditional remote network cyberattacks, but the possibility of their use may require all in authority to consider their airspace as another component of an attack surface that must be defended. The requirement for both the attacker and the drone to be in close proximity to a target will limit the frequency with which drone-based attacks will be used, but the threat nonetheless remains real and should not be underestimated and provides evidence of how innovative cybercriminals are leveraging disruptive drone technology, which, as a direct result, has become decidedly dangerous.

It is clear to see why drones offer a new tactic for cybercriminals, as they can be operated anonymously and remotely, they present little or no risk to their operators of detection or prosecution, they can be acquired cheaply and easily, and their operation can be mastered simply and safely. The use of drones to commit cybercrime has signaled that the rogue drone

threat landscape is increasingly diverse and has become more aggressive. The emergence of rogue drone activity has created a new dimension and a fundamental shift in the way in which the safety and security of buildings, personnel, data, and other assets should be protected from the threat of hostile cyberattack. The adaption of drones to facilitate all manner of cyberattacks is a new cyber security threat vector, but, worryingly, drones have also proved themselves to be vulnerable to cyberattack.

1.8.2 Cyber Drone-Jacking

The introduction of military UAVs by the U.S. Central Intelligence Agency (CIA) in the skies over Afghanistan in 2000 represented a fundamental shift in intelligence-gathering capabilities [107]. Today, UAVs are used for a wide range of military missions such as border surveillance, reconnaissance, transportation, and armed attacks. Following their successful deployment in military and intelligence applications, drones have seen rapid adoption in both public and private sectors, acting as a supplement or substitute for traditional modes of delivery. UAVs are presumed to be reliable, automated, and autonomous machines, providing their services at any time. Based on these presumptions, government, military, and emergency service leaders hope that UAVs will improve national security and public safety while business leaders expect to see positive returns on their investment to improve their services. From a purely technical perspective, UAVs are highly exposed, multilinked, complex pieces of hardware.

To fulfill their missions, UAVs need to collect and process data. Contemporary UAVs may contain information about troop movements to environmental information and commercially sensitive business operations. The volume of information contained within and communicated to and from drones has already made them a high value target for espionage, endangering UAVs to manipulation through cyberattack [108]. Despite the high value and sensitivity of data being received, transmitted, or contained within drones, security measures to counter attacks could not prevent Predator drones from being hacked in 2009 by Iraqi insurgents who reportedly intercepted live video feeds from the military drones using a $25.95 Windows application that allowed them to track the pilotless aircraft undetected [109].

Senior defense and intelligence officials said that Iranian-backed insurgents intercepted the video feeds by taking advantage of an unprotected communications link [110]. Hackers working with Iraqi militants were able to determine which areas of the country were under surveillance by the U.S. military [109]. The inexpensive software, created by a Russian company called SkyGrabber, was downloadable from the internet and intercepted

data received from a satellite dish [110]. The software developer Andrew Solonikov has insisted that the SkyGrabber was not developed for the use of hacking military drones, stating that [111]: "Somebody has invented a way to use this program outside of its intended purpose but generally speaking, this points to a large security gap that the American military has missed." The incident not only potentially compromised sensitive operations but also sparked serious concern among government security and defense experts in the cyber security of UAVs.

The full extent of the cyber-threat vulnerability of UAVs in military operations was globally acknowledged following the capture of a U.S. RQ-170 Sentinel UAV by the Iranian military in December 2011. The Iranian government pushed the propaganda advantage after showing that it had captured the intact U.S. stealth drone on a spying mission 140 miles inside Iran [112]. Hours after Iran state TV displayed the cream-colored American bat-wing RQ-170 Sentinel drone, its undercarriage hidden by the banners of a U.S. flag, with stars replaced by skulls and marked with anti-U.S. slogans, Iranian officials said the spy craft was proof of enduring U.S. hostility toward Iran [112]. The Sentinel spy drone, which was reportedly monitoring Iran's nuclear program, was a significant loss for the United States during an incident that may constitute the earliest UAV attack, which led directly to the public questioning of a nation's cyber power [113]. While the exact method by which the RQ-170 was compromised has never been publicly confirmed, researchers proved subsequently that it is possible to hijack drones in flight through GPS spoofing. This incident called into question U.S. cyber competency and has been frequently cited in arguments against UAV use to highlight their lack of controllability in military scenarios. One line of argument suggests that this kind of attack constitutes electronic warfare, rather than pure cyberattack. However, consider that producing a hostile effect by introducing compromised data into an operating system meets a reasonable definition of cyber, rather than electronic, attack. In any case, experience of current combat operations shows that the dividing lines between these different kinds of warfare are becoming increasingly blurred and irrelevant. Furthermore, regardless of the status of debate over the nature of the attack, the wide variety of available attack scenarios is one of the aspects that make UAVs especially vulnerable. From a pragmatic point of view, it does not matter how control of a software or hardware component is lost. Besides communication links, another exploitable component is the UAV's operating system (OS) or micro-controller unit. The type of OS varies between UAV manufacturers, and prototypes have been developed using smartphones as UAV control systems [113]. Thus, any known exploit in the smartphone's OS also becomes relevant in a UAV context, leading to a broader security and safety threat. It is also noteworthy that many

smartphones are already compromised without the users being aware of it. By 2012, the U.S. military had increased its investment in research and production of UAVs from $2.3 billion in 2008 to $4.2 billion, including advances in capabilities to protect against cyberattack.

1.8.3 Malicious Drone Malware

As digital circuitry and wireless technology become an integral part of increasing numbers of consumer and industrial goods, the opportunities available for cybercriminals to compromise or exploit these items grows. UAVs are now an emerging security concern, both as targets for cyberattack and as potential attack vectors for malicious actors. Drones use the most advanced technological equipment and research into these vehicles is providing continuous improvements, resulting in a new generation of UAVs characterized by high performance, high autonomy, and extreme versatility, which makes their use suitable for many applications [114]. Despite the new generation of drones being packed with the latest technical tools, a team of researchers at the Netherlands' University of Twente has demonstrated how high-end drones commonly deployed by government agencies and police forces can be remotely exploited by rogue hackers. The research team found security flaws in drones' radio connections, providing an opportunity to attack the vehicle with only a laptop and a cheap USB-connected chip [115]. The researchers found that they could easily exploit the lack of encryption between the drone and its controller module. Furthermore, the team warned that any sophisticated hacker who is able to reverse-engineer the drone device's software would be able to send navigational controls, block all commands from the real operator, or even crash it to the ground [115]. The research at the University of Twente is just one of a growing number of independent tests that are discovering a worrying array of UAV security design flaws in what is a rapidly expanding market place.

Hacking aimed at connected devices, those falling under the auspices of the Internet of Things (IoT), is becoming more prevalent, and the first piece of evidence that UAVs were being targeted by cybercriminals was the discovery of the malware, Maldrone, built specifically to infiltrate drones [116]. While drones are becoming more commonplace and are being adapted for more uses, such as data collection, they are quickly becoming a more valuable target for hackers who want to seize either the drone for nefarious purposes or the data being collected. Maldrone is a type of malware specifically aimed at UAVs and intended to hack into drones via internet connections [116]. Drones, after all, are essentially flying computers. As such, they are susceptible to the same type of hacks as a laptop or smartphone. Drone-hacking technology can be used to either swipe the data that the

machines collect or even take over their physical control through malware, which is a contraction of malicious software. Malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing damage and disruption. Viruses, Trojans, spyware, and ransomware are among the different kinds of malware in use today by cybercriminals, who often create malware in teams working together, usually amplifying their opportunities to make money, either by spreading the malware themselves or selling it to the highest bidder on the Dark Web [117]. However, there can be other reasons for creating malware: it can be used as a tool for protest, a way to test security, or even as weapons of war between governments; this has raised acute international security concerns of the development of the Maldrone malware, which, for the contemporary hacker, was the next logical step in proving that drones can be commandeered for more nefarious purposes.

1.9 Reducing the Risk

The latest UAV research suggests that annual revenues from commercial drone sales were expected to reach $500 million in 2016, up by 84% on 2015's figure of $261 million [118]. Research focusing upon the consumer and commercial applications, regulations, and opportunities for 2015 to 2020 found that a low price point had significantly reduced the barrier to entry in many sectors, with high-performance models now available for less than $3,000 [11]. The cost-effectiveness of commercial UAVs has seen their successful deployment as crucial links in supply chain logistics for the pharmaceutical industry, enabling delivery of fresh blood plasma and essential drugs to remote regions inaccessible to other forms of transport.

UAVs have also proven their value as reconnaissance and delivery agents in the health-care and emergency services sectors, supporting fire and rescue operations. In agriculture, drones are being used to chart patterns and success rates for irrigation and to monitor the health of growing crops via infrared and other technologies. Video and still cameras mounted on UAVs provide promotional imagery for the real estate market and innovative angles for documenting sporting events and other public gatherings. A small number of innovative retail outlets, food chains, and restaurants are now routinely using drones to fulfill customer demands for a high-speed service, amplifying growth in a new commercial market for UAV capabilities.

The rapid proliferation of UAVs is having a real impact for authorities who are seeking ways in which to effectively manage and safeguard the use of drones. Unfortunately, "widespread" does not necessarily equate to "safe to use." Many UAVs have inherent and potentially serious design flaws.

Given their maneuverability, small size, and the fact that their combination of on-board processing power, photographic equipment, and connectivity makes them the equivalent of flying computers, it is no wonder that drones are now perceived as viable threats to information security. Poorly secured or unsecured wireless networks are seen as particularly vulnerable, with attack scenarios envisaged where compromised or purpose-bought UAVs could be flown or discreetly landed in the vicinity of a hot spot and used to stage man-in-the-middle attacks, data injection, and similar attacks over guest and short-range Wi-Fi, Bluetooth, and other wireless connections [105]. As drones are relatively cheap technologies for military use (certainly cheaper than the use of satellites for surveillance), off-the-shelf drones are being purchased to gather intelligence, without any significant development effort. Therefore, moving forward, it will be essential to safeguard every single component of this sophisticated, off-the-shelf, unmanned aerial military fleet from cyberattack, especially as when drones were initially developed, cyber security was not considered a priority [119].

The jacking of drones presents a new and emerging danger within the ever-expanding attack vectors of the contemporary cybercriminal. As the technology evolves and new opportunities for cyberattackers present themselves, security professionals will need access to a range of measures to combat a growing threat. To reduce the risk, in-depth research into cyberattack threats and vulnerability identification of UAV systems is needed. This research should include the study of more sophisticated attack scenarios together with the development of metrics for UAV cyberattacks. According to research conducted at Purdue University in the United States, so far, a metric for measuring either a likelihood (or probability) or a damage potential of cyberattacks on a UAV does not exist [120]. Conducting rigorous programs of UAV cyber-security research will serve to strengthen the safe use of drones and reduce their vulnerability to attack from contemporary cybercriminals.

The risk of increasing drone use by cybercriminals is married to the cyber-threat landscape, which is subject to constant change with far-reaching vulnerabilities, faster attacks, files held for ransom, and the continued presence of data breaches. Advanced cybercrime threats continue to evolve with criminal gangs increasingly adopting cyberattack techniques that were previously the preserve of nation states. Cyber vulnerabilities remain a big part of the security picture and all the evidence from cybercrime-related threat and risk assessments indicate that the attackers are moving faster than the practical and operational implementation of effective cyber defenses and countermeasures, which includes measures to protect drones from cyberattack. Through constant innovation, cybercriminals are developing

increasingly sophisticated malware and rogue mobile apps and more resilient botnets. With the rapidly expanding cybercrime-as-a-service marketplace, all these products are becoming much more widely available—and more exploitable by criminals with little or no technical knowledge. Unfortunately, this position is unlikely to change in the near future, and the cyberattackers will continue to have the upper hand unless more can be done to anticipate future threats and risks, which require the ability to horizon scan for the weak signals, indicating the early signs of new trends. To combat these cyber-threat trends, law enforcement agencies are tending to favor intelligence-driven security approaches that can operate in mobile and cloud environments, making greater use of behavioral analytics, and taking advantage of smart device capabilities to protect users and data. Even if cyberattacks cannot be blocked completely, having access to the right intelligence makes it possible to detect an attack more quickly, significantly reducing the attacker's window of opportunity and minimizing the potential for loss or damage.

Despite major investments in cybercrime units, training and the introduction of new powers and investigative techniques, law enforcement agencies across the world continue to be challenged on many fronts in combating contemporary cybercrime. These challenges are amplified by the emergence of the UAV threat from hackers, which remains underestimated. However, all in authority have yet to realize the sheer scale of the cyber security challenge, which would become clearer if they treated cyberspace for what it is: a separate socio-spatial dimension in which billions of people across the world choose not only to communicate, but also to dwell, trade, socialize, and cultivate; to create intellectual property and generate economic wealth; to begin and end relationships; to forage, feud, and thrive; and to heal, harm, and steal [121]. Viewed in this way, cyberspace is another continent, vast, viable, and virtual, a distinct jurisdiction that not only requires its own constitution and legal system, but its own law enforcement and safeguarding agencies. The adaption of drones to commit all manner of cyber-related crimes and security breaches is the latest cyber threat to emerge, and amplifies the nefarious use of drones, brought about by the combination of advancements in UAV technology and the unlimited creativity of actors with hostile intent, introducing new layers of complexity to the global drone threat landscape.

References

[1] World Economic Forum, "Drones and Tomorrow's Airspace," 2020, https://www.weforum.org/communities/drones-and-tomorrow-s-airspace.

[2] Scott, G., and T. Smith, "Disruptive Technology: What Is Disruptive Technology?" *Investopedia*, March 21, 2020, https://www.investopedia.com/terms/d/disruptive-technology.asp/.

[3] Pricewaterhouse Coopers LLP (PwC), "Skies Without Limits: Drones – Taking the UK's Economy to New Heights," 2018, https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf.

[4] Amazon, "Amazon Prime Air – How Will It Work?" 2020, https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.

[5] Folk, E., "This Is How Drones Could Help to Fight Climate Change," *World Economic Forum*, May 24, 2018, https://www.weforum.org/agenda/2018/05/the-surprising-way-drones-can-help-fight-climate-change.

[6] Kelly, S. A., "Drone Tech Offers New Ways to Manage Climate Change," *Cornell Chronicle*, Cornell University, August 8, 2017, https://news.cornell.edu/stories/2017/08/drone-tech-offers-new-ways-manage-climate-change.

[7] Baggaley, K., "Drones Are Setting Their Sights on Wildlife - And They're Making Science Safer for Everyone Involved," *Popular Science*, February 10, 2017, https://www.popsci.com/drones-wildlife-biology-animal-research/#page-4.

[8] BBC News, "Coronavirus: Northamptonshire Police Could Use Drones," March 23, 2020, https://www.bbc.co.uk/news/uk-england-northamptonshire-52004297.

[9] Holroyd, M., "Coronavirus: Italy Approves Use of Drones to Monitor Social Distancing," *Euronews*, March 23, 2020, https://www.euronews.com/2020/03/23/coronavirus-italy-approves-use-of-drones-to-monitor-social-distancing.

[10] Halaschak, Z., "California Police Consider New Uses for Drones During Coronavirus Pandemic," *Washington Examiner*, March 23, 2020, https://www.washingtonexaminer.com/news/california-police-consider-new-uses-for-drones-during-coronavirus-pandemic.

[11] Juniper Research, "Game of Drones," 2016, https://www.juniperresearch.com/document-library/white-papers/game-of-drones.

[12] Business Insider, "Intelligence Commercial Unmanned Aerial Vehicle (UAV) Analysis–Industry Trends, Forecasts and Companies," February 10, 2020 https://www.businessinsider.com/commercial-uav-market-analysis?r=US&IR=T.

[13] Wagner, I., "Projected U.S. Commercial Drone Market from 2020 to 2022, by Key Area of Application," *Statista*, February 7, 2020, https://www.statista.com/statistics/739797/us-commercial-drone-market-breakdown-by-application/.

[14] Her Majesty's Government, "Counter-Unmanned Aircraft Strategy," 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf.

[15] Goldman Sachs, "Technology Driving Innovation: Drones Reporting for Work," 2019, https://www.goldmansachs.com/insights/technology-driving-innovation/drones/.

[16] Towers, T., "Cops Warn of Drone Crime Spike Thanks to Scammers, Burglars and Paedos Taking to Using Flying Cams," The Sun, August 8, 2016, https://www.thesun.co.uk/news/1570512/police-report-fourfold-rise-in-crime-re-

ports-involving-drones-amid-fears-paedophiles-are-using-them-over-kids-playgrounds/.
[17] Kulsov, I., "Air Alert: 8 Dangerous Drone Incidents," *Kapersky Daily*, October 21, 2019, https://www.kaspersky.co.uk/blog/drone-incidents/16832/.
[18] Schmidt, M. S., and M. D. Shear, "White House Drone Crash Described as a U.S. Worker's Drunken Lark," *New York Times*, January 27, 2015, https://www.nytimes.com/2015/01/28/us/white-house-drone.html.
[19] DJI News, "DJI Has Released the New Firmware v3.12 for Phantom 2 Series Quadcopter," *DJI Newsroom*, March 3, 2015, https://www.dji.com/newsroom/news/dji-has-released-the-new-firmware-v3-12-for-phantom-2-series-quadcopter.
[20] The United States Attorney's Office, District of Columbia, "U.S. Attorney's Office Will Not Pursue Charges Against Man Whose Errant Drone Landed at White House," March 18, 2015, https://www.justice.gov/usao-dc/pr/us-attorneys-office-will-not-pursue-charges-against-man-whose-errant-drone-landed-white.
[21] Pigott, R., "Heathrow Plane in Near Miss with Drone," *BBC News*, December 7, 2014, https://www.bbc.co.uk/news/uk-30369701.
[22] Ali, A., and D. Baldwin, "Drone Intrusion Shuts Down Dubai, Sharjah Airports," *Gulf News*, October 29, 2016, https://gulfnews.com/going-out/society/drone-intrusion-shuts-down-dubai-sharjah-airports-1.1920833.
[23] McNabb, M., "Drone Operator Interviewed in Blackhawk Helicopter and Drone Collision," *Drone Life*, October 6, 2017, https://dronelife.com/2017/10/06/drone-operator-interviewed-blackhawk-helicopter-drone-collision/.
[24] Pham, S., "Drone Hits Passenger Plan in Canada," CNN Business, October 16, 2017, https://money.cnn.com/2017/10/16/technology/drone-passenger-plane-canada/index.html.
[25] Evans, M., "Gatwick Airport Drone Investigation Closed by Police Without Anyone Being Charged," The Telegraph, September 26, 2019, https://www.telegraph.co.uk/news/2019/09/26/gatwick-drone-investigation-closed-without-suspect-identified/.
[26] BBC News, "Drone Collides with Commercial Aeroplane in Canada," October 16, 2017, https://www.bbc.co.uk/news/technology-41635518.
[27] Cullen, E., "Timeline: How the Drone Chaos at Gatwick Airport Unfolded," The Independent, December 21, 2018, https://www.independent.ie/world-news/europe/britain/timeline-how-the-drone-chaos-at-gatwick-airport-unfolded-37647539.html.
[28] Stevenson, S., "Gatwick Chaos: Police to 'SHOOT DOWN' Maniac Drone That Caused 120,000 Flight Disruptions," *The Express*, December 21, 2018, https://www.express.co.uk/news/uk/1062090/gatwick-airport-drone-chaos-shoot-down-drone-christmas-travel-disruption-flight-cancelled.
[29] Press Association, "MoD Removes Anti-Drone Military Hardware from Gatwick," *The Guardian*, January 2, 2019, https://www.theguardian.com/uk-news/2019/jan/02/mod-removes-anti-drone-military-hardware-from-gatwick.
[30] Jackman, A., "Consumer Drone Evolutions: Trends, Spaces, Temporalities, Threats," *Defence & Security Analysis*, Vol. 35, No. 4, October 24, 2019, pp. 362–383, https://www.tandfonline.com/doi/abs/10.1080/14751798.2019.1675934?src=recsys&journalCode=cdan20.
[31] Thompson, T., "Gatwick Drone Inquiry Has 'No Lines of Inquiry' Left to Pursue," *Police Professional*, September 21, 2019, https://www.policeprofessional.com/news/gatwick-drone-inquiry-has-no-lines-of-inquiry-left-to-pursue/.

[32] BBC News, "Gatwick Drones: Sussex Police 'Sorry' for Arrested Couple," December 29, 2018, https://www.bbc.co.uk/news/uk-england-sussex-46709353.
[33] Lyons, I., and A. Mikhailova, "Gatwick Drone Investigation: Couple Wrongly Arrested Feel 'Completely Violated', as Ministers Accuse Sussex Police of 'Messing Up,'" *The Telegraph*, December 25, 2018, https://www.telegraph.co.uk/news/2018/12/24/ministers-accuse-sussex-police-messing-gatwick-drone-investigation/.
[34] Detrick, H., "Gatwick's December Drone Closure Cost Airlines $64.5 Million," *Fortune*, January 22, 2019, https://fortune.com/2019/01/22/gatwick-drone-closure-cost/.
[35] Kollewe, J., and G. Topham, "EasyJet Says Gatwick Drone Chaos Cost It £15Million," *The Guardian*, January 22, 2019, https://www.theguardian.com/business/2019/jan/22/easyjet-gatwick-drone-cost-brexit-flights.
[36] Topham, G., "Gatwick Drone Disruption Cost Airport Just £1.4m," *The Guardian*, June 18, 2019, https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m.
[37] BBC News, "Gatwick Drone Policing Costs 'Shocking,'" March 25, 2019, https://www.bbc.co.uk/news/uk-england-47696499.
[38] BBC News, "Gatwick Drone Arrests: Sussex Police Pays Out £200,000," June 14, 2020, https://www.bbc.co.uk/news/uk-england-sussex-53041256.
[39] Burridge, T., "'Sustained' Drone Attack Closed Gatwick, Airport Says," *BBC News*, February 20, 2019, https://www.bbc.co.uk/news/business-47302902.
[40] Worksmart, "What Are the Five Steps to Risk Assessment?" 2020, https://worksmart.org.uk/health-advice/health-and-safety/hazards-and-risks/what-are-five-steps-risk-assessment.
[41] United Nations, "The Climate Crisis – A Race We Can Win," 2020, https://www.un.org/en/un75/climate-crisis-race-we-can-win.
[42] Agence France-Presse,"Drones Spotted over Seven French Nuclear Sites, Says EDF," *The Guardian,* October 30, 2014, https://www.theguardian.com/environment/2014/oct/30/drones-spotted-over-seven-french-nuclear-sites-says-edf.
[43] Greenpeace, "About Greenpeace," https://www.greenpeace.org.uk/about-greenpeace/.
[44] Leveque, T., and S. la Hamaide, "Greenpeace Activist Paraglides into French Nuclear Plant," *Reuters*, May 2, 2012, https://uk.reuters.com/article/us-france-nuclear-greenpeace/greenpeace-activist-paraglides-into-french-nuclear-plant-idUSBRE8410F8201205029.
[45] Agence France-Presse, "Greenpeace Activists Set Off Fireworks at Nuclear Plant in France," *The Local France,* October 12, 2017, https://www.thelocal.fr/20171012/greenpeace-activists-set-off-fireworks-at-nuclear-plant-in-france.
[46] Agence France-Presse, "Greenpeace Protesters Jailed for Fireworks Stunt at French Nuclear Plant," *The Local France,* February 28, 2018, https://www.thelocal.fr/20180228/greenpeace-protesters-jailed-for-fireworks-stunt-at-french-nuclear-plant.
[47] De Clercq, G., "Greenpeace Crashes Superman-Shaped Drone into French Nuclear Plant," *Reuters*, July 3, 2018, https://uk.reuters.com/article/uk-france-nuclear-greenpeace/greenpeace-crashes-superman-shaped-drone-into-french-nuclear-plant-idUKKBN1JT17G.
[48] Gliadkovskaya, A., "Greenpeace Activists Pilot and Crash Drone into French Nuclear Plant's No-Fly Zone," *Euronews*, July 3, 2018, https://www.euronews.

com/2018/07/03/greenpeace-activists-pilot-and-crash-drone-into-french-nuclear-plant-s-no-fly-zone.

[49] Reuters, "Qarabag Game Halted After Armenian Flag Flies over Stadium Azerbaijani Side's Europa League Game Against Dudelange," *Daily Mail*, October 4, 2019, https://www.dailymail.co.uk/sport/football/article-7535859/Qarabag-game-halted-Armenian-flag-flies-stadium-Europa-League-fixture.html.

[50] Euronews, "Europa League Football Match Halted by Drone Flying Flag of Disputed Nagorno-Karabakh," October 4, 2019, https://www.euronews.com/2019/10/04/europa-league-football-match-halted-by-drone-flying-flag-of-disputed-nagorno-karabakh.

[51] Murphy, K., "Man Accused of Flying Drone over NFL Football Games Charged," *Digital Photography Review*, June 1, 2019, https://www.dpreview.com/news/0816823562/man-accused-of-flying-drone-over-nfl-football-games-charged.

[52] Cerbair, "After Gatwick Could Sports Venues Be the Next Great Drone Debacle?" 2020, https://www.cerbair.com/after-gatwick-could-sports-venues-be-the-next-great-drone-debacle-blog/.

[53] Centre for the Protection of National Infrastructure (CPNI), "Hostile Reconnaissance: Understanding and Countering the Threat," June 2016, https://www.cpni.gov.uk/system/files/documents/23/de/understanding-hostile-reconnaissance-understanding-and-countering-the-threat.pdf.

[54] Burgess, M., "Revealed: How UK Police Are Taught to Deal with Drones," *Wired*, November 3, 2015, https://www.wired.co.uk/article/police-fly-drone-crash-danger-terrorism-rules.

[55] Abbott, C., et al., *Hostile Drones: The Hostile Use of Drones by Non-State Actors Against British Targets*, Remote Control Project, Network for Social Change, Oxford Research Group, January 2016, https://www.openbriefing.org/docs/Hostile-use-of-drones-report_open-briefing.pdf.

[56] DJI Store, "Phantom Series," 2020, https://store.dji.com/shop/phantom-series?from=menu_icon.

[57] Chulov, M., "Isis Fighters Surround Syrian Airbase in Rapid Drive to Recapture Lost Territory," *The Guardian*, August 22, 2014, https://www.theguardian.com/world/2014/aug/22/isis-syria-airbase-tabqa.

[58] Hubbard, B., "ISIS Tightens Its Grip with Seizure of Air Base in Syria," *New York Times*, August 24, 2014, https://www.nytimes.com/2014/08/25/world/middleeast/isis-militants-capture-air-base-from-syrian-government-forces.html.

[59] Russell, J. S., "How Important Is the Battle for Iraq's Baiji Oil Refinery?" *BCC News*, May 12, 2015, https://www.bbc.co.uk/news/world-middle-east-32663262.

[60] "Savage Battle Rages in Iraq for Control over Nation's Biggest Oil Refinery," *The Economic Times*, June 19, 2014, https://economictimes.indiatimes.com/news/international/world-news/savage-battle-rages-in-iraq-for-control-over-nations-biggest-oil-refinery/articleshow/36786767.cms?from=mdr.

[61] Tomlinson, S., and L. Edwards, "Obama to Unleash Air Strikes on ISIS: America Prepares to Target Islamic Fanatics as Shiites Rush to Join 'Peace Brigades' to Defend Iraq's Holy Sites," *Daily Mail*, June 19, 2014, https://www.dailymail.co.uk/news/article-2662272/This-similar-Nazi-occupation-Europe-says-Iraq-chief-ISIS-burn-cigarettes-Sharia-law-Britain-warned-militants-target-UK.html.

[62] Derzsi-Horvath, A., H. Nasser, and M. Schulz, "Iraq After ISIL: Baiji," *GPPi*, September 13, 2017, https://www.gppi.net/2017/09/13/iraq-after-isil-baiji.
[63] Schmidt, M. S., and E. Schmitt, "Pentagon Confronts a New Threat from ISIS: Exploding Drones," *New York Times*, October 11, 2016, https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?_r=0 9.
[64] Drone Defence, "Drones and Business Espionage – A New Corporate Threat," December 29, 2017, https://www.dronedefence.co.uk/drones-and-business-espionage/.
[65] T-Systems, "Defense Shield Against Drone Attack," 2020, https://www.t-systems.com/dk/en/security/managed-cyber-defense/drone-defense.
[66] Morgan, T., "Aintree Festival Drone Warning Amid Fears Celebrities' Helicopters Could Be Grounded," *The Telegraph*, April 4, 2019, https://www.telegraph.co.uk/news/2019/04/04/aintree-festival-drone-warning-amid-fears-celebrities-helicopters/.
[67] Tecniqode, "Is Paparazzi by Drone Legal?" *Martek Counter UAS*, September 3, 2019, https://martekcuas.com/is-paparazzi-by-drone-legal/.
[68] Sheridan, P., and C. Graham, "Attack of the Drones: Hollywood Celebrities Are Besieged by Paparazzi Spies in the Sky. Worried? You Should Be... Because They'll Soon Be a Regular Fixture over YOUR Home," *Daily Mail*, September 6, 2014, https://www.dailymail.co.uk/news/article-2746231/Attack-drones-Hollywood-celebrities-besieged-paparazzi-spies-sky-Worried-You-ll-soon-regular-fixture-YOUR-home.html.
[69] INTERPOL, "Framework for Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners," INTERPOL Innovation Centre: Singapore, January 2020.
[70] Europol, "European Union Serious and Organised Crime Threat Assessment 2017 – Crime in the Age of Technology," February 28, 2017, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.
[71] Global Financial Integrity, "Executive Summary: The Retail Value of Transnational Crime," *Transnational Crime and the Developing World*, March 2017, https://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final-_exec-summary.pdf.
[72] Europol & European Monitoring Centre for Drugs and Drug Addiction, "EU Drugs Market Report 2019," 2019, https://static.rasset.ie/documents/news/2019/11/eu-drugs-market-report.pdf.
[73] Bennett, J. T., "Coronavirus: Trump Sends in Military Amid Fears of 'Losing Ground' to Drug Cartels During Pandemic," *Independent*, April 2, 2020, https://www.independent.co.uk/news/world/americas/us-politics/trump-coronavirus-mexican-drug-cartels-smuggling-covid-19-pandemic-a9441431.html.
[74] Davis, K., "Drone Smuggles Heroin into U.S.," *The San Diego Union-Tribune*, August 12, 2015, https://www.sandiegouniontribune.com/sdut-drone-smuggle-heroin-us-calexico-drug-2015aug12-story.html.
[75] Wolfe, F., "U.S. DEA: Border Wall or No, Drone Drug Smuggling Likely to Increase," *Rotor & Wing International*, January 10, 2019, https://www.rotorandwing.com/2019/01/10/u-s-dea-border-wall-no-drone-drug-smuggling-likely-increase/.
[76] U.S. Government, "President Donald J. Trump's Address to the Nation on the Crisis at the Border," U.S. White House, January 8, 2019, https://www.white-

house.gov/briefings-statements/president-donald-j-trumps-address-nation-crisis-border/.

[77] Fiegal, B., "Narco-Drones: A New Way to Transport Drugs," *Small Wars Journal*, 2016, https://smallwarsjournal.com/jrnl/art/narco-drones-a-new-way-to-transport-drugs.

[78] Castellano, A., "Drug-Traffickers Intended to Transport More Than 100 Kilos of Cocaine with a Drone," *Panama Today*, November 16, 2016, https://www.panamatoday.com/panama/drug-traffickers-intented-transport-more-100-kilos-cocaine-drone-2422.

[79] Press Association, "Man Jailed for Using Drone to Fly Drugs into Prisons," *The Guardian*, July 21, 2016, https://www.theguardian.com/uk-news/2016/jul/21/man-jailed-for-using-drone-to-fly-drugs-into-prisons.

[80] Press Association, "Seven Jailed over Plot to Fly Drugs into UK Prisons with Drones," *The Guardian*, October 26, 2018, https://www.theguardian.com/uk-news/2018/oct/26/seven-jailed-over-plot-fly-drones-drugs-uk-prisons.

[81] Press Association, "Eight Jailed over Plot to Smuggle Drugs and Phones into UK Prisons," The Guardian, December 13, 2017, https://www.theguardian.com/society/2017/dec/13/eight-jailed-plot-to-smuggle-drugs-and-phone-into-uk-prisons.

[82] Doffman, Z., "Warning over Terrorist Attacks Using Drones Given by EU Security Chief," *Forbes,* August 4, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones/#4bcb380d7ae4.

[83] Europol, *European Union Terrorism Situation and Trend Report 2019*, June 27, 2019, https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat.

[84] Tarallo, M., "Fatalities from Terror Attacks Continue to Decrease," *ASIS Security Management Magazine*, March 1, 2020, https://www.asisonline.org/security-management-magazine/articles/2020/03/fatalities-from-terror-attacks-continue-to-decrease/.

[85] Jenkins, M. B., "The New Age of Terrorism," RAND, 2006, https://www.rand.org/pubs/reprints/RP1215.html.

[86] Rassler, D., *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technologies*, Combating Terrorism Center at West Point, United States Military Academy, October 2016, https://www.ctc.usma.edu/wp-content/uploads/2016/10/Drones-Report.pdf.

[87] BBC News, "Aum Shinrikyo: The Japanese Cult Behind the Tokyo Sarin Attack," July 6, 2018, https://www.bbc.co.uk/news/world-asia-35975069.

[88] Police National Legal Database & Staniforth, *A Blackstone's Counter-Terrorism Handbook*, Oxford, U.K.: Oxford University Press, 2013.

[89] Inagaki, K., and L. Lewis, "Japan Executes Cult Leader Behind 1995 Tokyo Subway Gas Attack," *Financial Times*, July 6, 2013, https://www.ft.com/content/eafbd67c-80b0-11e8-bc55-50daf11b720d.

[90] Fishman, A., "What Really Went Wrong in Botched 1997 Shayetet 13 Operation?" *Ynet News Magazine*, June 21, 2017, https://www.ynetnews.com/articles/0,7340,L-4977429,00.html.

[91] Sof, E., "Ansariya Ambush: Israel's SOF Greatest Military Defeat," *Spec Ops Magazine*, 2018, https://special-ops.org/44395/ansariya-ambush-israels-sof-greatest-military-defeat/.

[92] Hubbard, B., "Iran Out to Remake Mideast with Arab Enforcer: Hezbollah," *The New York Times*, August 27, 2017, https://www.nytimes.com/2017/08/27/world/middleeast/hezbollah-iran-syria-israel-lebanon.html.
[93] Weiner, R., "Thanks to Supreme Court, Convicted Member of Jihadi 'Paintball' Group Leaving Prison Decades Early," *The Washington Post*, July 19, 2018, https://www.washingtonpost.com/local/public-safety/he-was-supposed-to-serve-85-years-for-backing-terrorism-thanks-to-the-supreme-court-hell-be-released-after-10/2018/07/19/242fcc22-8b7a-11e8-8aea-86e88ae760d8_story.html.
[94] "Maryland Man Sentenced for Aiding LeT," *The Economic Times,* August 26, 2006, https://economictimes.indiatimes.com/news/politics-and-nation/maryland-man-sentenced-for-aiding-let/articleshow/1927878.cms.
[95] Freeman, S., "Judge Pleads for Power to Jail Terror Fundraiser for Life," *The Times*, March 17, 2006, https://www.thetimes.co.uk/article/judge-pleads-for-power-to-jail-terror-fundraisers-for-life-n32kc2fhfbs.
[96] Counter Extremism Project, "Profile of Lashkar-e-Taiba," 2020, https://www.counterextremism.com/threat/lashkar-e-taiba.
[97] U.S. District Court for the Eastern District of Virginia, Memorandum Opinion, *United States v. Khan*, 309 F. Supp. 2d 789 (E.D. Va. 2004), March 4, 2020, Justia United States Law, https://law.justia.com/cases/federal/district-courts/FSupp2/309/789/2310743/.
[98] Hambling, D., "How Islamic State Is Using Consumer Drones" *BBC*, December 9, 2016, https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones.
[99] BBC News, "Venezuela President Maduro Survives 'Drone Assassination' Attempt," August 5, 2018, https://www.bbc.co.uk/news/world-latin-america-45073385.
[100] Gallon, N., E. Perez, and P. Walsh, "Inside the August Plot to Kill Maduro with Drones," *CNN*, June 21, 2019, https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html.
[101] Internet World Statistics, "The Internet Big Picture 2019: World Internet Users and Population Statistics," https://www.internetworldstats.com/stats.htm.
[102] Bank My Cell, "How Many Smartphones Are There in World?" https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.
[103] Young, J., "Global Ecommerce Sales to Reach Nearly $3.46 Trillion in 2019," Digital Commerce 360, November 13, 2019, https://www.digitalcommerce360.com/article/global-ecommerce-sales/.
[104] Zephoria Digital Marketing, "The Top 20 Valuable Facebook Statistics," June 2020, https://zephoria.com/top-15-valuable-facebook-statistics/.
[105] Booz Allen Hamilton, *Top 9 Cyber Security Trends for 2020*, https://www.boozallen.com/c/insight/publication/top-9-cybersecurity-trends-for-2020.html.
[106] Forcepoint, "Cyber Education: What Is Bring Your Own Device (BYOD)? BYOD Defined, Explained, and Explored," https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod.
[107] Sifton, J., "A Brief History of Drones," *The Nation*, February 7, 2012, https://www.thenation.com/article/brief-history-drones/.
[108] Harmann, K., and C. Steup, "The Vulnerability of UAVs to Cyber-Attacks: An Approach to the Risk Assessment," *Cyber Conflict (CyCon), 2013 5th International Conference*, January 2013, https://www.researchgate.net/publica-

tion/261449270_The_vulnerability_of_UAVs_to_cyber_attacks_-_An_approach_to_the_risk_assessment.

[109] McCullagh, D., "Predator Drones Hacked in Iraq Operations," *CNET*, December 17, 2009, https://www.cnet.com/uk/news/predator-drones-hacked-in-iraq-operations/.

[110] Cole, A., Y. J. Dreazen, and S. Gorman, "Insurgents Hack U.S. Drones," *The Wall Street Journal,* December 17, 2009, https://www.wsj.com/articles/SB126102247889095011.

[111] Mount, M., and E. Quijano, "Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates," *CNN*, December 18, 2009, http://edition.cnn.com/2009/US/12/17/drone.video.hacked/.

[112] Peterson, S., "Downed US Drone: How Iran Caught the 'Beast,'" *The Christian Science Monitor*, December 9, 2011, https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.

[113] Giles, K., and K. Hartmann, "UAV Exploitation: A New Domain for Cyber Power," *8th International Conference on Cyber Power*, Otto von Guericke University Conflict Studies Research Centre Magdeburg, Germany, 2016, https://ccdcoe.org/uploads/2018/10/Art-14-assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf.

[114] Paganini, P., "Hacking Drones: Overview of the Main Threats," *Information Security Institute*, June 4, 2013, http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/#gref.

[115] Cuthbertson, A., "Drones Knocked Out of the Air by Sound Waves," *International Business Times,* August 10, 2015, http://www.ibtimes.co.uk/drones-knocked-out-air-by-sound-waves-1514781.

[116] De Looper, C., "Drones Now Big Hacking Target, First Drone Malware Identified," *TechTimes*, February 4, 2015, http://www.techtimes.com/articles/30634/20150204/drone-hacking-next-big-security-concern.htm.

[117] Regan, J., "What Is Malware? How Malware Works & How to Remove It," *AVG Signal*, July 11, 2019, https://www.avg.com/en/signal/what-is-malware.

[118] Smith, S., "Commercial Drone Sales to Rise by More Than 80% This Year as Annual Sales Approach $500mn," *Juniper Research*, January 18, 2016, https://www.juniperresearch.com/press/press-releases/commercial-drone-sales-to-rise-by-more-than-80.

[119] Ahmed, M., and P. Haskell-Dowland, "Aerial Threat: Why Drone Hacking Could Be Bad News for the Military," *The Conversation*, October 7, 2019, http://theconversation.com/aerial-threat-why-drone-hacking-could-be-bad-news-for-the-military-124588.

[120] Aldridge, H., et al., "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," American Institute of Aeronautics and Astronautics, 2012, https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf.

[121] Sampson, F., "Chapter 1 – Cyberspace: The New Frontier for Policing?" *Cyber Crime and Cyber Terrorism Investigator's Handbook*, New York: Elsevier, 2014.

CHAPTER

2

Contents

Understanding Drone Technologies

2.1 Introduction

According to *The Free Dictionary* [1], the original definition of a drone is: "A male bee, especially a honeybee, that is characteristically stingless, performs no work, and produces no honey. Its only function is to mate with the queen bee." The more conventional definition is: "A remotely controlled or autonomous aircraft with no pilot on board."

The word drone was introduced as U.S. naval jargon in 1935 by Commander (later Rear Admiral) Delmer Fahrney (1898–1984). It was referring to the modified de Havilland DH82B "Queen Bee" British-made biplane, which flew unmanned for target practice and was controlled by an operator on a mother ship, likened to a queen bee [2]. A photograph of this drone is shown in Figure 2.1.

Historically, drones were developed to support military and surveillance activities. The first use of drones was recorded well before piloted flights commenced. Ignoring anecdotal stories about the use of drones by the Chinese in thirteenth century, the very first documented

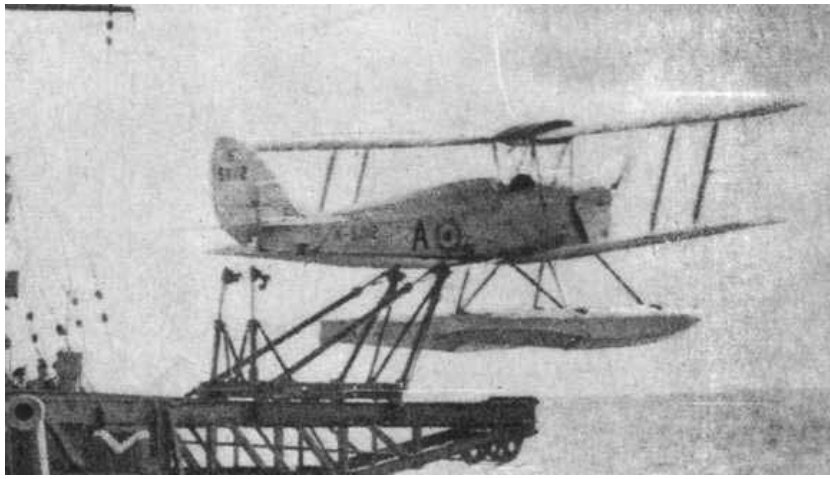

Figure 2.1 The de Havilland DH82B Queen Bee drone. (We express our gratitude to the staff of www.historyofwar.org website for their permission to use a photograph of the de Havilland Queen Bee drone.

use of drones happened in 1849 when the Republic of San Marco was surrounded by Austrian forces who bombarded Venice using unmanned, Austrian-made, hot-air balloons [3]. The exact number of balloons used in this operation is still uncertain (reports vary between 2 and 200), but only a few of these balloons were successful and reached the intended target with the help of favorable wind conditions, while some of them flew back and bombed their own positions due to unfavorable winds. Similar balloons were also used in the United States during the U.S. Civil War [4, 5].

The use of conventional drones for warfare and surveillance started as early as in 1898 by the U.S. Army during the Spanish-American War [6]. The progress in drone development was going on in parallel with the progress in the aviation industry, and it is not surprising that the first drones were built utilizing structures from the conventional aircraft of the time. However, the introduction of the first quadcopter (see Figure 2.2) in 1922 could be considered as a starting point for many modern commercial quadcopters, even though its maximum attitude was only 5m [7].

As many other modern technologies, drones were initially developed and utilized primarily for military appl supporting the "three Ds" (i.e., dull, dirty, or dangerous) missions [8]. The first publicly known military use of UAVs was in 1982 during the Israeli-Syrian conflict, where Israel used battlefield drones to jam Syrian communications and to survey positions. The success of this operation was so significant that it raised strong interest in drone technologies, providing a strong incentive for the development of military drones. This eventually generated interest from the scientific

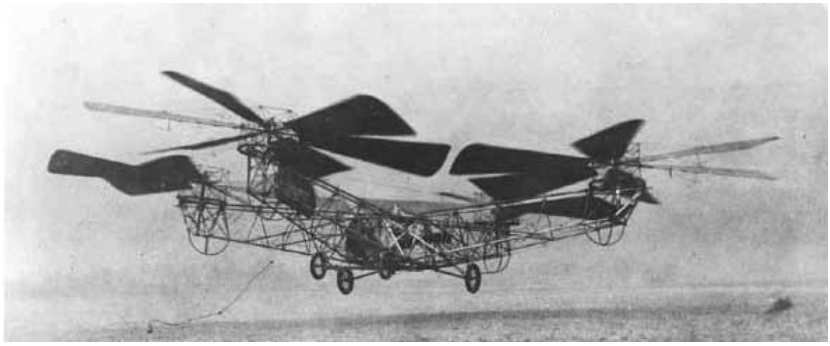

Figure 2.2 First quadcopter UAV.

and commercial communities in exploiting drones for science missions and other commercial applications.

2.2 The Most Common UAV Applications

Although initially UAVs were introduced for military applications, they are currently used in aspects of human activities and the range of applications is growing continuously. There are even predictions that UAVs may dramatically change the way that we work and relax, similarly as internet and mobile phone technology did. The most common UAV applications are:

- *Search and rescue:* UAVs are used during the "golden hour" of any disaster recovery or in search and rescue operations providing detailed video and sensory data without any risk of life.
- *Inspection:* These are inspections of wind turbines, bridges, construction sites, power lines, and pipelines, reducing the cost of manual inspections in remote areas.
- *Agriculture:* This is the inspection of fields and crops to accurately assess crop progress and applying the required pesticides only in the affected areas, when required as shown in Figure 2.3 [9].
- *Surveillance:* All drones are equipped with an EO camera, but most professional drones have both electro-optical (EO) and infrared (IR) cameras as an integral part of the payload. These cameras provide live video feeds helping to survey rural or dangerous areas.
- *Geo-mapping:* A dedicated payload, consisting of laser scanners and multispectral cameras, allows the collection of a unique data that is

Figure 2.3 Agricultural use of UAVs. (The authors would like to express their gratitude to Rinicom Ltd. for providing this photo and details of their FOLIUM project.)

significantly more accurate and easier to obtain, compared to traditional manual mapping.

- *Unmanned cargo system:* This application is driven by both Amazon and Google, promising to develop a cost-effective, safe, and environmentally friendly way to deliver lightweight packages. One specific application is gaining strong moment is delivery of medical supplies and first aid to rural or difficult-to-reach areas.
- *Aerial photography:* UAVs are successfully and efficiently replacing traditionally used helicopters due to their ability to hover at lower altitudes compared to the helicopter.
- *Environmental monitoring and research:* UAVs are used to monitor remote and unsafe areas such as volcanoes, glaciers, and radiation-contaminated areas (like the Chernobyl exclusion zone), providing unique data for environmental research.

Recent technological advances and cost reduction have stimulated a significant increase in drone usage for civilian and recreational activities. As a side effect of the technology progress, this has given rise to several cases where drones were involved (intentionally or unintentionally) in a number of well-publicized security and safety incidents. To address this growing

concern, the U.K. Civil Aviation Authority (CAA) introduced Dronecode [10] with the following definition:

- **D**on't fly near airports or airfields.
- **R**emember to stay below 400 feet and at least 150 feet away from buildings and people.
- **O**bserve drone.
- **N**ever fly near aircraft.
- **E**njoy responsibly.

More specifically, the U.K. CAA defines the following simple and important rules for all drone pilots [11]**:**

- *Always keep your drone in sight:* This means you can see and avoid other things while flying.
- *It is against the law to fly your drone over 400 ft (120m):* This reduces the likelihood of a conflict with manned aircraft.
- *From November 30, 2019, and for drones over 250g, you must pass the drone test and register with the CAA before you fly:* Passing the test and registering will help to keep you and others safe.
- *Keep the right distance from people and property:* The following distances are defined: people and properties: 150 ft (50m), crowds and built-up areas: 500 ft (150m), and do not overfly.
- *The legal responsibility lies with you. Failure to fly responsibly could result in criminal prosecution:* You are responsible for each flight.
- *If your drone endangers the safety of an aircraft, it is a criminal offense and you could go to prison for 5 years.*

In recognition of the importance of the problem, the U.K. National Air Traffic Services (NATS) has published eight top tips for flying drones safely [11].

In the United States, the U.S. Congress adopted the Federal Aviation Administration (FAA) Reauthorization Act of 2018, which requires drone pilots to pass an aeronautical knowledge and safety test. It also regulates how drone pilots can request authorization to fly near any controlled airspace such as airports [12]. The FAA applies the same rules for drone piloting (for example, recreational drones must fly below 120m in uncontrolled airspace) as the CAA, but it requires pilots to obtain prior authorization

from the FAA before flying near airports. All the certified UAV pilots are issued with an unmanned aerial system (UAS) certificate, which is similar to a driver's license.

2.3 UAV Configurations

In the context of this book, we will refer to a drone as a UAV or remotely piloted aircraft (RPA), which itself is a component of a larger unmanned aerial system (UAS), consisting of a (number) of UAVs, a ground station (GS), and various communication links between the UAVs and GS. UAVs can operate in a controlled mode piloted by a pilot, or in autonomous mode, utilizing on-board computers and navigation equipment. A typical UAS configuration is shown in Figure 2.4. All the UAS components shown in Figure 2.4 will be described in detail in this chapter.

Due to a wide variety of applications, there is no one unified classification of UAVs. Defense and security UAV operators use their own standards, while civilian operators and users have their own ever-evolving classifications of UAVs. Despite all the obvious differences, both civilian and military classifications define UAVs by size, range, type, and endurance, and adopted a tier system classification similar to that is utilized by the military [8]. Further on in this chapter, we will describe some of the most widely used classification standards.

Recently, the concept of UAV swarms was introduced [13, 14] and the use of UAV swarms is becoming more prevalent [13], stimulated by the introduction of Low-Cost UAV Swarming Technology (LOCUST) developed with the support of the U.S. Navy [15]. This technology is replacing the small number of expensive piloted UAVs with a large number of cheap

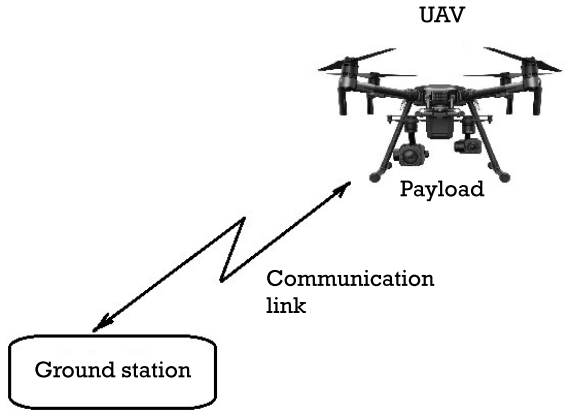

Figure 2.4 Typical single UAV configuration.

but similarly capable UAVs flying in swarm formations in the autonomous mode guided by on-board artificial intelligence and a predefined flight plan. A typical UAV swarm configuration is shown in Figure 2.5.

The main advantage of a swarm is the ability to operate as a unit with a shared objective. To achieve this, the swarm must be intelligent and self-configuring, capable to change formation and behavior per the overall mission goal and the specifics of the operational scenario in the particular time instant. A typical swarm will include elements of artificial intelligence and mesh networking, allowing UAVs to be aware of each other's movements and autonomously create flying formations as required by the overall mission objective.

Piloting the swarm brings additional challenges for the coordinator as, instead of piloting a single drone, the operator must manage the whole swarm simultaneously. This is a particular advantage in military applications as, due to low flight altitude and small size, swarms are invisible to anti-aircraft batteries and, even if detected, these batteries often do not have enough ammunition to stop them, as was proven in the attack on Saudi oil refineries in 2020 [16]. These advantages of swarms create additional challenges for the developers of C-UAV systems as the simultaneous detection, tracking, and classification of a large number of UAVs attacking a target could lead to a high percentage of false-positive and false-negative errors. At the same time, if all the UAVs in the swarm are detected and classified by the C-UAS systems, it may not be able to neutralize all the UAVs due to a lack of time or a shortage of ammunition.

In the context of this book, developing a C-UAV system capable of dealing with both the single UAV and the UAV swarm threats has additional challenges, which will be described one by one in the rest of this book.

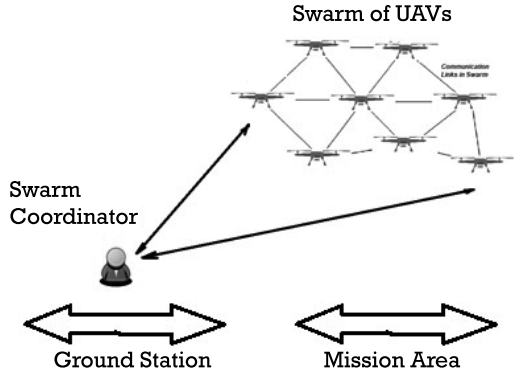

Figure 2.5 Typical swarm configuration.

2.4 Categories of UAVs and Their Classifications

2.4.1 Categories of UAVs

No C-UAS system can detect, classify, and eliminate all types of drones [16, 17]. Anti-missile defense systems are suitable when dealing with large drones and missiles; however, they are completely unsuitable when dealing with small drones or swarms of small drones. Respectively, C-UAV systems developed for the protection of privacy or large events (rock concerts, football matches, and other large outdoor events) are powerless against large attack drones. Therefore, one of the key elements in the development of a C-UAV system is to clearly define the relevant security threats and the types of drones associated with this threat. This will also define the cost and performance requirements of the C-UAV system and will allow security services to implement the most suitable action plan for dealing with detected drones and any follow-up forensic investigation. Therefore, it is essential to have a clearly defined classification system to ensure that the developers, manufacturers, and end users of the C-UAV system are consistent in their definitions.

Unfortunately, there is no single standard for the classification of UAVs today. Defense agencies, as early adopters of UAVs, have their own classifications that vary from country to country and even within country from force to force. For example, the U.S. Air Force and the U.S. Marine Corps have their own independent and noncompatible classification systems. These classification systems are described in depth in numerous publications [8, 18–22].

In these classification systems, UAVs are categorized as:

- VTOL (vertical take-off and landing);
- LASE (low altitude, short endurance);
- LALE (low altitude, long endurance);
- MALE (medium altitude, long endurance);
- HALE (high altitude, long endurance).

One of the most comprehensive review of various UAV classification systems is presented in [18], which includes the classification of categories of drones, as shown in Figure 2.6. As shown in this figure, UAVs can be organized into the following groups:

- UAV (unmanned air vehicle);
- Micro-UAV (micro unmanned air vehicle);

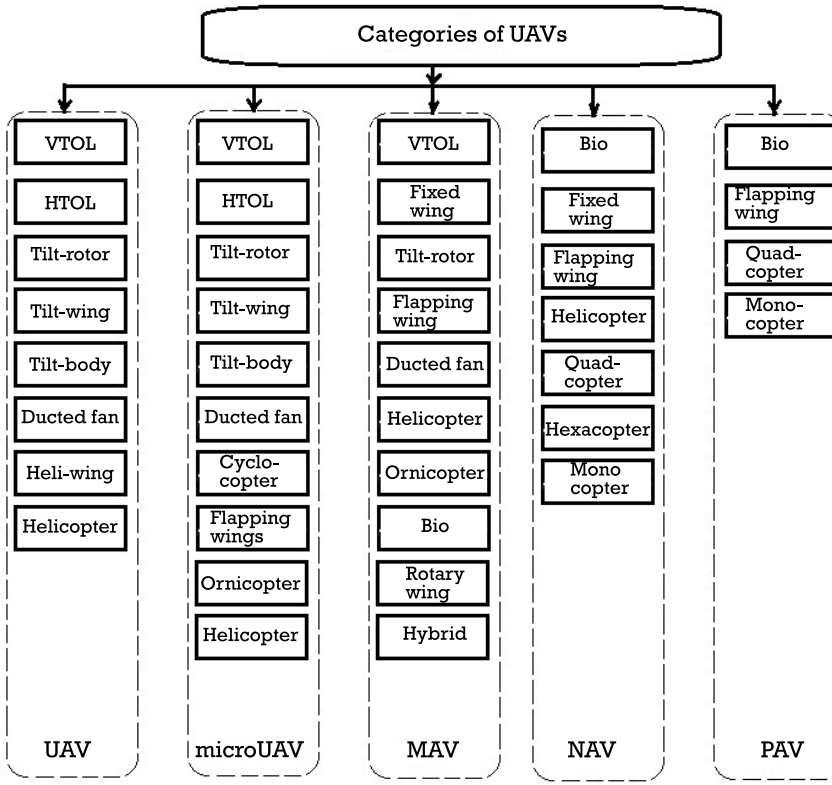

Figure 2.6 Categories of UAVs.

- MAV (miniature air vehicles);
- NAV (nano air vehicles);
- PAV (pico air vehicle).

There is a new category of rapidly emerging UAVs, called Small Dust (SD) [23], which, due to their very small size and swarm formation, could become the most challenging type of UAVs from the point of C-UAV system developers, where each group may include the same types of UAVs, such as:

- *HTOL* (*horizontal take-off and landing):* HTOL are tail plane-aft, tail plane-forward, tail-aft on booms, and tailless or flying wing UAVs [24]. These UAVs may have the propulsion systems at the rear of the fuselage or at the front side of the UAV.

- *VTOL (vertical take-off and landing):* VTOL UAVs can take off and land vertically and do not need a runway for take-off.
- *Hybrid-tilt-wing, tilt-rotor, tilt-body, and ducted fan:* These UAVs combine the capability of both VTOL and HTOL types [25].
- *Helicopter:* There are four types of helicopter UAVs, namely, single rotor, coaxial rotor, tandem rotor, and quad-rotor [26].
- *Heliwing:* Heli-wing UAVs are types of drones that use a rotating wing as their blade. They can fly as a helicopter vertically and also fly as a fixed wing UAV.
- *Various unconventional types:* These are UAVs that cannot be placed in previously defined categories. Usually, bio-inspired flying machines are assigned to this group.

Figure 2.7 [18] illustrates the various types of UAVs.

In an integrated classification of drones by weight and flight, a range was proposed and is shown in Table 2.1.

Another widely accepted classification is the classification proposed by the U.S. Department of Defense (DoD), where UASs are classified into five categories, according to their size, maximum gross take-off weight (MGTW), operating altitude, and airspeed as shown in Table 2.2 [27].

2.4.2 Classification According to Size

2.4.2.1 Very Small UAVs

The very small UAV class applies to UAVs with dimensions ranging from the size of a large insect to 30 to 50 cm long. Typical examples include the DJI MAVIC drones and insect-like UAVs with flapping or rotary wings.

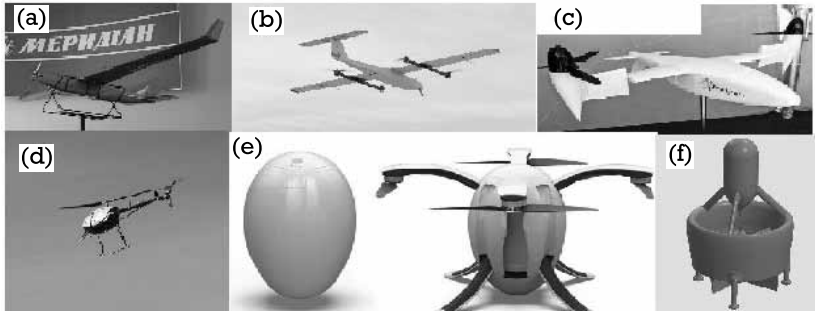

Figure 2.7 Types of UAVs: (a) HTOL, (b) VTOL, (c) tilt-rotor UAV, (d) helicopter tilt-wing UAV, (e) unconventional egg-shaped UAV, and (f) ducted fan UAV.

Table 2.1
Classification of UAVs by Weight and Flight Range

No	Designation	Weight Range	Flight Range
1	Micro-UAVs and mini-UAVs close range	W ≤ 5 kg	25 km ≤ R ≤ 40 km
2	Lightweight UAVs small range	5 kg < W ≤ 50 kg	10 km ≤ R ≤ 70 km
3	Lightweight UAVs medium range	50 kg < W ≤ 100 kg	70 km ≤ R ≤ 250 km
4	Average UAVs	100 kg < W ≤ 300 kg	150 km ≤ R ≤ 1,000 km
5	Medium to heavy UAVs	300 kg < W ≤ 500 kg	70 km ≤ R ≤ 300 km
6	Heavy to medium range UAVs	500 kg ≤ W	70 km ≤ R ≤ 300 km
7	Heavy UAVs, large endurance	1,500 kg ≤ W	R ≤ 1,500 km
8	Unmanned combat aircraft	500 kg < W	R ≤ 1,500 km

Table 2.2
UAS Classification According to the U.S. DoD

Category	Size	Maximum Gross Take-Off Weight (MGTW) (lbs)	Normal Operating Altitude (ft)	Airspeed (knots)
Group 1	Small	0–20	<1,200 AGL*	<100
Group 2	Medium	21–55	<3,500	<250
Group 3	Large	<1,320	<18,000 MSL**	<250
Group 4	Larger	>1,320	<18.000 MSL**	Any airspeed
Group 5	Largest	>1,320	>18,000 MSL**	Any airspeed

*AGL = Above ground level. **MSL = mean sea level. Note: If the UAS has even one characteristic of the next level, it is classified in that level.

Examples of very small UAVs are the Israeli IAI Malat Mosquito surveillance drone that is capable of a vertical take-off and hover flight. The drone has a wingspan of 35 cm and an endurance of 40 minutes. Its payload includes a 0.15-gram color camera and memory card, and it is managed remotely. The drone is noiseless and flaps its four wings 14 times per second and is smaller compared to some natural butterflies [28].

This is one of the most dynamic areas of research and development in the UAS and new miniature drones with enhanced capabilities are introduced on a regular basis. It is not feasible to list all these drones in this chapter; however, some examples of the very small UAVs that are already used in various applications include:

- The U.S. Aurora Flight Sciences Skate (with a wingspan of 60 cm and length of 33 cm) [29];
- The Australian Cyber Technology CyberQuad Mini (with 42 × 42 cm square), and their latest model, CyberQuad Maxi [18, 30];

- The T-Hawk Micro-UAV from Honeywell, which is used by the U.S. Army and the U.S. Navy Explosive Ordnance Division to search areas for roadside bombs and inspect targets;
- The autonomous flapping-wing micro-UAV from Tamkang University in Taiwan, which weighs 8g and is 20 cm wide [29];
- The Black Hornet Nano UAV, developed by Prox Dynamics and used by the British Army to support infantry operations [31].

2.4.2.2 Small UAVs

The small UAV category includes UAVs that have at least one dimension in the range between 50 cm and 2m. Most of the small UAVs are constructed using the fixed-wing model and are usually hand-launched by throwing them in the air, as shown in Figure 2.8, where the Ukrainian border guard is launching SPECTATOR UAV made by the MERIDIAN Corporation in Ukraine.

A good example of a small UAV for target shooting is the MISHEN BERTA 08 UAV, developed by OOO ENICS in Russia. The complete UAS has the following characteristics[1]:

Figure 2.8 Launch of SPECTATOR UAV made by the Meridian Corporation. (We would like to express our gratitude to Meridian JSC in Kiev, Ukraine, for their permission to present this product.)

1. We would like to express our gratitude to OOO ENICS in Kazan, Russia, for sharing information regarding this UAV.

- Flight range: 50 km;
- Flying altitude: 1,000m;
- Number of UAVs that could be controlled simultaneously: 4;
- Flight duration: 30 minutes;
- Operating temperature: −20°C to 50°C;
- Operating team: 4 people.

A photograph of MISHEN BERTA 08 UAV is shown in Figure 2.9.

2.4.2.3 Medium UAVs

The medium UAV category includes UAVs that usually have a wingspan of up to 10m and can carry payloads up to 200 kg. There are numerous examples of these types of UAVs as almost every large defense manufacturer has its own version of the medium UAVs. A typical MALE MQ-9 Reaper made by General Atomic is a typical example of a medium UAV.

2.4.2.4 Large UAVs

The large UAV category includes large UAVs that are used primarily for combat operations. The most typical example of a large UAV will be the U.S. General Atomics Predator series and the U.S. Northrop Grumman Global Hawk. It needs to be emphasized that other countries are catching up very quickly in introducing new large combat UAVs.

Figure 2.9 MISHEN BERTA UAV. (We would like to express our gratitude to ENICS Corporation for their permission to present this product.)

References

[1] *The Free Dictionary*, "Drone," 2019, https://www.thefreedictionary.com/drone.

[2] Richard, J., "History of War," 2019, https://www.dehavillandmuseum.co.uk/aircraft/de-havilland-dh82b-queen-bee/

[3] Watts, A., L. Kobziar, and H. Percival, "Unmanned Aircraft Systems for Wildland Fire Monitoring and Research," *Proc. of 24th Tall Timbers Fire Ecology Conference: The Future of Fire: Public Awareness, Health, and Safety,* Vol. 2, 2009, pp. 86–90.

[4] Haydon, F. S., *Military Ballooning During the Early Civil War,* Johns Hopkins University Press, July 14, 2000.

[5] Bowden, D., *Encyclopaedia of War Machines: An Historical Survey of the World's Great Weapons.* London: Peerage Books, 1977.

[6] Hannavy, J., *Encyclopedia of Nineteenth-Century Photography,* London, U.K.: Routledge, Taylor & Francis Group, 2007.

[7] FliteTest, "A Brief History of Drones," February 28, 2018, https://www.flitetest.com/articles/a-brief-history-of-drones.

[8] Watts, A. C., V. G. Ambrosia, and E. A. Hinkley, "Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use," *Remote Sensing,* Vol. 4, 2012, pp. 1671–1692.

[9] Rinicom, 2019, https://www.rinicom.com.

[10] Drone Safe, 2019, http://www.dronesafe.uk.

[11] NATS, "8 Top Tips for Flying Your Drone Safely," 2019, www.nats.aero/droneflyingtips.

[12] FAA 2018, https://fas.org/sgp/crs/misc//R45207.pdf

[13] Hambling, D., *Swarm Troopers: How Small Drones Will Conquer the World,* self-published with Archangel Ink, 2015.

[14] Miller, P. M., *Mini, Micro, and Swarming Unmanned Aerial Vehicles: A Baseline Study,* Washington, D.C.: Library of Congress, Federal Research Division, November 2006.

[15] Smalley, D., U.S. Navy, "LOCUST: Autonomous, Swarming UAVs Fly into the Future," *Navy News Service*, April 14, 2015, https://www.navy.mil/submit/display.asp?story_id=86558.

[16] Rohrlich, J., "Drones Just Attacked the World's Largest Refinery," *Quartz*, September 14, 2019, https://qz.com/1709290/drones-attack-worlds-largest-oil-refinery-in-saudi-arabia/.

[17] Reuters, "Somali Militants Attack US Drone Base and European Convoy," *The Guardian*, September 30, 2019, https://www.theguardian.com/world/2019/sep/30/somali-militants-attack-us-drone-base-and-european-convoy.

[18] Hassanalian, M., and A. Abdelkefi, "Classifications, Applications, and Design Challenges of Drones: A Review," *Progress in Aerospace Sciences,* Vol. 91, 2017, pp. 99–131.

[19] Cavoukian, A., *Privacy and Drones: Unmanned Aerial Vehicles,* Ontario, Canada: Information and Privacy Commissioner of Ontario, 2012.

[20] Gupta, S. G., M. M. Ghonge, and P. M. Jawandhiya, "Review of Unmanned Aircraft System (UAS) Technology," *International Journal of Advanced Research in Computer Engineering & Technology*, Vol. 2, No. 4, 2013.
[21] Cai, G., J. Dias, and L. Seneviratne, "A Survey of Small-Scale Unmanned Aerial Vehicles: Recent Advances and Future Development Trends," *Unmanned Systems*, Vol. 2, No. 2, 2014, pp. 175–199.
[22] Arjomandi, A., et al., *Classification of Unmanned Aerial Vehicle,* Adelaide, Australia: University of Adelaide, 2006.
[23] Villa, T. F., et al., "An Overview of Small Unmanned Aerial Vehicles for Air Quality Measurements: Present Applications and Future Prospectives," *Sensors*, Vol. 16, No. 17, 2016.
[24] Stefanovic, V., M. Marjanovic, and M. Bajovic, *Conceptual System Designs Civil UAV for Typical Aerial Work Applications,* Belgrade, Serbia, 2012.
[25] Wikipedia, "Bell Boeing V-22 Osprey," 2019, https://en.wikipedia.org/wiki/Bell_Boeing_V-22_Osprey.
[26] Austin, R., *Unmanned Aircraft Systems: UAVS Design, Development and Deployment,* New York: John Wiley & Sons, 2011.
[27] U.S. Army, "U.S. Army Roadmap for Unmanned Systems 2010-2035," April 15, 2010.
[28] Top Secret Airplanes, "Israeli Mosquito – Spy Butterfly," May 17, 2013, http://topsecretairplanes.blogspot.com/2013/05/israeli-mosquito-spy-butterfly.html.
[29] Aurora Flight Sciences, 2020, https://aurora.aero/.
[30] Brandon, A., "CyberQuad: Best of Both Worlds UAV Designed for Urban Reconnaissance," *New Atlas*, December 23, 2009, https://newatlas.com/cyberquad-uav/13652/.
[31] "PD-100 Black Hornet Nano Unmanned Air Vehicle," *Army Technology*, 2020, https://www.army-technology.com/projects/pd100-black-hornet-nano/.

CHAPTER

3

Contents

Know Your Enemy

3.1 Introduction

The ancient military writer, Sun Tzu, taught [1]: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

When applied to our book, this could be interpreted as: "You will defeat all illegal drones if you know their strengths, weaknesses, and tactics as well as you know your own. If you do not understand UAVs, you will be successful in your C-UAV efforts only half of the time or less."

More specifically, when developing a C-UAV system, one must ask the following questions:

- How do we detect a drone (preferably as far away and early as possible)?
- How do we classify a drone (preferably as early and as accurately as possible)?
- How do we track a drone (preferably for as long as possible)?

- How do we detect the pilot and his or her location (preferably as accurately as possible)?
- How can we detect and classify a payload?
- What is the most appropriate countermeasure and when should we apply it?
- How do we provide evidence for forensic investigation and criminal prosecution?

To answer these questions, a comprehensive knowledge of drones is required, and this section will provide some basic information with relevant references for more in-depth study.

3.2 Drone Architecture

As described previously, there is a huge variety of drone types and drone architecture. However, despite all the differences between the various UAVs, there are common components of knowledge that are critical for developing an efficient C-UAV system. For example, as shown earlier, every UAS will consist of a UAV, a ground station, a pilot, or an operator, and the communications links between them; hence, detecting a drone, its ground station, pilot, or operator, and its communication links is the primary goal of the C-UAV systems.

A typical drone is composed of the following components:

- Engine or motors units;
- Fuel cell or battery;
- Navigation system;
- Autopilot system;
- Satellite navigation module and the corresponding satellite navigation antenna (these could be GPS [2–4] or BeiDou [5]);
- Control channel to the pilot;
- Video downlink;
- Video module (day and night cameras, recorder, and gimbal);
- Variety of sensors (these could vary from mission to mission, but most UAVs have an accelerometer, gyroscope, and barometer as standard).

The typical architecture of a UAS is presented in Figure 3.1 [6, 7]. In Figure 3.1, the following items are shown:

- *Power systems module (PSM):* This provides power for both the payloads, the motors, and flight control components. It generates a variety of voltages ranging from 5V to 27V, depending upon the type of payloads and flight components selected. Importantly, PSM also includes a backup battery system for the increased reliability and (potential) endurance of the UAV. On some UAVs with advanced power systems modules, a power distribution software is implemented, allowing one to conserve power and regulating power withdrawal per the requirements of the motor and payload.
- *Communications and surveillance module:* This includes uplink (UL) operating at 915 MHz for receiving flight commands and (in some UAVs) commands for pan-tilt modules, telemetry radio modem operating on 915 MHz, camera and digital video transmitter, operating on 1.3 GHz, and pan-tilt mechanisms for controlling the on-board camera.
- *Navigation module:* This includes the autopilot, compass, GNSS receiver, altitude meters, and air data computer (ADC).
- *Flight control module:* This includes the rudder, elevators, aileron, and throttle, all controlled by the servo board, which itself is controlled by autopilot.

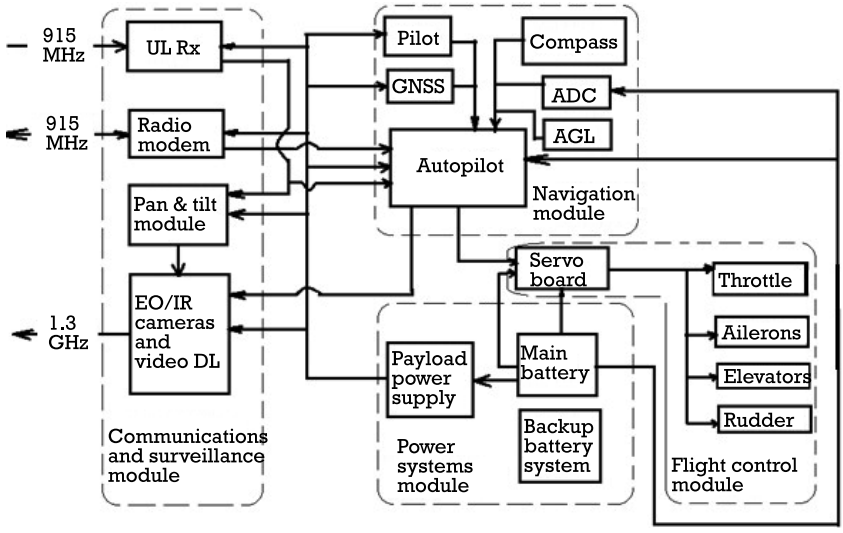

Figure 3.1 Typical UAV architecture.

3.3 UAV Propulsion System

Understanding the specifications of UAV propulsion systems and how they work is important for developers of C-UAV solutions as one of the most efficient countermeasures includes stalling the UAV's propulsion system. This could be achieved in several ways (such as kinetic, RF jamming, mechanical, and physical interception); hence, knowing the basics of UAV propulsion system can help to apply the most appropriate countermeasure.

The propulsion system of a UAV consists of the following elements [8]:

- *Source of energy:* This could be a single source or a combination of two or more sources as a hybrid source. Typical examples are electricity, fossil fuels, biofuels, solar energy, hydrogen, methanol, and energy mechanics.
- *Storage facilities:* Depending on the source of energy used, the appropriate storage facilities are implemented, such as batteries, fuel tanks, capacitors, and metal hydrides, just to name a few.
- *Mechanical energy converter:* Typical examples include fuel cells, an electric motor, and an internal combustion engine.
- *Lift/thrust converter:* The choice of these systems is defined by the type of aircraft (fixed wing, rotary, lighter than air) and includes a rotor, propeller, or jet engine (in some cases, a combination of the two).

Most of the existing UAVs use electrical batteries as the main source of energy. The preferred choice of UAV manufacturers is lithium polymer (LiPo) batteries due to their high-energy density for a given weight. As LiPo batteries are constructed by concatenation of individual cells, they provide a wide range of voltages and powers for different types of drones. A typical structure of LiPo battery is shown in Figure 3.2 [9].

As shown in this figure, a typical LiPo battery consists of individual cells where each cell is built of a special metal and chemicals that, in combination, generate an electrical power. The most common cells generate a voltage equal to 3.7V and 3 cells per battery (*3s LiPo battery*) is often used on micro-UAVs and mini-UAVs. Higher voltages are feasible by concatenation of a larger number of cells. LiPo batteries require specialized charges with a balance plug to ensure that the voltage of all the cells is balanced equally. This also helps to maximize battery lifetime by increasing the number of charges-discharges. A typical LiPo battery installed on a small quadcopter provide the following performance [10]:

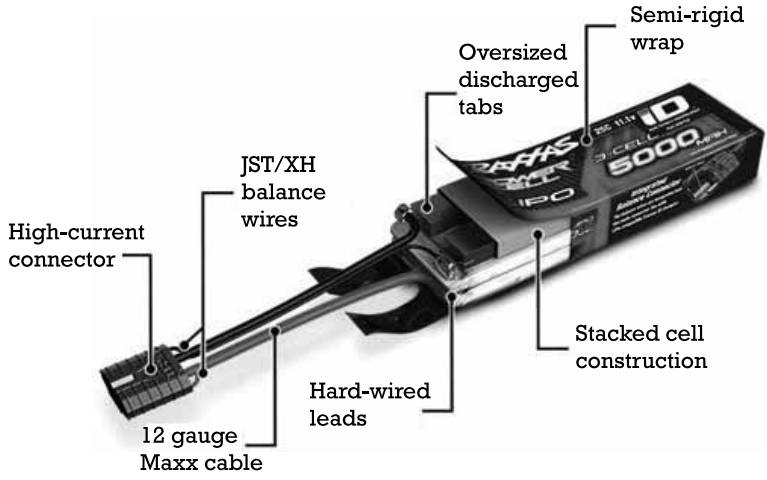

Figure 3.2 Typical LiPo battery.

- A 4-A, 4-S LiPo battery continuously generates 4A for 60 minutes at 14.7V and produces 59W.
- The same battery continuously supplies 31.5A at 14.7V and produces 460W of power for 7.0 minutes.

As the endurance of the drones is one of the key parameters, the search for new, more efficient energy sources is constantly underway. Recently introduced UAV propulsion systems based on fuel cells have attracted significant attention in recent years due to their potential to dramatically improve the efficiency of the UAV applications [11]. Figure 3.3 illustrates a block diagram of a typical propulsion system for UAVs [8, 12, 13] utilizing fuel cells.

In this example, energy is generated by hydrogen with a hydrogen tank selected as the storage facility. The mechanical energy converter is implemented as the combination of a fuel cell and an electric motor, while a propeller represents the lift/thrust converter.

The advantages of a fuel cell stimulated further research aiming at improving their efficiency, potentially extending flight times of UAVs. It was reported in [14] that a propulsion system based on fuel cells allowed up to a threefold increase of flight durations compared to LiPo batteries. These air-cooled fuel cell systems use hydrogen and ambient air to produce voltage with low harmonics and are a simple, cost-effective, robust, and lightweight alternative to LiPo batteries. They have a higher generated energy to mass ratio than battery-based systems and can be refueled in a few minutes [14].

The efficiency of the UAV in general and its propulsion system depends on numerous parameters. In this section, we will briefly describe the most

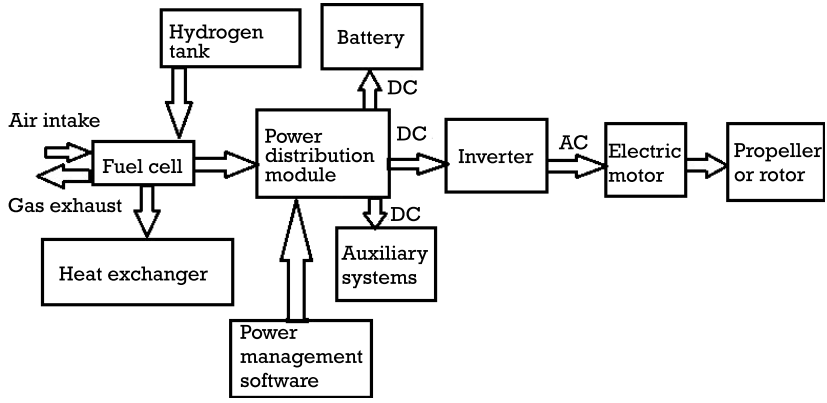

Figure 3.3 An example of a UAV propulsion system.

critical components and for a more comprehensive review will direct readers to specialized literature

The following two parameters determine the selection of motors for a UAV:

- UAV total weight;
- UAV frame size (which also defines the propeller size for VTOL UAVs).

Once these parameters are defined, it is possible to determine how much thrust the individual drone motor can generate. Typically, UAV motors are required to provide at least twice as much thrust as the weight of the UAV [15]. The minimum frame dimension defines the maximum size of the propeller. Furthermore, it is recommended to provide spaces between the propellers as overlapping the propellers will reduce the thrust efficiency of the propeller below [15]. Retrospectively, this can be used to define kinetic efforts that need to be applied to this UAV as part of the neutralization by the C-UAV.

Another important parameter of a UAV motor is the electric motor efficiency, which is defined as the ratio between the mechanical power output and the electrical power input [15]. Knowing these parameters will help to estimate the battery life (or endurance) of the UAV and apply the most appropriate countermeasure. The summarized power requirements for the most commonly used UAVs are shown in Table 3.1.

As follows from Table 3.1, a wide variety of UAVs requires different types of propulsion systems, which is intuitively expected. However, the variety of propulsion systems generates additional challenges for the developers of countermeasures as an integral part of C-UAV systems. Obviously,

Table 3.1
Summarized Power Requirements for the Most Common UAVs

Type of UAV	Power Requirement
Mini-UAV	1 kW
Helicopter UAV	1 kW
Medium UAV	5 to 10 kW
Airship UAV	<10 kW
HALE UAV	>10 kW

kinetic-based countermeasures developed for nano-UAV or mini-UAV will be less efficient when neutralizing medium or HALE-type UAVs. These would need to be considered when deriving requirements for C-UAV systems, clearly defining the types of drones that need to be neutralized by the system.

3.4 Navigation Systems for Drones

3.4.1 Introduction

All modern drones have an on-board navigation system, which is used for flight planning, location and positioning, autonomous flights, and target detection. Navigation for UAVs is defined as a process consisting of the following three steps [16]:

- Setting up a flight plan that needs to be executed;
- Determining the UAV's location and position relative to the defined flight plan;
- Maintaining the implementation of the defined flight plan and correcting all unexpected deviations from the flight plan.

Navigation systems have been used since humans started traveling. The first navigation systems were utilizing beacons, such as landmarks and stars in the sky. These were followed by purpose-built beacons, such as lighthouses and radio navigation radars for aircraft, to name a few. These techniques have evolved dramatically and, in the modern day, there are several different types of navigation systems [16]:

- *Pilotage:* This is navigation based on visual ground landmarks or specially designed references.

- *Astronavigation:* This is navigation based on angular measurements taken between a celestial body (the sun, the moon, a star) and the visible horizon.
- *Dead reckoning:* This is navigation that uses visual checkpoints (starting point) along with speed, time traveled, and heading measures to calculate the distance traveled.
- *Inertial navigation:* This is an on-board navigation system that fuses data from various sensors (speedometer, altitude meter, accelerometers, gyroscopes, and magnetometers) in order to give the current location relative to a known start point.
- *Radio aided navigation:* This is a navigation system that uses radio signals from various beacons (ground-based radars, satellite-based systems) to evaluate the current position.

Navigation is a well-developed subject, which is significantly broader compared to the scope of this book [17–19]. Therefore, in this section, we will address only topics that are relevant to the navigation of UAVs in general and counter-UAV systems in particular. As such, we will provide an overview of the navigation systems utilized in modern UAVs.

3.4.2 Satellite Navigation

Satellite navigation, also known as Global Navigation Satellite System (GNSS), is the most common navigation type used in most UAVs in the same way as it is used in smart phones and cars. The main aim of the system is to determine the position (longitude, latitude, altitude), velocity, and timing of the UAV utilizing one or several existing satellite navigation systems, such as GPS [2], GLONASS [3], GALILEO [4], and Beidou [5]. All existing satellite navigation systems use satellites as beacons, which send dedicated radio signals utilized in GNSS receivers.

More specifically, GNSS is based on a constellation that includes several medium Earth orbit (MEO) satellites spread between several orbital planes and numerous ground stations. The number of satellites and ground stations varies from system to system, depending on the required Earth coverage, accuracy, applications, and other criteria. For example, the GPS constellation consists of 32 satellites covering the whole planet while the GLONASS constellation consists of only 24 satellites located on 3 orbital planes and covering primarily the Northern Hemisphere [20]. Figure 3.4 illustrates GPS and GLONASS constellations.

GNSS provides high accuracy in determining the location of a UAV by using time signals transmitted by the satellites and the concept of

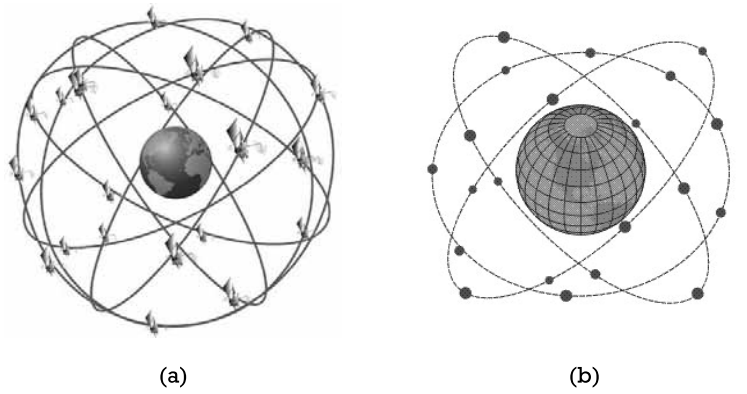

Figure 3.4 GNSS constellations: (a) GPS, and (b) GLONASS. (We would like to express our gratitude to www.gisgeography.com for their permission to use this photograph.

triangulation. Triangulation is a way of determining someone's location by forming triangles to the point from known beacons [21]. Figure 3.5 illustrates the construction of triangles between the UAV, satellites, and a ground station.

To determine a UAV's location, an on-board GPS receiver measures with high accuracy the time that it takes for a signal transmitted from the

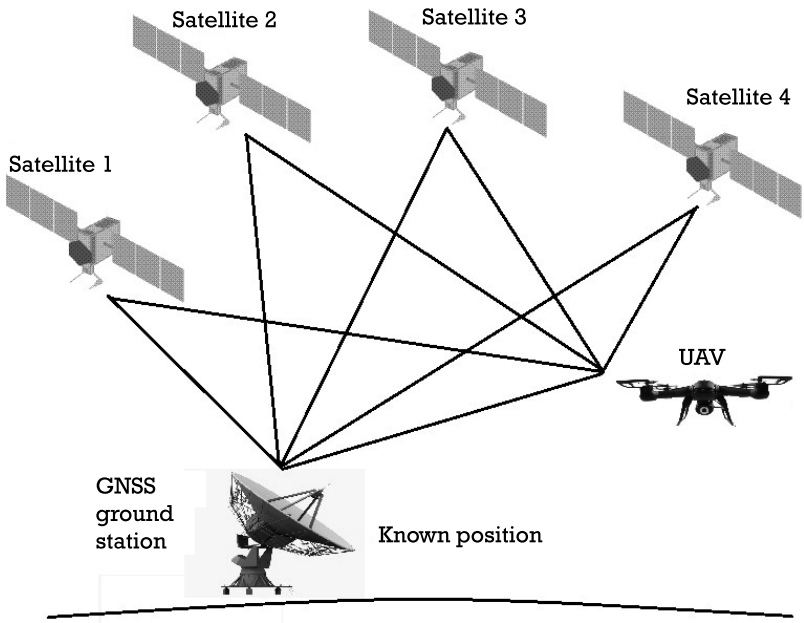

Figure 3.5 Example of triangulation in GNSS.

satellite (that contains orbital data) and the ground station to reach the UAV (usually less than 100 m/s). Assuming that radio waves propagate in open space with a speed of 300,000 km/sec, the measured propagation time is multiplied by the speed of radio waves to obtain the distance between the UAV and the satellite. This puts the receiver somewhere on the surface of an imaginary sphere with a radius equal to the calculated distance. Similar calculations are completed with signals from three other satellites and the crossing point of four imaginary spheres will determine the UAV's current longitude, latitude, and altitude as shown in Figure 3.6. (Note that, for in-car based navigation systems, signals from three satellites are sufficient to determine the location on the Earth's surface; however, if an object is above the Earth's surface and the knowledge of altitude is required, then the signals from the fourth satellite are essential.)

In addition to orbital signals (which are used for the calculation of the satellite's position), the satellite or ground station transmits a dedicated

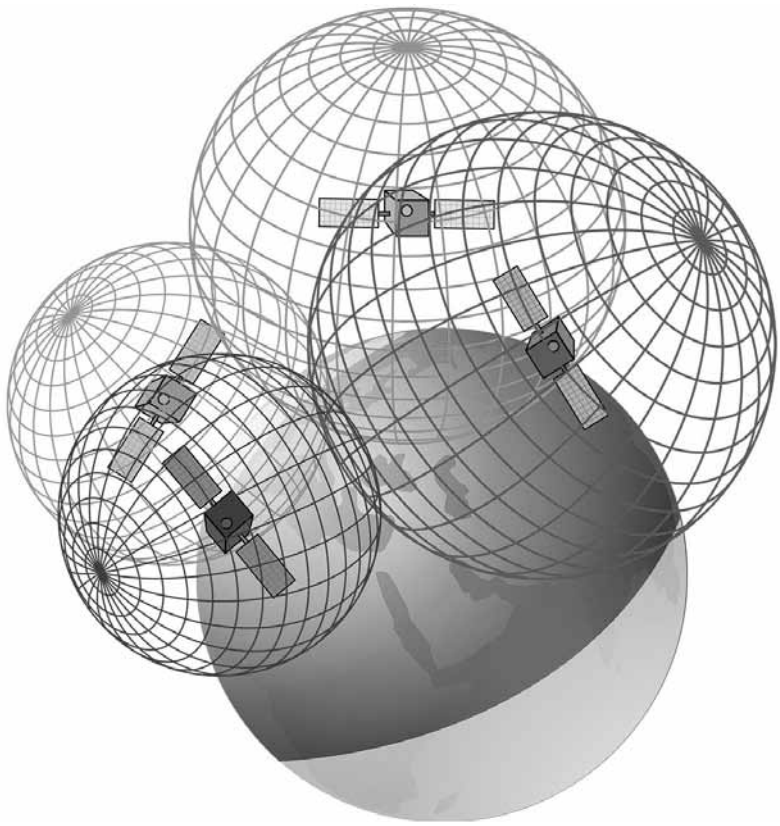

Figure 3.6 Triangulation calculations for UAVs. (We would like to express our gratitude to www.gisgeography.com for their permission to use this photograph.)

synchronization signal that serves as a timing reference and is used to accurately calculate the current local time. All satellites in the constellation use atomic clocks to maintain synchronization of all satellites and ground stations. The combined relative motion of the satellites used in triangulation also creates Doppler shifts [19], which are measured by the on-board receiver and are critical for calculating UAV velocity and direction of movement.

Despite the relatively simple concept, GNSS is a complex system consisting of numerous subsystems, such as:

- Constellation of satellites;
- On-ground auxiliary system (maintenance);
- The UAV's GNSS receiver;
- Augmentation systems:
  - *Air-based augmentation system (ABAS):* This processes the GNSS signals in order to check the integrity.
  - *Satellite-based augmentation system (SBAS):* This uses GNSS measurements by referencing ground stations deployed across the GNSS coverage area to detect GNSS errors and complement the original GNSS message in the covered area.
  - *Ground-based augmentation system (GBAS):* This is similar to SBAS but uses very high-frequency (VHF) and ultrahigh-frequency (UHF) bands to complement the original GNSS signals on the covered area.

All the above-mentioned GNSS systems utilize the same principle and the main difference is usually in the number of satellites in the constellation, the coverage area, the operating frequency, and the signal bandwidth. For example, Tables 3.2 and 3.3 illustrate GPS and GLONASS frequency bands [22].

Knowledge of these parameters is of particular importance for developing jamming countermeasures in C-UAV systems as the utilization of the jamming power is dependent on the accuracy and precision of the frequency and bandwidth.

However, modern navigation systems utilize signals from more than a single GNSS to improve navigation accuracy and robustness against jamming (for example, if a UAV navigation system utilises receivers with both GPS and GLONASS chipsets, jamming only the GPS signals will not affect the GLONASS navigation and the C-UAV system will fail its objective). Therefore, the developers of C-UAV jamming solutions should include multi-GNSS jamming options as part of the overall solution.

Table 3.2
GPS Frequency Bands

System/Band	Frequency, Bandwidth
GPS L1	1,575.42 MHz, 15.345 MHz
GPS L2	1,227.6 MHz, 11 MHz
GPS L5	1,176.45 MHz, 12.5 MHz

Table 3.3
GLONASS Frequency Bands

System/Band	Frequency, Bandwidth
GLONASS I-L1	1,602 MHz, 6.5 MHz
GLONASS I-L2	1,246 MHz, 5 MHz
GLONASS II-L1	1,575.42 MHz, 6.5 MHz
GLONASS II-L1	1,600.995 MHz, 15.365 MHz
GLONASS II-L2	1,248.06 MHz, 8.75 MHz
GLONASS II-L3	1,202.025 MHz, 20.46 MHz
GLONASS II-L5	1,176.45 MHz, 10.22 MHz

3.4.3 Non-GPS-Based Navigation

GNSS-based navigation systems provide obvious benefits to UAV users. However, in many applications, the use of GNSS navigation is not recommended or is not feasible, which generates strong interest in alternative, non-GNSS-based navigation systems. Unsurprisingly, nonlegitimate users of UAVs also have a strong interest in achieving their goals without the reliance of GNSS (which could be jammed or spoofed), generating strong stimulus in developing non-GNSS-based navigation systems for UAVs. Although these systems are still in the development or early adoption phase, from a C-UAV system development perspective, it is essential to ensure that the developed C-UAV system will be capable of neutralizing UAVs that are not using GNSS-based navigation.

Traditionally, non-GNSS systems are using an inertial navigation system (INS). The most common INSs use accelerometers to determine acceleration and gyroscopes to determine angular rotation [23]. The generic block diagram of an INS is shown in Figure 3.7.

As shown in Figure 3.7, the accelerometers and gyroscopes are packaged together into an inertial measurement unit (IMU), which provides the information required for calculation of navigation parameters. If the initial position is known at the start of the journey, an INS can determine the position, orientation, and angular velocity using the IMU readings, elapsed time, and results of navigation calculations. The main problem with an INS is in the accumulation of errors and degradation of accuracy over time. Therefore, maintaining the required accuracy regular recalibrations during the

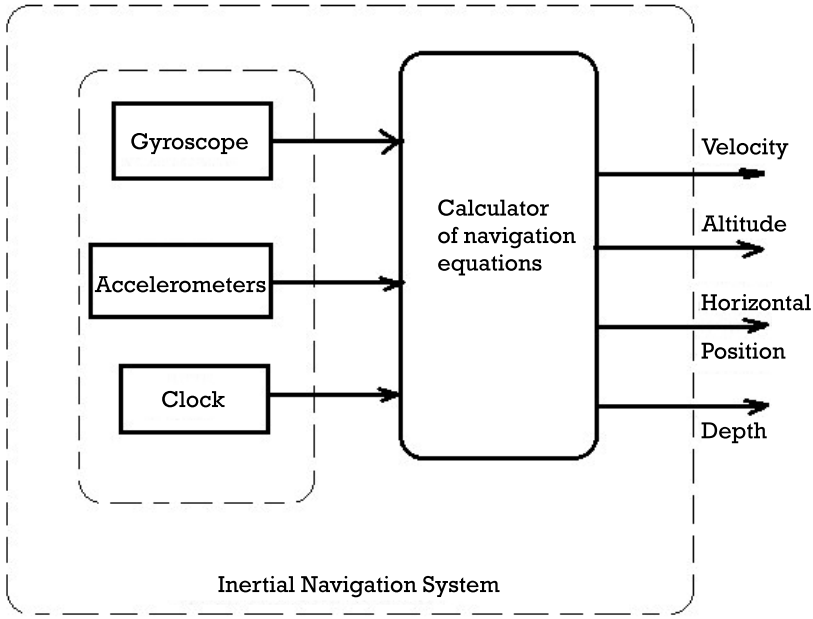

Figure 3.7 Block diagram of a typical INU.

flight is required. To achieve this, the most advanced UAVs have combined a satellite navigation receiver with an INS. During the times that the satellite signal is not available or could be jammed, the INS takes over. However, to compensate for accumulated errors in the INS, combined GNSS/IMS fusion algorithms are being developed to utilize the benefits of both technologies.

Another promising type of non-GNSS-based navigation is image-aided navigation (IAN), which utilizes electro-optical and infrared (EO/IR) sensors to generate measurements of three-dimensional (3-D) terrain imagery to navigate. The EO/IR sensor images are correlated with the stored imagery map and an error is calculated and used to calibrate an INS. This method does not require any additional ground-based infrastructure and can be fused with INS systems. The accuracy of this method depends on the richness of the pre-installed imagery map and terrain and does not work well in poor landmark environments, such as deserts or the ocean [24]. A good example of such a system would be the system currently being developed by GPU maker NVDIA, which relies on visual recognition and the JETSON TX1 computer learning module to process data from two on-board cameras. Although the system is still in the development stages, early trials have shown satisfactory performance in demonstration flights in a deep forest, where UAVs managed to successfully navigate between the trees [25].

Another alternative navigation system is being developed in Australia by Locata Corporation [26]. A network of terrestrial-based transceivers forms a positioning network that operates either in combination with GNSS or totally independent of GNSS (e.g., indoors or in urban areas), providing centimeter accuracy. As the signals are 10^6 times stronger than GNSS signals, the system is very reliable and hard to jam. A conceptual diagram of LOCATA is shown in Figure 3.8.

A similar approach is taken by the U.K.-based BAE Systems, which has introduced a UAV navigation and positioning system that uses signals of opportunity called Navigation Signals of Opportunity (NAVSOP) [27]. Although the system shows good performance in the majority of cases, its performance deteriorates when a signal from one particular source (for example, a cellular base station) dominates other signals and triangulation is not feasible.

One of the most promising alternative navigation systems (although still in the very early stages of development as of the time of this writing) is the quantum navigation system. The system utilizes lasers that can trap and cool a cloud of atoms placed in a vacuum to a fraction of a degree above absolute zero. Once chilled, the atoms achieve a quantum state that is easily perturbed by an outside force and another laser beam can then be used to track them. The system monitors changes caused by a perturbation and the detected changes are used to estimate the outside force [28]. The system already shows remarkable performance in laboratory and early trials environments; however, its current size and weight are not suitable for UAV applications.

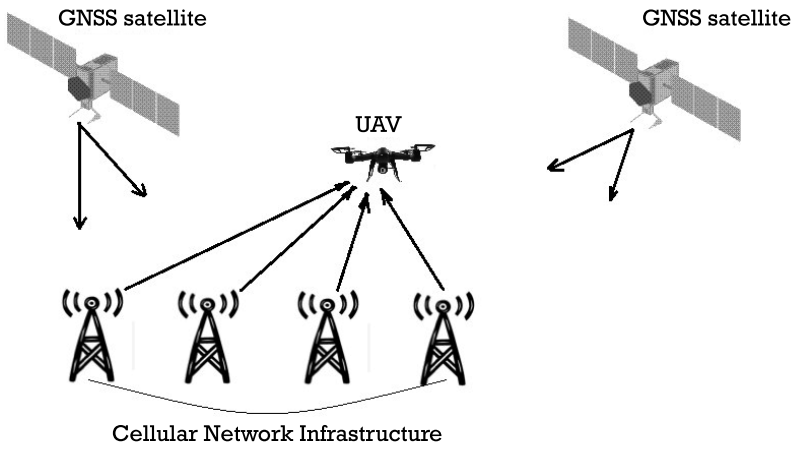

Figure 3.8 Conceptual diagram of LOCATA.

3.5 Communication Links

3.5.1 Introduction

Most of the modern UAVs have a number of communication systems that are used for various applications:

- Flight control and command channel with the ground station;
- Communications with other UAVs in the swarm;
- Video and data links;
- Telemetry channels for sensory data.

Usually, telemetry and command channels are implemented separately from the video data link and sensory channels. However, in some consumer nano-UAVs and mini-UAVs, these channels are combined (for example, flight control and sensory telemetry channels). In UAVs that are used for mission-critical operations, these systems usually operate on different frequencies with different communication protocols to ensure the reliability and robustness of communications.

As in all radio communication systems, communication links for UAVs must operate in the designated frequency bands assigned by the respected regulatory bodies, such as Ofcom (Office of Communications) in the United Kingdom or the Federal Communications Commission (FCC) in the United States. For civilian UAV applications, the following frequencies are assigned:

- 2.4–2.485 GHz: spread spectrum band for general control;
- 900 MHz, 1.2 GHz, 2.4 GHz, 5.8 GHz: communications for payload and video transmission;
- 433 MHz or 869 MHz: telemetry transmission;
- 5,030–5,091 MHz: for small unmanned aircraft systems (under consideration by the FCC).

3.5.2 UAV Control

UAV command and control signals do not require wide bandwidth but instead require very high reliability and link availability over long-distance ranges. It is worth mentioning that command and control data rate requirements are different for uplink (UL) and downlink (DL) channels as the UL is used to control the UAV, to change the flight plan as required and to protect from unauthorized use by encryption protocols. The bandwidth

requirements are also different for various phases of the flight as the data rate requirement for en route is far lower than for the departure and arrival flight phase. This is because additional information (such as GPS synchronization) is transmitted during departure and arrival but not during the en route flight phase. For example [29], during a possible collision or a system problem, a UAV will be sending four messages per second; on takeoff and landing, the same UAV will be sending one GPS synchronized message per second; and en route during the mission, the UAV will be sending only one message every 10 seconds. Furthermore, the retransmission rate for departure and arrival is typically twice as high as for the en route phase, while in automatic mode (AM), the data rate requirement is lower than for manual mode (MM), as reports are sent up to 20 times less frequently [30].

Table 3.4 lists the raw data (no overheads) rate r equirement for telemetry and telecommand links (note: data rates are given in bits per second) [30].

The most popular command and control data links currently used in UAVs are 433 MHz, 869 MHz, and 900 MHz. In these frequency bands, long-distance ranges (up to 75 km) could be achieved with relatively small output transmission power (and hence not draining the UAV battery) in very challenging environments, such as urban, wooded, or mountainous areas.

From a C-UAV perspective, a knowledge of command and control communication links is essential for drone detection and classification, while the neutralization of these links should be among the tools offered by the C-UAV system.

3.5.3 Video Transmission

Video transmission links have evolved from legacy analog video transmission systems to unidirectional coded orthogonal frequency division multiplexing (COFDM) data links with integrated MPEG-2/MPEG-4 video codecs, to bidirectional IP-based COFDM links capable of transmitting multiple high-definition (HD) video streams [31–35]. The utilization of COFDM, which

Table 3.4
UAV Control Bandwidth Requirements

	Flight Phase					
	Departure		**En Route**		**Arrival**	
	AM	**MM**	**AM**	**MM**	**AM**	**MM**
DL Telemetry	480	3,008	280	1,240	672	4,008
UL Telecommand	408	1,256	152	632	656	2,424

was initially developed for digital TV [36], was a big step that dramatically increased the range of applications where UAVs could be used.

The basic principle of COFDM is to divide the available channel bandwidth into a number of subchannels (subcarriers) and to demultiplex the input high-rate information data into these subchannels. By choosing the number of subcarriers to be very large (on the order of a few thousand), the symbol duration will increase correspondingly and the component subchannels will be very narrow band with almost flat fading. This reduces the relative amount of dispersion in time caused by multipath delay spread and makes the equalization process relatively simple [36]. To obtain a high spectral efficiency, the spectral responses of the component subchannels must be overlapping and orthogonal.

In order to eliminate intersymbol interference, a guard interval is introduced in every COFDM symbol. This guard interval must be longer than the expected delay spread of the signal. In this case, multipath components between the two neighboring symbols cannot interfere with each other, while the effect of the Doppler shift caused by a relative movement between the COFDM transmitter and receiver could be controlled by changing guard intervals.

If no symbol is transmitted during the guard interval, the orthogonality between the subcarriers will be lost, resulting in interchannel interference. In order to eliminate interchannel interference, the COFDM system is cyclically extended in the guard interval by introducing a cyclic prefix [37]. This prefix is a copy of the last part of the COFDM symbol as shown in Figure 3.9.

The most popular COFDM data links in UAVs operate in the 1.3-GHz, 2.4-GHz, and 5.8-GHz frequency bands. It is worth mentioning that 2.4-GHz and 5.8-GHz bands are used primarily by nano-UAVs and small UAVs utilizing Wi-Fi signals with all the advantages and drawbacks of Wi-Fi. Most nonconsumer UAVs use the 1.3-GHz frequency band with COFDM links en-

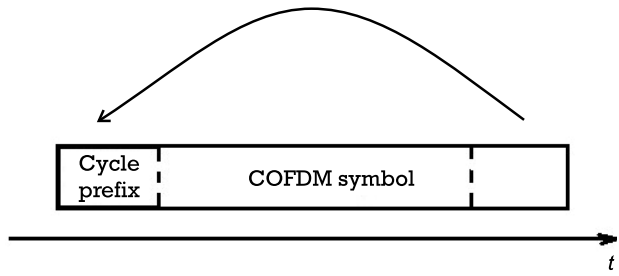

Figure 3.9 Insertion of the cyclic prefix.

hanced with a dedicated encryption (typically AES-256) reaching distance ranges of close to 100 km with a 1-W, on-board power amplifier [34].

Some UAVs carry more than one camera as part of the payload. These could be EO/IR cameras for surveillance and a dedicated camera for sense and avoidance in automatic mode. Therefore, video data links must be capable of transmitting more than one video stream simultaneously, which brings additional requirements for the channel bandwidth such as prioritization of video streams in the required bandwidth and fast download of the recorded videos.

The advantages and drawbacks of other frequencies are summarized in Table 3.5.

3.5.4 Communication Systems for Military UAVs

Compared to civilian drones, military drones' missions are frequently longer in duration and often require striking capabilities in addition to providing aerial visuals of the battlefield below. Military UAVs are expected to operate in the presence of signal jamming, which puts additional requirements on the communication links. When signal jamming is applied, it may affect both the control and video data links. Therefore, most military UAVs are designed to return to base after a loss of communications contact or switch to autonomous flight mode utilizing INS [38]. Another challenge in military applications is the required interoperability between tactical UAS systems among the allied forces as, traditionally, military UAS have been developed by various vendors with proprietary telemetry and sensor data streams. Consequently, systems lack the ability to interoperate with each other, reducing capabilities for asset sharing by allied nations and diversifying the UAS concept of operations.

To address these challenges, in 1998, a NATO Specialist Team comprising members of government and industry began work on the NATO Standardization Agreement 4586 (known as STANAG-4586), which defines the standard for the interface of the unmanned control system (UCS) UAV interoperability [39]. It defines architectures, interfaces, communication pro-

Table 3.5
Advantages and Drawbacks of Other Frequency Bands

Frequency Band	Distance Range	Comments
3 GHz	40+ miles	Strong penetration capabilities
4 GHz	15+ miles	Potential interference with 2.4-GHz links used for control
8 GHz	5+ miles	Power performance in non-line-of-sight conditions

tocols, data elements, and message formats. It includes data link, command and control, and human/computer interfaces.

The STANAG-4586 defines five levels of interoperability (LOI), which represent the degree of control that a user has over the UAV, its payload, or both. These LOIs are defined as:

- Level 1: Indirect receipt/transmission of UAV-related data and metadata;
- Level 2: Direct receipt/transmission of UAV-related data and metadata;
- Level 3: Control and monitoring of the UAV payload, not the unit;
- Level 4: Control and monitoring of the UAV without launch and recovery;
- Level 5: Control and monitoring of the UAV including launch and recovery.

STANAG-4586 does not regulate UAS hardware, software, design, or materials. Instead, the objective of this standard is to specify UAS control system architecture, data link interfaces, command control (C2) interface, and human control interface (HCI).

A typical military UAV communications payload system is shown in Figure 3.10 [38].

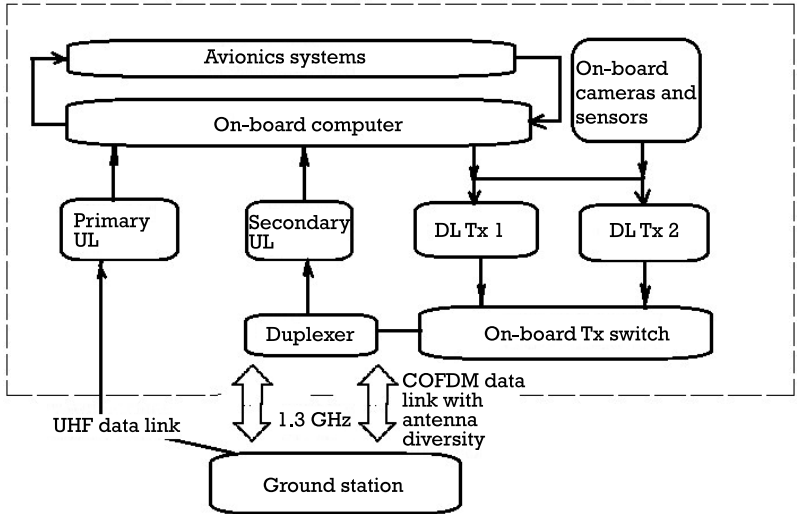

Figure 3.10 Military UAV communications payload.

As shown in Figure 3.10, a typical military UAV has two ULs in low and high-frequency bands (UHF and C/L/S/Q/KU) and one DL in a high-frequency band (C/L/S/Q/KU). This is to increase the reliability of the UAV control (which is done over UL) as the loss of UL may lead to the loss of the UAV. Both ULs transmit simultaneously on different frequencies. As a result of this configuration, UAVs have one UHF antenna for UL and one integrated high-frequency antenna (C/L/S/Q/KU) for both the UL and DL high-frequency channels (C/L/S/Q/KU).

3.5.5 Communications for Swarm of UAVs

As mentioned above, swarms of UAVs are expected to replace legacy UAVs in various operational scenario, eliminating the drawbacks of conventional single UAV solutions:

- Limited payload;
- Limited flight time;
- Need for remote pilot to operate UAV.

However, it provided the following advantages [40]:

- Time savings;
- Reduction in man-hours;
- Reduction in labor and a reduction in other associated operational expenses.

However, these advantages can only be realized by making significant changes to UAV architectures, including changes to UAV communication links. In Figure 3.11, we present a typical communication architecture for a legacy single UAV.

The typical communications architecture for a swarm of UAVs is shown in Figure 3.12.

As follows from these figures, communications systems for swarms of UAVs should be able to cope with the following challenges:

- Bandwidth sharing on the control channel between numerous UAVs in the swarm;
- Communications between the UAVs in the swarm;

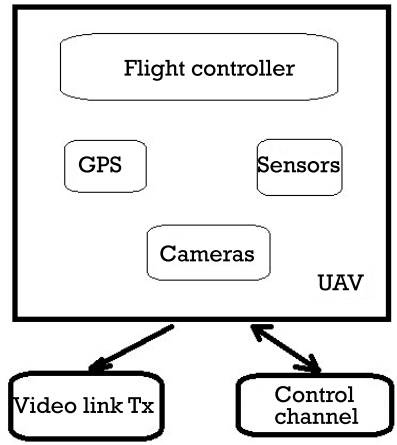

Figure 3.11 Typical communications architecture of a UAV.

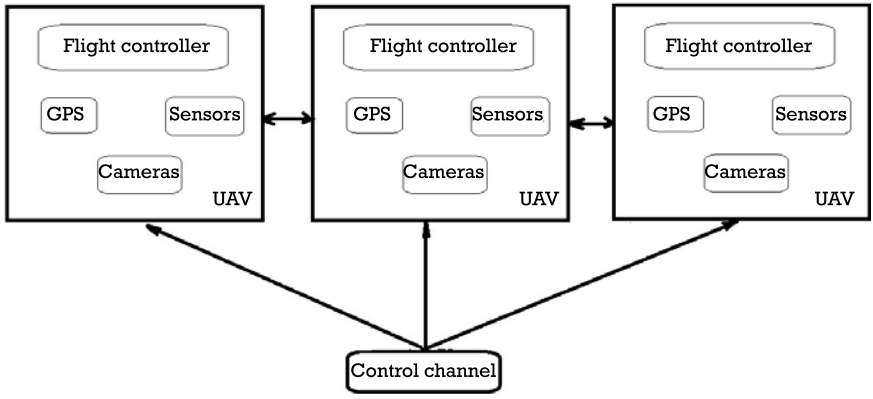

Figure 3.12 Communications architecture for a swarm of UAVs.

- Quality of service and adaptive prioritization depending on the mission scenario.

The only solution that could meet all these requirements without relying on additional ground infrastructure is dynamic ad hoc IP mesh networks with smart routing protocols [34]. A wireless ad hoc network (sometimes also called infrastructureless communications network) is a wireless network that does not rely on existing infrastructure to establish and maintain

the network. It does not require routers or access points, and its nodes are dynamically assigned and reassigned based on dynamic routing algorithms.

In [41, 42], such a flying ad hoc network, called FANET, is proposed to provide communication links between all the UAVs in a swarm. In FANET, all UAVs are communicating with each without any centralized access point or ground infrastructure. Theoretically, all the UAVs can communicate with a ground base station, but, in practice, it is sufficient for only one UAV to be connected to the ground station as shown in Figure 3.13 [40].

To support communication between all UAVs that are constantly changing their position in the swarm, a distributed decision-making system, which is not dependent upon any pre-installed infrastructure, is required. This allows the use of swarms in various scenarios without advance preparation. However, dynamic routing in a swarm often leads to a packet loss, which could be a limiting factor in applications where accurate data exchange between the UAVs is essential.

To address this issue, a hybrid approach utilizing dynamic ad hoc networks with ground-based infrastructure is promising the required performance. Such a solution is proposed in [40] where the telemetry of each UAV is communicated to every other UAV via cellular mobile infrastructure, as shown in Figure 3.14.

Similar approach is proposed by the EUROCAE WG-105 standardization group, which considers the LTE ground infrastructure for command control and communication links of UAVs [43]. The limiting factor for such an approach is the availability of ground infrastructure.

However, with the emerging availability of 5G networks, which will have sufficient ground-based infrastructure, the integration of FANET with 5G infrastructure could bring very promising results opening new opportunities for swarms of UAVs.

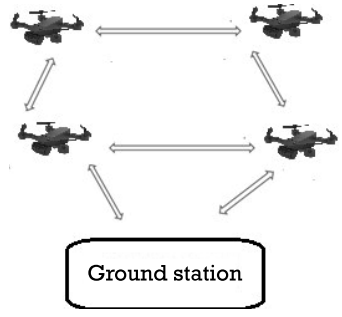

Figure 3.13 FANET configuration.

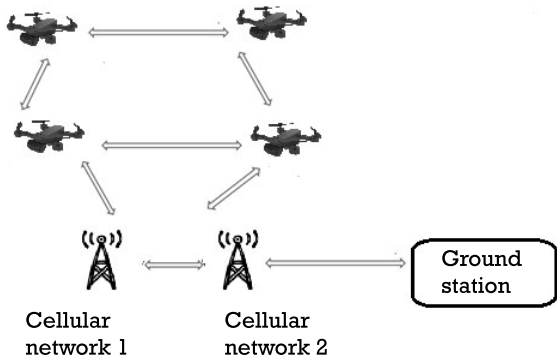

Figure 3.14 Hybrid mesh-cellular swarm network.

3.6 UAV Payload

It is not feasible to explain all possible types of UAV payloads in one section; the topic of UAV payloads could be a whole book by itself. Therefore, we will address this subject briefly from the point of C-UAV system developers and operators.

In some C-UAV scenarios, the neutralization of a UAV (for example, shooting down) could result in a significant collateral damage or chemical, biological, radiological, nuclear, and explosive (CBRNE) safety threat. At the same time, in many threat scenarios, it will be sufficient to eliminate the relevant on-board sensors rather than the UAV itself. For example, when dealing with intruder drones that disturb privacy of celebrities or aim to obtain an unauthorized recording of restricted events (concerts, weddings), it will be sufficient to neutralize the on-board camera or video data link rather than shooting down the UAV. Therefore, knowing the types of payloads is critical for successful C-UAV operation.

The payload is the weight that a UAV can carry in addition of the weight of the UAV frame itself [44]. It includes anything additional to the drone, such as extra cameras, sensors, or packages for delivery. Therefore, the greater a payload that a UAV can carry, the highly operational flexibility it can provide by carrying specific tools required for operation. Like in all aspects of life, this a complex question that requires careful considerations and compromises. For example, increasing the weight of payload will increase operational capabilities of a UAV, while at the same time decreasing its flight time and eventually decreasing operation capabilities. Hence, there is always a trade-off between the weight of the payload and the required flight time.

Usually, UAV payloads are classified as:

- Essential for flying;
- Essential for providing the required services.

Payloads essential for flying were described in previous sections and usually include:

- GNSS receiver;
- GNSS antenna;
- INS;
- Cameras for visual navigation.

Payloads essential for providing services are more diverse and include:

- Stabilized EO/IR cameras;
- Sensors of all types (CBRNE, spectrum analyzers);
- LIDAR;
- Radar;
- Delivery packages;
- Anything else that is required for providing services, such as a spraying system for agricultural use or first aid for medical use.

The most used UAV payload is the stabilized camera. There are a huge variety of these cameras, ranging from of the shelf GoPro cameras with every increasing resolution to specialized custom-made cameras combined with UAVs' stabilization system and allowing PTZ capabilities without heavy and inertial mechanical parts [34]. As not all sensors are required on all UAV missions, many UAVs are designed to carry various payloads, which could be added or removed when required. For more detailed information, the reader is addressed to the more specific literature [44, 45].

3.7 Summary

In Part II, we demonstrated that UAV technology is not standing still and we provided a brief overview of various technologies that are essential for understanding UAVs and developing suitable C-UAV solutions for neutralizing

unlawfully flying UAVs. As the UAV market expands dramatically and the range of new UAVs being introduced to the market is more diverse, we focused on general concepts and features of UAVs that are common for all types of UAVs. We dedicated a significant portion of Part II to the classification of UAVs, as no single C-UAV system can be efficient against all types of UAVs, and it is critical to specify against which UAVs the desired C-UAV system is intended to be used.

We dedicated a substantial part to UAV navigation systems as neutralizing a navigation system is still one of the preferred counter-UAV measures. We also show that market expansion is based on new technological advances that create additional new challenges for the developers of C-UAV systems. We included a special section on non-GNSS based navigation as UAVs capable to operate in a GNSS-denied environment will be resilient to all RF jamming systems currently being developed for C-UAV applications.

Part II also addressed communication links for UAVs as the neutralization of communications links could be efficient and not very expensive solution in neutralizing UAVs in many applications. We show that the introduction of swarms of UAVs and 5G cellular technologies will create new challenges as LTE/5G-enabled swarms have almost no limits on communication ranges and jamming these drones will mean jamming existing networks, which may result in a bigger collateral damage.

We show that the introduction of swarms of UAVs creates new challenges, specifically in the defense environment. For example, a swarm of drones will be difficult to neutralize by interceptor drones as the number of UAVs in the swarm is likely to be larger than the capture capacity of interceptor drones.

Finally, we suggest that the proliferation of C-UAV technologies will also accelerate the development of new UAVs, which will be capable of countering the C-UAV systems, and this chase will go on for a foreseeable future.

References

[1] Tzu, S., *The Art of War,* Maple Classics, 2012.

[2] Kaplan, E., *Understanding GPS: Principles and Applications,* Norwood, MA: Artech House, 1996.

[3] Polischuk, G. M., et al., *The Global Navigation System Glonass: Development and Usage in the 21st Century*, December 2002, https://apps.dtic.mil/dtic/tr/fulltext/u2/a484380.pdf.

[4] GALILEO GNSS, 2019, https://galileognss.eu/.

[5] China National Space Administration, *The Construction of BeiDou Navigation System Steps into Important Stage: "Three Steps" Development Guideline Clear and Certain* (in Chinese), 2010.

[6] Bamberger, R. J., et al., "Flight Demonstration of Unmanned Aerial Vehicle Swarming Concepts," *John Hopkins APL Technical Digest*, Vol. 27, No. 1, 2006.

[7] Teh, S. K., et al., "Experiments in Integrating Autonomous Uninhabited Aerial Vehicles (UAVs) and Wireless Sensor Networks," *Australasian Conference on Robotics and Automation*, Canberra, Australia, 2008.

[8] González-Espasandín, Ó., T. J. Leo, and E. Navarro-Arévalo, "Fuel Cells: A Real Option for Unmanned Aerial Vehicles Propulsion," *The Scientific World Journal*, 2014, p. 12.

[9] Drone Battery, "What Is a LiPo Battery?" *RC Drone & FPV Lipo Battery,* December 21, 2016, https://dronebattery.wordpress.com/2016/12/21/what-is-a-lipo-battery/.

[10] Goli, N., *Development of an Integrated UAS for Agricultural Imaging Applications,* Huntsville, AL: University of Alabama, 2015.

[11] Roessler, C., J. Shoemann, and H. Beier, "Aerospace Applications of Hydrogen and Fuel Cells," *Hydrogen and Fuel Cells*, 2010, pp. 661–680.

[12] Navarro Arévalo, E., O. Mosquera, and A. di Bernardi, "Diferentes opciones de propulsion para una future aviación general con sensibilidad ambiental," *2nd Congreso Argentino de Ingeniería Aeronáutica*, Córdoba, Argentina, November 2010.

[13] González-Espasandin, Ó., T. J. Leo, and E. Navarro, "Fuel Cells: Alternative Propulsion for Unmanned Aerial Vehicles," *Proc. on Workshop on Research, Development and Education on Unmanned Aerial Systems (RED-UAS '11)*, Seville, Spain, November-December 2011.

[14] Intelligent Energy, "Fuel Cell Powers for UAVs," 2019, https://www.intelligent-energy.com/our-products/uavs/.

[15] Drone Omega, "The Beginner's Guide to Drone Motor Essentials," 2019, https://www.droneomega.com/drone-motor-essentials/.

[16] UAV Navigation, "Global Navigation Satellite System (GNSS)," 2019, https://www.uavnavigation.com/support/kb/general/general-system-info/global-navigation-satellite-system-gnss.

[17] Bhatta, B., *Global Navigation Satellite Systems: Insights into GPS, GLONASS, Galileo,* Boca Raton, FL: CRC Press, 2011.

[18] Teunissen, P. J. G., and O. Montenbruck, (eds.), *Handbook of Global Navigation Satellite Systems,* New York: Springer, 2017.

[19] Re, E., and M. Ruggieri, *Satellite Communications and Navigation Systems,* New York: Springer, 2007.

[20] Bhatta, B., *Global Navigation Satellite Systems: Insights into GPS, GLONASS, Galileo,* Boca Raton, FL: CRC Press, 2011.

[21] Britannica, "Triangulation," *Encyclopaedia Britannica*, 2019, https://www.britannica.com/topic/triangulation-navigation.

[22] "GNSS Frequency Band | GPS Frequency Band-GPS L1, GPS L2," *RF Wireless World*, 2019, https://www.rfwireless-world.com/Terminology/GPS-Frequency-Band-and-GNSS-Frequency-Band.html.

[23] Le Mieux, J., "Explaining the Alternatives for UAV Navigation," *Defence iQ*, August 28, 2012, https://www.defenceiq.com/air-forces-military-aircraft/articles/explaining-the-alternatives-for-uav-navigation.
[24] Krajnık, T., et al., "A Simple Visual Navigation System for an UAV," *International Multi-Conference on Systems, Signals & Devices*, 2012.
[25] Ridden, P., "Nvidia's Autonomous Drone Keeps on Track Without GPS," *New Atlas*, June 14, 2017, https://newatlas.com/nvidia-camera-based-learning-navigation/50036/.
[26] Locata, "About Us," 2019, http://www.locata.com/about/.
[27] BAE Systems, "Navigation via Signals of Opportunity (NAVSOP)," 2019, https://www.baesystems.com/en/product/navigation-via-signals-of-opportunity-navsop.
[28] Marks, P., "Quantum Positioning System Steps in When GPS Fails," *Technology Daily Newsletter, New Scientists*, May 14, 2014.
[29] Barnard, J., *Small UAV Command, Control and Communication Issues*, Barnard Microsystems Ltd., 2007.
[30] Kakar, J. A., *UAV Communications: Spectral Requirements, MAV and SUAV Channel Modeling, OFDM Waveform Parameters, Performance and Spectrum Management*, Virginia Polytechnic Institute and State University, Blacksburg, VA, 2015.
[31] Rinicom, "PodNode-I," 2019, https://rinicom.com/communications/podnodes/podnode-i/.
[32] Rinicom, "R1000," 2019, https://rinicom.com/communications/r1000-cofdm-video-links/r1000/.
[33] Rinicom, "R1000HD," 2019, https://rinicom.com/communications/r1000-cofdm-video-links/r1000hd/.
[34] Rinicom, 2019, https://www.rinicom.com.
[35] Rinicom, "Rinicom Ltd and FOLIUM Science Wins Innovate UK Award to Develop New Technology to Treat Blights in World Crops," January 7, 2019, https://rinicom.com/rinicom-ltd-and-folium-science-wins-innovate-uk-award-to-develop-new-technology-to-treat-blights-in-world-crops/.
[36] Drury, G. M., G. Markarian, and K. Pickavance, *Coding and Modulation for Digital Television*, Boston, MA: Kluwer Academic Publishers, 2000.
[37] Peled, A., and A. Ruiz, "Frequency Domain Data Transmission Using Reduced Computational Complexity Algorithm," *IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, Denver, CO, April 9–11, 1980, pp. 964–967.
[38] Çuhadar, I., and M. Dursun, "Unmanned Air Vehicle System's Data Links," *Journal of Automation and Control Engineering*, Vol. 4, No. 3, 2016, pp. 189–193.
[39] Lockheed Martin, "STANAG-4586," 2019, https://www.lockheedmartin.com/en-us/products/cdl-systems/stanag-4586.html.
[40] Campion, M., P. Ranganathan, and S. Faruque, "UAV Swarm Communication and Control Architectures: A Review," *Journal of Unmanned Vehicle Systems*, Vol. 7, No. 2, June 2019.
[41] Bekmezci, I., O. Z. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A Survey," *Ad Hoc Networks*, Vol. 11, No. 3, 2013, pp. 1254–1270.
[42] Sahingoz, O. K., "Networking Models in Flying Ad-Hoc Networks (FANETs): Concepts and Challenges," *Journal of Intelligent Robotic Systems*, Vol. 74, No. 1-2, 2014, pp. 513–527.
[43] EUROCAE, "Working Groups," 2020, https://eurocae.net/about-us/working-groups/.

[44] Hayley, "Understanding Drone Payloads," Coptrz, June 7, 2016, https://www.coptrz.com/understanding-drone-payloads/.
[45] Fahlstrom, P. G., and T. J. Gleason, *Introduction to UAV Systems,* 4th ed., New York: John Wiley & Sons, 2012.
[46] Sharma, P., *Global Stratospheric UAV Payloads Technology Market: Analysis and Opportunity Assessment 2019-2025*, 2019.

CHAPTER

4

Contents

The C-UAV Problem

4.1 Introduction

It is like the story of the computer. At first, you needed a whole room to house a computer. Now everyone has one in their pocket.

—Andreas Rastopoulos, founder of the *Matternet* start-up in Silicon Valley

Security threats from the UAVs have existed for a long time and the use of drones by terrorists has reported since the early 1990s. Table 4.1 summarizes some of the earlier terrorist attacks in which perpetrators employed different types of UAVs with various degrees of sophistication [1].

These were very dangerous but isolated cases with effects restricted by limitations of technologies available to terrorists. However, the number of UAVs that are owned by the general public, businesses, and government agencies is growing at astonishing rate and the use of these UAVs is varying from recreational activities to agriculture, postal delivery, search and rescue, defense, and security, to name just a few. These UAVs range from large MALE and HALE systems to tactical drones, mini-UAVs, and micro-UAVs, as described previously. Accordingly, all

Table 4.1
Early Terrorist Attacks Utilizing UAVs

Date	Name of Organization/ Individual	Nature of Threat	Preparation Level	Support Base	Source of Information
1995	Aum Shinrikyo, the Japanese terrorist group	Attacked the Tokyo subway	Planned to use remote-control helicopters to spray Sarin gas (dangerous chemicals from the air)	Japanese terrorist group	Literature available on this subject [2]
2001	Osama bin Laden	Planned to kill George W. Bush and other heads of state at the G-8 Summit in Genoa, Italy	Considered using remote-control airplanes packed with explosives	Al-Qaeda	Intelligence inputs [3]
June 2002	Al-Qaeda	Planned to attack passenger aircraft	Considered using model airplanes	Al-Qaeda	Reuters News Agency [4]
August 2002	Revolutionary Armed Forces of Colombia or FARC	Exact target not known	Possession of nine remote-controlled unmanned aircraft	FARC	Colombian Army Unit [5]
December 2002	Palestinian terrorist group	Attacked built-up Israeli area	Model planes for conversion into miniature air bombers with explosive payloads	—	Counter terror Report [5]
November 2003	A British National held at Camp Delta, Guantanamo Bay, Cuba	Attack the British House of Commons	Acquire a drone to attack with anthrax	Al-Qaeda	London *Independent* newspaper [7]
March 2004	A Palestinian extremist group	Attack a Jewish settlement in the Gaza sector	Use of a UAV loaded with explosives	Palestinian extremist group	Israeli intelligence [8]

the latest technologies incorporated in these UAVs are readily available to players who are prepared to use them unlawfully.

The most common consumer and commercial drones typically weigh under 10 kg and the majority weighs less than 2 kg. Quadcopters with four horizontal rotor blades are the most commonly used, but small, fixed-wing drones are gaining more popularity. These consumer drones can stay in the air for up to 30 minutes at a time, with quick battery changes, and can

lift small payloads of 500g, while commercial drones can carry payloads in excess of 6 kg. As an illustration, Table 4.2 shows the key parameters of the various drones manufactured by the market leader, DJI [9].

It is apparent that even these commercially available UAVs could be flown into a restricted area or civilian and/or military airspace and result in accidental or deliberate damage [10][1].

Even though governments are introducing restrictions on the use of these UAVs and vendors build in special countermeasures to eliminate the flights in the restricted areas (like geofencing in all latest DJI drones), new models with enhanced performance and reduced cost are introduced on a regular basis and, in the hands of terrorists, could create a serious distraction and both political and commercial damage.

Cases in which commercially available UAVs have been flown inside the security perimeters of critical infrastructure such as airports, prisons, the White House, government embassies, nuclear power plants, and oil refineries are reported on a regular basis. With ever-improved flight characteristics of the UAVs, they now easily could be flying in the same airspace as passenger aircraft preparing for landing or take-off. Numerous studies in the United Kingdom and the United States [11] have shown that a drone collision with an aircraft is more damaging than an equivalent-energy bird strike and that drones colliding with aircraft can damage the structure to cause a crash.

Table 4.2
Technical Characteristics of DJI UAVs

	Spark	**Mavic**	**Phantom**	**Inspire**	**Matrice 600**
					
Dimensions	14x14x6 cm	31x24x9 cm	29x29x20 cm	48x47x32 cm	167x152x73 cm
Weight	300g	700g	1.4kg	3.4kg	10kg
Maximum Flight Time	16 mins	31 mins	30 mins	27 mins	18 mins
Maximum Speed	50 km/h	72 km/h	72 km/h	94 km/h	65 km/h
Maximum Altitude	4 km	6 km	6 km	—	5 km
Maximum Transmission Distance	2 km	8 km	7 km	7 km	5 km
Maximum Recommended Payload	N/A	N/A	N/A	810 g	6 kg
Autonomous Flight Capable?	Yes	Yes	Yes	Yes	Yes

1. We would like to express our gratitude to Bill Haraka of ROBIN Radar (www.robinradar.com) for kindly sharing this white paper.

A nightmare scenario for all airport security managers is drone attack on one of the airplanes during the refueling at a terminal with numerous aircraft in the short proximity, potentially creating a domino effect. The scope of security threats is growing exponentially as new drones could fly longer and faster with larger payloads.

Government agencies, armed forces, and the leading industries around the world are looking for ways to counter the threat from unlawfully flying UAVs. Every stakeholder in this challenge acknowledges that this is a complex problem that cannot be resolved by one solution suitable for all possible security threats. Furthermore, there is a common understanding that only a comprehensive solution scalable for various scenarios could produce the required level of counter-UAV protection. Although there are a wide variety of views on the details of this comprehensive solution and how this problem should be addressed and solved, there is a generic agreement that the solution should be a combination of two approaches:

- *Regulatory:* These are addressed in earlier sections.
- *Technological:* These will be addressed in this part of the book.

In order not to be lost in the minor details in variations of the different C-UAV systems, we start with the classification of these systems. The generic classification of the C-UAV systems was introduced in [12] and is presented in Table 4.3.

There are different technologies available for both monitoring (i.e., detection, tracking, and classification) and neutralization of drones. Detection, tracking, and classification are allowed and are recommended as the key step in the countering UAV process; for more details, please refer to Section 6.9, as there exist some restrictions even for detection systems. The neutralization of drones is still (in most countries) not legally permitted and cur-

Table 4.3
Generic Classification of C-UAV Systems

Type of C-UAV System	Description
Ground-based: fixed	Systems developed for installations in fixed or nomadic applications
Ground-based: mobile	Systems developed for installations on vehicles and to be operated on the move
Hand-held	Systems developed to be operated by a single individual by hand; most of these systems look like rifles or small arms
UAV-based	Systems developed to be installed on UAVs

rently is the subject of numerous regulatory and legal discussions. Typical monitoring technologies are summarized in Table 4.4 [12].

Each of these technologies has its individual advantages and limitations and it is a common agreement of all stakeholders that a C-UAV system should incorporate an integration of various sensors to compensate the shortcomings of induvial sensors. The advantages and limitations of various sensors are summarized in Table 4.5 [13].

Most UAV neutralization techniques have emerged from other military applications. Therefore, it is not surprising that number of possible neutralization techniques is even larger than the number of detection techniques. Not all these techniques are legal and/or affordable for nonmilitary applications, but we thought it would still be beneficial to mention these techniques. The typical neutralization techniques are summarized in Table 4.6 [12].

However, as pointed out in [14], destroying the drone does not mean that the problem is solved. Even if a drone is neutralized by one of the above-mentioned means, this is only half of a solution. To solve the problem comprehensively, it is essential that the operator of the illegally flying

Table 4.4
Types of Sensors Used in C-UAV Systems

Type of Sensor	Description
Radar	Detects and tracks UAVs by their radar signature
Radio frequency (RF)	Detects, tracks, and identifies both the UAV and the pilot by monitoring radio frequencies used by UAVs
Electro-optical (EO)	Detects, tracks, and classifies UAVs utilizing EO cameras
Infrared (IR)	Detects, tracks, and classifies UAVs utilizing IR cameras
Acoustic	Detect UAVs with the array of acoustic microphones
Visual monitoring by humans	Relies on security personnel visually monitoring skies with binoculars
Combined sensors	Multiple sensors fused together to provide more reliable detection, tracking, and classification of UAVs

Table 4.5
Comparison Table for Various Detection Sensors

Type of Sensor	Detection Range	Position Accuracy	Identification and Classification	Auto Mode	Detection of Pilot	Multiple Targets	Low Visibility/ Night	Passive System	Price
Radar	++++	++++	+	–	–	++++	++++	–	–
RF	++++	++++	++	–	+++	++++	++++	++++	+
EO/IR	++	++++	++++	++++	–	++++	++	++++	++++
Acoustic	–	–	+	–	–	+	++++	++++	++++
Human	–	–	+++	–	–	–	–	++++	+
Thermal imaging	–	+	++	++	–	+++	++++	++++	–

Table 4.6
Countermeasures Used in C-UAV Systems

Countermeasure	Description
RF jamming	
GNSS jamming	Disrupts UAV's GNSS link, GPS, or GLONASS; without synchronization with GNSS system, a UAV will hover, land, or return to home
Spoofing	Allows the C-UAV system operator to take control of or misdirect the targeted UAV by creating a virtual GNSS channel with wrong navigation information
Hacking	Interception of UAVs navigation system and reading its flight plan and flight data
Dazzling	Implementation of high-power laser beam(s) to blind the camera(s) on the UAV
Laser	Burns a critical part of the UAV's frame and components (see Chapter 3) using direct energy, causing a crash of the UAV
High-power microwave	Send pulses of high-power microwave signals, destroying the UAV's electronics components
Shooting nets	Entangles drones and/or its propellers
Projectiles	Employs regular or custom-designed ammunition to destroy the incoming UAV
Water cannons	Directs high-pressure water towards incoming UAV, causing crash
Interceptor drone	A drone designed to intercept the target drone and bring it back to base
Collision drone	A drone designed to collide with the target UAVs
Falcon	A specially trained falcon bird that catches UAVs as prey
Missiles	Conventional missiles used for destroying large UAVs
Guns	Conventional rifles used by snipers to shoot down the UAV
Combined effectors	A number of different and complementary neutralization techniques used in the same C-UAV system for increased reliability of neutralization

UAV is located and detained. Without this, it is very likely that a determined operator will return with a newer and better UAV capable of causing more distraction and damage. Therefore, when developing a C-UAV system, a comprehensive set of procedures and requirements needs to be defined, covering the whole process from detection to classification to neutralization and prosecution.

In the rest of this chapter and in the following chapter we will discuss in greater detail advantages and shortcoming of various sensors.

4.2 Comprehensive Approach to C-UAV and C2 Platforms

As the demand to mitigate threats caused by UAVs grows, industry players from around the world are developing solutions to detect and neutralize

hostile and unlawfully flying UAVs. A quick search of the internet identifies over 200 companies worldwide,[2] claiming to have products and solutions for addressing the problem; these solutions range from acoustic noise signature detection to RF detectors, radars, EO/IR cameras, lasers, and jammers and even include eagles and UAVs equipped with nets that fly around the perimeter trying to catch other UAVs. However, as emphasized earlier, there is no single-bullet solution that we will work efficiently and economically in all possible threat scenarios. For example, a C-UAV system for protecting the privacy of celebrities on a yacht will be different from a C-UAV system intended to minimize the delivery of contraband to prison or across the state borders and from a C-UAV system installed at a large airport or oil refinery. Therefore, it is important to clearly define the advantages and drawbacks of each of the sensor and develop the most efficient way for the integration of the sensors ensuring the improved performance of the overall system. Hence, developing a generic C-UAV system architecture that could be adopted for various applications addressing different security threats is the first task for every C-UAV system vendor.

Before we analyze how this challenge could be solved in the most efficient way, we need to explain a few definitions currently being used by the C-UAV system developers and users:

- *Detection:* This means that the C-UAV system is able to detect drones reliably. However, single detection sensors usually are not sufficient, as no sensor can provide 100% detection accuracy. For example, a radar that detects drones may also detect birds or reflections from surrounding infrastructure, leading to a high probability of false alarms while the RF detection sensor will be less efficient in an urban environment or when detecting drones flying in auto mode.
- *Classification:* This means the ability to distinguish drones from other types of objects, such as birds, planes, and all other moving objects (trains, automobiles, humans, clouds).
- *Identification:* This means the ability to identify a particular model of the UAV, including the type of payload, and to identify the drone or controller's digital fingerprint, such as a media access control (MAC) address and pilot's location. This level of identification is essential for forensic and prosecution purposes.
- *Tracking:* This means that once a UAV is detected, classified, and identified, its behavior is continuously monitored. This is particularly impor-

2. The exact number is 277 companies in 38 countries offering 537 products, as shown in [12].

tant for real-time situation awareness and the ability to deploy appropriate countermeasures at the most appropriate time. This information is always recorded for future forensic and training purposes.

- *Neutralization:* This means that, according to the situation awareness scenario, the most suitable countermeasure (jamming, kinetic, sniper, interceptor UAV, drone catcher eagle) should be deployed. In some cases, taking no active countermeasures but governing forensic data could be the most appropriate countermeasure (for example, neutralizing advertising or TV drones during mass public events).

Ideally, civil, security, and military authorities will need a C-UAV system to detect, identify, classify, track, and neutralize any type of hostile UAV in any setting. Differences between civilian and military C-UAV solutions are mainly in the detection ranges and the implementation of the command control (C2) and neutralization tools. In most civilian applications, there are no neutralization measures, and these systems act primarily as an alerting system when a UAV is detected (this is due to complex regulatory situation and for minimization of collateral damages).

In [15], a comprehensive analytical approach to the C-UAV operations was proposed. More specifically, the authors introduced the SWOT (Strengths-Weaknesses-Opportunities-Threats) analysis enhanced with the Tree analysis (SWOT+Tree) to provide a broader look for investigating the factors related to C-UAV operations and analysis.

A similar concept of comprehensive approach was adapted by THALES in support of their efforts to develop a C-UAV system [16]. The company's sophisticated knowledge of UAVs and their mission systems was utilized to develop effective countermeasures against these same systems [16]. The system provides the complete solution from detection to neutralization and includes state-of-the-art technologies for the purpose of C-UAV: a broad range of detection sensors (both active and passive), the C2 platform, and effectors (both soft-kill and hard-kill systems such as laser, jammers, and other weapon systems). Acknowledging different requirements for security and military applications, THALES differentiated system architecture based on use cases. For security and civilian applications dealing with the protection of critical infrastructure and/or major events from low-flying, small UAVs, THALES's system integrate seamlessly with the existing SCADA (Supervisory Control And Data Acquisition) systems and has benefits of providing additional operational capabilities against these security threats. This version of the C-UAV system incorporates a variety of sensors, nonlethal neutralization, and a central C2 software suite for data correlation and recording. Technology solutions are complemented with a value analysis to ensure that the proposed solutions meet cost constraints, are not

unnecessarily complicated to install, and are economical to operate. Depending on the identified security threat, concepts of operations (CONOPS) analysis is applied to select the most appropriate suite of sensors tailored to the particular threat scenarios, legal contexts, and regulations on radiating sensors and effectors.

An example of such a tailored application is the HOLOGARDE solution, which THALES developed in cooperation with DSNA and Group ADP and is installed at the Paris-Charles de Gaulle Airport. According to claims in the open literature [18], the system is capable of detecting drones at a distance of 5 km (3.1 miles), although the size of drones and conditions are not clarified.

In general, HOLOGARDE offers two solutions:

- *HOLOGARDE:* Complete drone system detection and neutralization response as an option;
- *HOLOGUIDE:* Collaborative drone management solution that manages flight plans and authorizations.

HOLOGARDE C-UAV offers three additional models, named A, B, and C [19].

- *Model A:* This is a nomadic version, designed for event protection, which can be rapidly installed on a desired site. It is a comprehensive UAV detection system that could include C2 software, radar, RF detection, and EO/IR sensors. Model A also offers an option for integration of the Unmanned Aircraft System Traffic Management (UTM) data.
- *Model B:* This is developed for the protection of major critical infrastructure sites and requires comprehensive development (including networking and construction of towers) prior to installation. It is a comprehensive C-UAV detection system that includes the C2 HOLOGARDE platform, radars, RF sensors, EO/IR sensors, and the neutralization system. Model B provides interfaces for integration with the UTM systems. The complexity of Model B is illustrated in Figure 4.1 [20].
- *Model C:* This is a situation awareness solution primarily designed for large airport installations to provide appropriate to the detected UAV threat, which is also complementary to the HOLOGARDE models A and B. On receiving a drone detection alarm from HOLOGARDE C2, Model C will generate new flight plans for all collaborative UAVs and establish administrative authorizations for neutralization of the detected UAVs.

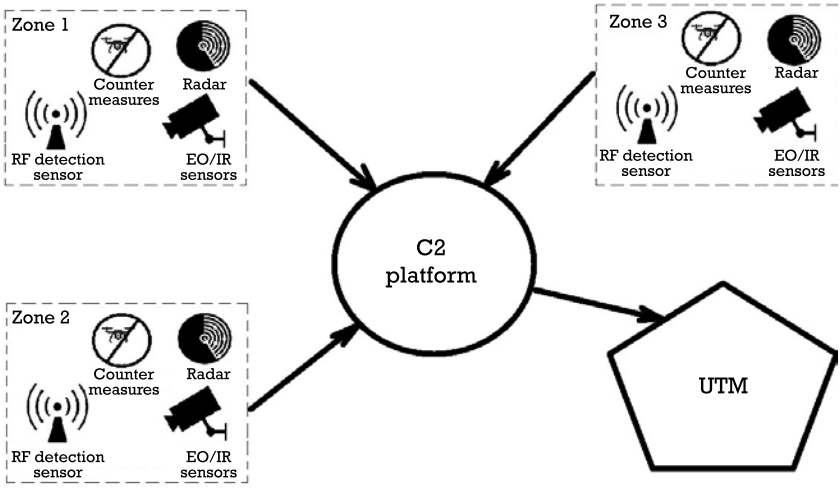

Figure 4.1 Block diagram of HOLOGARDE Model B.

- *Model D:* This is an integral part of the UTM system and is designed to manage flight plans and authorizations for collaborative UAVs.

The described comprehensive approach is now a de facto standard in the industry and almost all system integrators from around the world have adopted it. For example, ST Engineering (Singapore) was among the pioneers that developed and deployed one of the first commercial C-UAV systems for nonmilitary applications. The system, called SkyArcher [21], is a synergistic solution that detects and disrupts emerging threats posed by commercial drones.

The system uses the "3Ds" approach (detect, decide, and disrupt) to counter intruding drones in urban and RF-dense environments. The principle of the SkyArcher modus operandi is explained in Figure 4.2.

The SkyArcher detection sensors constitute a multisensor integrated system that uses RF signal detection, direction finding, and optical detection with visual analytics to automatically detect, classify, and track commercial drones. The RF signal detection provides an indication of the direction of drone pilot and target drones, coupled with visual analytics for identification, classification, and tracking of the target drones.

The SkyArcher Control and Synchronization Module (CSM) allows for the seamless operation and fusion of sensors to optimally detect drone targets on a timely basis. Through this capability, data from the detection sensors can be intelligently collated and used to classify, identify, and track the target drones. It also identifies the drone model based on the Drone Remote Control Libraries.

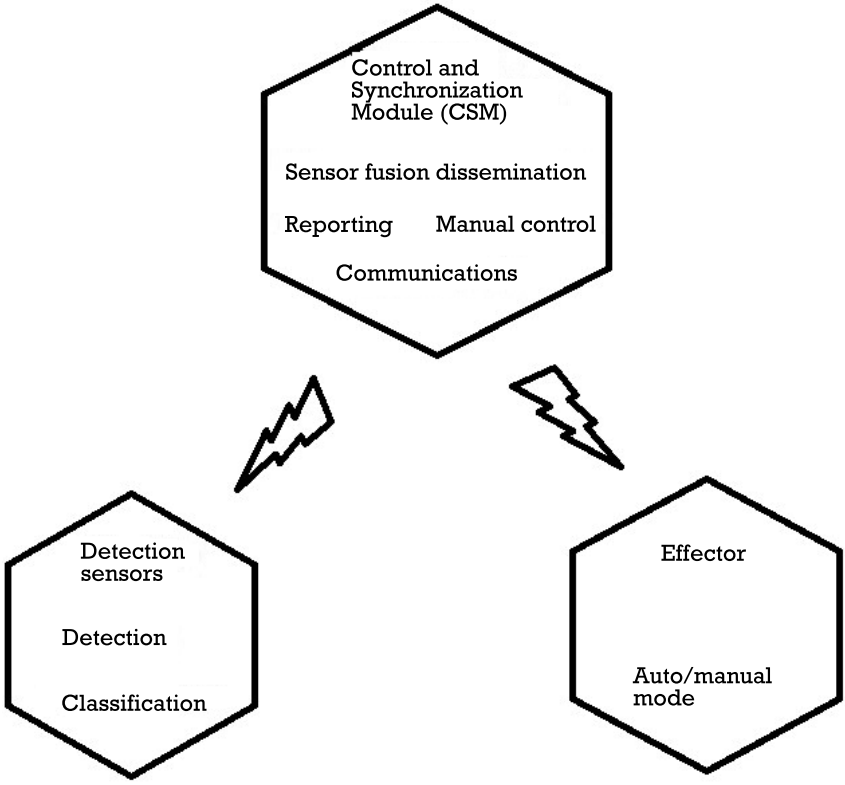

Figure 4.2 The SkyArcher modus operandi. (We would like to express our gratitude to ST Engineering, Singapore, for sharing information about SkyArcher, including this diagram.)

SkyArcher Effector offers a variety of effector options to meet different requirements for any environment. It is suitable for deployment by a single effector or a combination of effectors to effectively disrupt target drones.

The key features of SkyArcher are:

- Open architecture that allows sensor fusion and integration that enables the optimal detection and disruption of drone targets on a timely basis;
- Real-time tracking of unauthorized drone intrusions to automatically disrupt target drone or trigger remote alerts and notification to security personnel through their mobile devices;
- Correlate and display results of RF, direction finding, and visual sensors for easy target visualization;

- 360° panoramic view and target visualization in real time to enhance decision-making and incident management;
- Easy integration with other autonomous systems and robotics, including both friendly and interceptor drones.

Another C-UAV system that utilizes the comprehensive approach is the DroneGuardian C-UAV system developed by L3/HARRIS Inc., in the United Kingdom [21]. The system is based on L3/HARRIS's extensive experience in the delivery of solutions to detect and defeat airborne threat and utilizes Target Oriented Tracking System (TOTS) software, which requires taking raw collected data and compiling it into a real-time picture that can be disseminated using mapping and visualization, data, and analytics and creates effective workflow management. Drone Guardian, like TOTS, is built on an open architecture that can incorporate information from multiple integrated components and external sources, as shown in Figure 4.3.

Drone Guardian allows multiple target detection, identification, and tracking to mitigate the threat of the UAVs, and, unlike the SkyArcher C-UAV system from ST Engineering, it is applicable within both the commercial and military environments. Drone Guardian can be distributed to both fixed and deployable installations with an integrated security workflow enabling rapid security response times. Drone Guardian is hardware-agnostic and scalable and the base system sensors can be altered to more appropriate alternatives that can be readily integrated to utilize the best-of-breed components and to suit various operational scenarios. The suite of sensor subsystems incorporated in Drone Guardian includes radars, RF detection, optical, and acoustic and the integration of these subsystems into a layered C2 platform provides many benefits. As shown in Figure 4.3, the system operates in the continuous cycle of observe-orientate-decide-act and provides

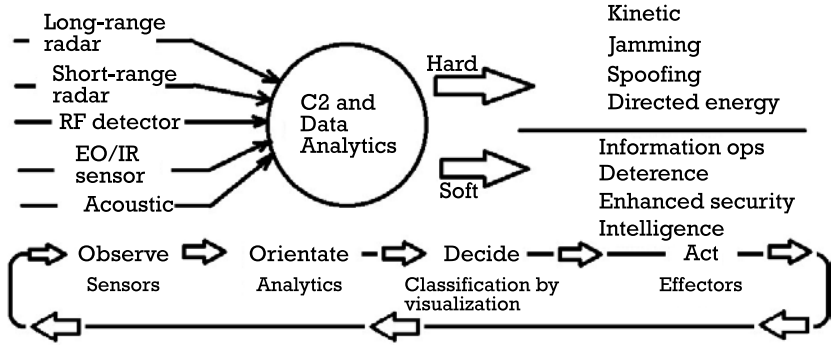

Figure 4.3 Effect-based DroneGuradian comprehensive C-UAV approach. (We would like to express our gratitude to L3-ASA Ltd. for sharing this diagram.)

uninterrupted early detection of multiple drones with reduced false alarms, mitigating security risks at a quicker response rate and reducing manpower required to operate the system. As proven in multiple installations, Drone Guardian operates alongside "friendly" drones and allows the early detection of foe drones providing additional valuable time to decide the appropriate course of action to defeat or minimize the threat.

The above-mentioned C-UAV systems share the same advantages of multisensor integration approach and the same drawback of the need for the continuous 24/7 presence of dedicated human operators to mitigate false alarms and ensure the man-in-the-middle concept when making a critical decision, including ways of neutralization. This leads to a very serious drawback that becomes apparent mainly after a C-UAV system is installed and becomes operational: a high operational cost.

An innovative approach to integrated intelligent C-UAV system is developed and implemented by Operational Solutions Ltd. in the United Kingdom. The system, called FACE [22], is an industry-leading business intelligence system, giving users the confidence that if drone misuse strikes, they are fully protected. FACE allows the operator to clearly identify drones and, where applicable, control commands to the drone effector, such as jammers and physical interception systems. The system consists of:

- An engine to consume incoming data and ensure that it is correct and consistent;
- A database to handle analysis;
- A user interface that can be accessed from any user-friendly device.

FACE is successfully installed in several large critical infrastructure sites in the United Kingdom and abroad, but importantly, FACE is a continuously developing concept and the latest generation of FACE combines the multisensor integrated approach in conjunction with artificial intelligence (AI) and machine learning (ML) algorithms embedded within the sensor agnostic C2 platform. A schematic diagram of this system is shown in Figure 4.4.

This solution eliminates the need for continuous 24/7 human monitoring by engaging human operators only when the AI/ML module classifies detected objects as UAVs. Operationally, this allows the integration of C-UAV monitoring into the existing surveillance monitoring process without additional operational expenditure. The solution already is accepted for installation on numerous high-profile critical infrastructure sites in the United Kingdom and abroad and is becoming a de facto standard for future C-UAV systems.

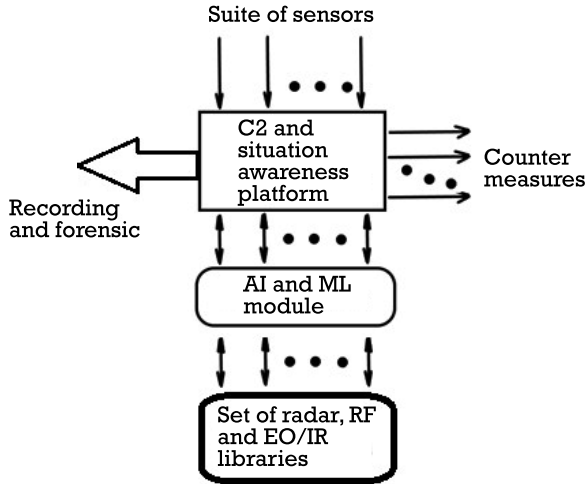

Figure 4.4 A Schematic diagram of comprehensive C-UAV system with AI and ML.

References

[1] Lele, A., and A. Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles," *Journal of Defence Studies*, Vol. 3, No. 3, July 2009, pp. 54–65.

[2] Mahan, S., and P. G. Griset, *Terrorism in Perspective*, 2nd ed., Los Angeles, CA: Sage Publications, 2008.

[3] Gips, M., "A Remote Threat," *Security Management Online*, October 2002.

[4] Mason, J., Reuters, "Obama Says U.S. Will Pursue Plane Attackers," *World News*, December 29, 2009, https://uk.reuters.com/article/uk-security-airline/u-s-boosts-airline-precautions-amid-recriminations-idUKTRE5BQ0ZR20091228.

[5] EFE, "Colombia - FARC Drones Discovered," *EFE News Service*, August 28, 2002.

[6] DEBKA, *Arafat's New Terror Weapon: Exploding Toy Planes*, DEBKA File Special Counter-Terror Report, January 14, 2003, https://www.debka.com/arafats-new-terror-weapon-exploding-toy-planes/.

[7] Gormley, "Testimony," *Independent*, 2004, https://www.theguardian.com/uk/2003/aug/01/politics.alqaida.

[8] Polit, B., "Terrorist Act with UAV Employment Has Been Prevented in Israel," *Polit. Ru*, March 10, 2004.

[9] DJI, https://www.dji.com.

[10] "White Paper on Countering Drones," ROBIN Radar Systems, 2018.

[11] CBS News, "FAA Research Finds Drone Collisions More Damaging Than Bird Strikes to Airplanes," November 29, 2017, https://www.cbsnews.com/news/faa-research-finds-drones-more-damaging-than-birds/.

[12] Michel, A. H., *Counter-Drones Systems,* 2nd ed., Report from the Center of the Study of the Drone at Bard College, December 2019.
[13] Wellig, P., et al., "Radar Systems and Challenges for C-UAV," *19th International Radar Symposium IRS 2018*, Bonn, Germany, June 20–22, 2018.
[14] CRFS, "Drone Detection: Myths and Reality," 2018, https://www.crfs.com/blog/drone-detection-myths-and-reality/.
[15] Turan, M., et al., "An Analytical Approach to the Concept of Counter-UA Operations (CUAOPS)," *Journal of Intelligent and Robotic Systems*, January 2011, pp. 1–4.
[16] Stevenson, B., "Thales Developing Counter-UAV Technology," *Flight Global*, June 8, 2015, https://www.flightglobal.com.
[17] Bastiaans, P., "Paris Air Show 2015: Thales C-UAV Solutions," *Military Technology*, June 16, 2015, http://www.miltechmag.com/2015/06/paris-air-show-2015-thales-c-uav.html.
[18] Forecast International, "Thales, DSNA, Groupe ADP Unveil the Hologarde C-UAV Airport Protection System," March 7, 2018, http://www.defense-aerospace.com/articles-view/release/3/191372/hologarde-counter_uav-airport-protection-system-unveiled.html.
[19] Hologarde, 2018, https://hologarde.com/solutions/#models.
[20] SkyArcher, "SkyArcher – Counter Drone System," ST Engineering, Singapore, 2014.
[21] L3 Harris, "Drone Guardian," 2019, https://www.l3-droneguardian.com.
[22] FACE, "Introducing FACE," 2018, https://osldronedetect.co.uk/osl-face.

CHAPTER

5

Contents

C-UAV Sensors and Situation Awareness

5.1 Situation Awareness[1]

If all we did was switch on radars, take the raw data and present it to air traffic controllers, there would be chaos. It is only when you can correlate that with the identity of those flights and their expected flight plans that you can see the outliers and those who are where they should not be."

—Andy Sage,
representative of U.K. NATS [1]

This transition from chaos to order becomes even more important in a world where traffic density increases, and unmanned air traffic emerges. The amount of information that requires presenting is too much for air traffic controllers to digest in a safe manner. A new challenge arises in ordering the chaos in a world where drones, benign or malicious, enter civilian or military air space.

As unmanned air traffic evolves, technologies and regulations will emerge that enable

1. We would like to express our gratitude to 42 Solutions B.V. (Netherlands) for providing material and sharing the supporting illustrations.

and mandate the drones to identify themselves. However, even if all commercially available drones will be enabled with this feature, the operators of C-UAV systems need to be prepared to deal with the fact that drones might not present themselves as required by law or regulation (for example, it took us less than 20 minutes to use a well-known search engine and find on the internet introductions on how to modify a UAV and disable geofencing restrictions).

As described earlier, a wide range of sensors to detect illegally flying drones is available for integration into a C2 platform to provide integrated solution and fuse sensor data into one concise picture. However, no C-UAV system is 100% perfect and a certain degree of false-positives or, maybe worse, false-negative detections should be incorporated into a response action plan. Unlike most of the critical infrastructure sites where the response is focused primarily on the neutralization of a UAV and capture of the pilot, the response action plan in airports must include an additional dimension of coordination with air traffic management (ATM) and ensuring safe diversion of aircraft from potential collision with a UAV.

Even when presented with a single source of data from C2 platform, the ATM operators may find some information difficult to digest or assess. The information will have to be presented in a comprehensive and user-friendly way to help them to make the right decision when changing flight plans to aircraft. The most efficient way to achieve this is by adding situation awareness to C2 platforms. A typical example of such a situation awareness platform is the Merlin IUTM system developed by 42 Solutions B.V. [2]. As shown in Figure 5.1, when integrated with a C-UAV platform, the system displays a map interface, and, depending on the suite of used sensors, it may show:

- Drone location, speed, and heading;
- Drone identity;
- Drone pilot location;
- Team member location.

The map can be a satellite image or a variety of geographical maps.

The Merlin IUTM system is designed to interconnect with a wide variety of sources:

- *Aircraft traffic management (ATM):* Track data will supply the real-time location of aircraft in the vicinity.

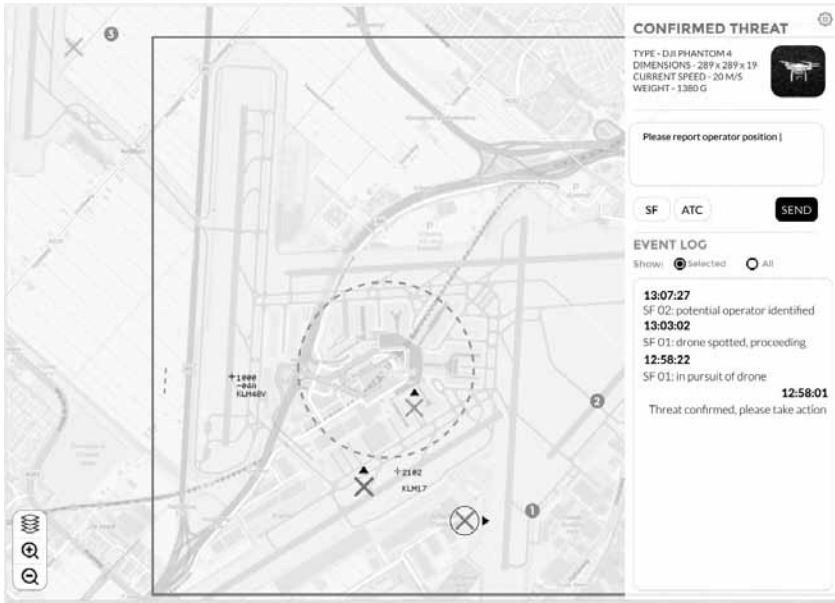

Figure 5.1 Screenshot of the Merlin IUTM platform.

- *Unmanned aircraft system traffic management (UTM):* Authorization from these systems will mark drones as safe for specific areas, although the drones will still be seen as a threat when they conflict with approaching traffic.
- *Other traffic reports/information systems:* These include the Automatic Dependent Surveillance – Broadcast (ADS-B) (aircraft) or other vehicle information.
- *Local data:* Information about sensitive areas, such as critical infrastructures or high security zones, that can be configured in the C2 system.

Combining all the available information, the system performs a threat assessment on each reported drone. As shown in Figure 5.2, the assessment is done using several algorithms to determine whether the drone poses a threat to specific areas or other traffic.

The threat assessment will trigger the C-UAV operator to inspect the situation and, if prudent, start a mitigation process in cooperation with the ATM or, alternatively, the mitigation process is started automatically, depending on the security choices made by the user. The automatic mitigation process will be faster, but with a higher risk of false-positives. If the drone

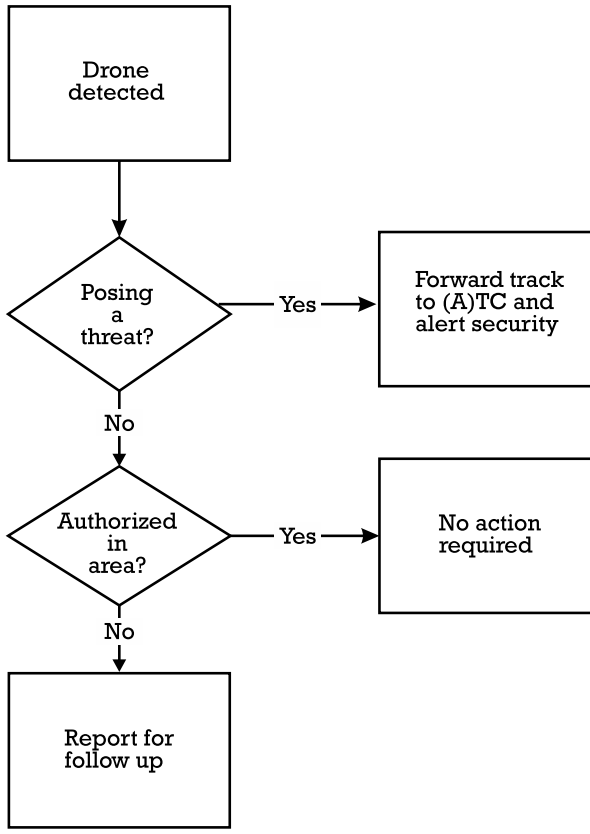

Figure 5.2 Flowchart of the Merlin UITM.

poses no threat, but is still in violation of the regulations, the information is recorded for follow-up actions and forensic investigation.

The mitigation process will involve multiple parties. Stakeholders in a drone incident are law enforcement, the airport, and air traffic control. However, it may be that other responders come into play as the event unfolds (e.g., military police or airport security may have to respond in order to find and apprehend the drone pilot).

Therefore, the Merlin IUTM system provides a common operational picture to offer shared situational awareness among all players. This minimizes the risk of misinterpretation of communication.

The mitigation process will start by sending the threat information to the stakeholders. This is done in such a way that the information facilitates the normal processes of the stakeholder as much as possible.

The information send to an ATC system will use their own message formats, sending a track clearly marked as a threat. On the basis of this information, the air traffic controller will be able to judge the necessary reaction to this threat and to follow the threat in real time. Security forces will need more information to enable them to neutralize the threat. They will receive the information on a specialized smartphone app that will give them the drone location and details and the location of their team members. The app also gives them the means to exchange (shortcode) messages.

As *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* illustrates [3], communication is key, but the timeliness, the temporal aspect of information, is an essential component of communication [4]. This is why the Merlin IUTM system provides incident reporting and messaging facilitating the team members and the C2 operator to create a response team in an agile fashion. It gives them the possibility to monitor progress and report on their findings, supporting a collaborative way to decide on their actions. The system also gives them the means to declare the incident mitigated.

5.2 Radars as C-UAV Sensors

5.2.1 Introduction to Radars and Radar Systems

RADAR stands for Radio Detection And Ranging and it is an active RF system that allows the detection of various objects, providing measurements of their range, velocity, and size. The concept of radar was originally discovered in the 1880s by H. Hertz, who experimentally proved detection capabilities of electromagnetic waves in the 455-MHz frequency band [5]. In 1904, a patent for a Telemobiloscope was granted to German engineer Christian Hülsmeyer [6]. However, it was only in 1930s, with World War II looming ahead, when almost all countries started active investigations in this field. In September 1938, the first British radar system, called the Chain Home, started its 24/7 operation along the east coast of the United Kingdom, providing early detection of German air attacks. The inventor of the Chain Home, Sir Robert Watson-Watt, had to resolve a common engineering dilemma: to develop an optimum system later or to deliver a suboptimum solution quicker. Eventually, he settled on a suboptimum system operating in the 30-MHz frequency band, which worked and, at that historical moment, was better than the ideal solution which was delivered a couple of years later.

A radar system consists of a transmitter producing electromagnetic waves at a certain frequency band, a corresponding pair of transmitting and receiving antennae (often integrated in a single antenna system), and

a receiver and processor to estimate the various properties of the object(s). The choice of the operating frequency band is dictated by applications and operating requirements and strongly influences the performance of the radar.

The basic principle of radar did not change dramatically since its discovery more than 100 years ago: transmitted radio waves reflect off the object and return to the receiver with a delay and distortion, containing information about the object's location, size, and speed. However, huge progress was made in this area, and various radar systems are currently in operation serving different purposes.

The radars are classified by applications and technology. Table 5.1 lists just a few types of radars used in different applications that are potentially suitable for implementation in C-UAV systems.

Radar also are classified according to the configuration of the transmitter(s), the receivers(s), the antenna, frequency band, wavelength, and scan protocols, just to name a few. A detailed description of these radars is outside the scope of this book, and the interested reader is advised to read literature specifically dedicated to radars. In this chapter, we will provide a brief overview of the above-mentioned types of radars, which should help us to identify the best candidates for the C-UAV applications.

Table 5.1
Types of Radars

Types of Radar	Application
Air defense radar	Determines the target location and guides the weapon to destroy the target.
Airborne radar	Used for aircraft navigation and guides aircraft in all weather conditions
Air-traffic radar	Determines the location of the landing aircraft and helps an aircraft to land in poor weather and visibility conditions
Bird radar	Detects birds in and around airports
Collision radar	Helps to prevent collisions between vehicles and aircraft
Docking radar	Guides vehicles to correct docking positions (for example, satellites on Earth orbit or automatic vacuum cleaner)
Ground radar	Used for creating ground maps from the satellite of arcraft
Ground-penetration radar	Used for detecting objects hidden below the Earth's surface
Marine radar	Determines the location of the ship and shore
Missile guidance radar	Monitors and controls the path of the missile launched from the ground
Police radar	Locates and determines fast-moving vehicles
See-through radar	Used for "seeing" through walls
Terrain guidance radar	Helps to guide aircraft and missiles when flying in mountains or terrain
Weather radar	Forecasts weather conditions and detects thunderclouds

5.2.2 Radar Systems

5.2.2.1 Monostatic Radar

This is the conventional configuration of a radar system in which the transmitter and the receiver are collocated. A typical diagram of the monostatic radar is shown in Figure 5.3.

The monostatic configuration is proven in various applications. It works reliably when the main transmitted signal lobe is reflected from the object back to the receiver. However, with the introduction of new technologies (e.g., stealth) that reflect very little or no energy in the direction of the monostatic radar, the efficiency of the monostatic configuration is reduced. To mitigate this effect, new radar configurations were developed.

5.2.2.2 Bistatic Radar

This is a radar system comprising a transmitter and a receiver that are separated by a distance comparable to the expected target distance as shown in Figure 5.4.

Most long-range surface-to-air and air-to-air missiles employ the use of bistatic radar. Initially, it was used as a weather radar where it makes use of the forward scattering of the transmitted energy. Bistatic radars have shown good performance in detecting stealth aircraft, which have the shape that reflects more energy sideward and then back to the transmitter.

5.2.2.3 Multistatic Radar

This is a complex radar system containing multiple spatially distributed monostatic and/or bistatic radar components with a shared area of coverage [7]. Such a system allows improved detection range and accuracy. Figure 5.5 explains the concept of multistatic radar.

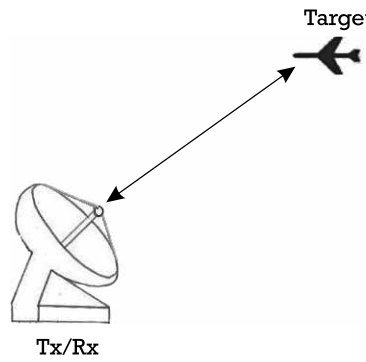

Figure 5.3 Monostatic radar.

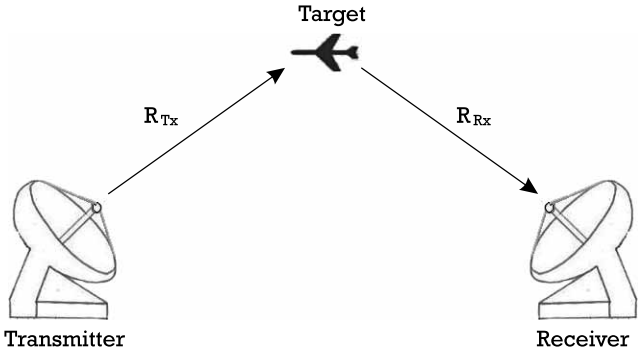

Figure 5.4 Bistatic radar.

In Figure 5.5, multistatic radar system consists of three monostatic radars (A, B, and C), which have the shared coverage area. In addition, there are two bistatic radar systems, created by radars A and B and B and C, respectively. To benefit from this configuration, multistatic radar system usually uses fusion of data obtained by all radar systems.

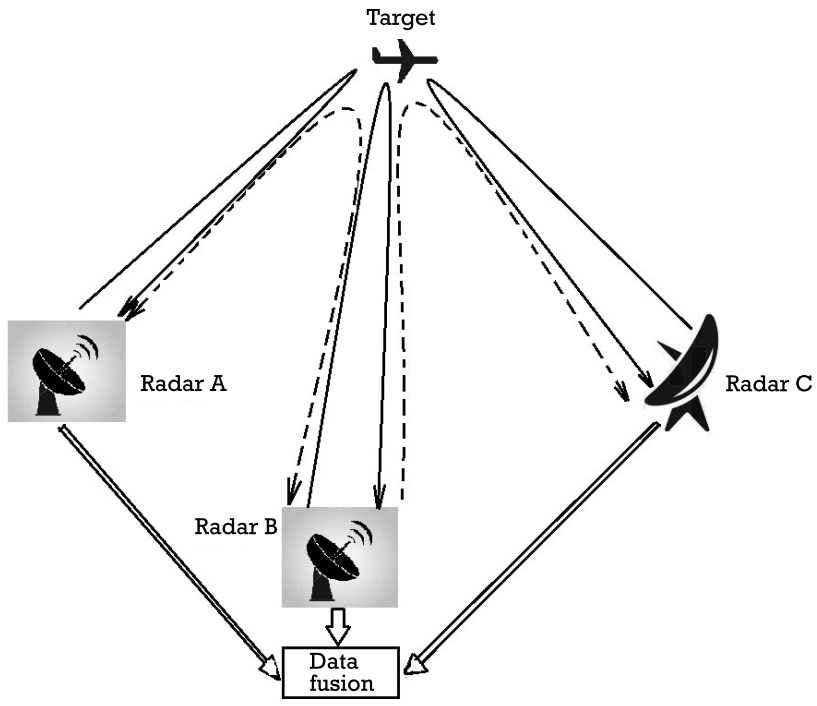

Figure 5.5 Conceptual diagram of multistatic radar system.

5.2.2.4 Doppler Radar

As the name suggests, this type of radar utilizes the Doppler effect to estimate the velocity of the target. It does this by analyzing how the object's dynamics has changed the frequency of the returned signal. Let c be the speed of light, f_t be the frequency of the transmitted signal, and f_r be the frequency of the received signal. From the well-known Doppler equation, we have:

$$f_r = f_t \frac{c + v}{c - v}$$

where v is the velocity of the object. Assuming that $v << c$ (which so far is the case for all man-made flying objects), we have the velocity of the detected object:

$$v = \frac{c \times \Delta f}{2 f_t}$$

where $\Delta f = f_t - f_r$, known as the Doppler shift.

As follows from the above simple equations, if no frequency change between the transmitted and received signals is detected, the target is stationary. However, when the object is moving towards the receiver, there will be an increase in the frequency and vice versa. This effect is also illustrated in Figure 5.6, explaining the classical Doppler effect.

The change between the transmitted and received frequency gives direct and highly accurate measurements of the radial component of a target's velocity relative to the radar. Doppler radars have applications in different industries including aviation, meteorology, health care, and many others.

5.2.2.5 Continuous-Wave Radar (CWR)

This is a radar in which a predefined continuous radio-wave signal is transmitted on a stable carrier frequency and the receiver is designed to receive this signal reflected from the object of interest. Usually, CWR utilizes Doppler technology for the detection of moving object and minimizing interference from the large stationary objects (e.g., buildings) or slow-moving objects. The advantage of CWR is their ability to determine the object velocity at a significant distance range without the high pick power, which leads to their low-cost implementation and operation.

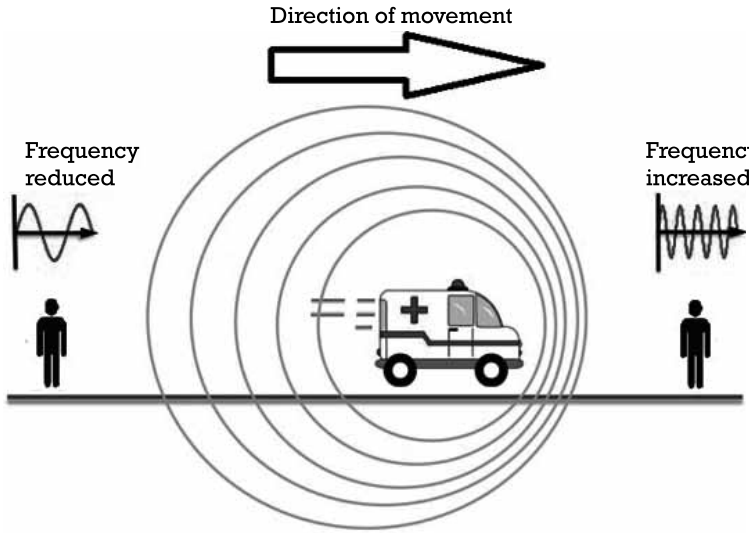

Figure 5.6 Doppler effect explained.

5.2.2.6 Frequency-Modulated Continuous Wave (FMCW) Radar

This radar transmits a continuous-wave signal similar to the CWR. However, unlike CWR, transmission frequency in FMCW radar is modulated in frequency (as the name suggests) and the frequency of the received reflected signal will be changed by a Δf and delayed by a Δt, similar to Doppler radars and as shown in Figure 5.7.

The FMCW radar will measure the frequency difference between the transmitted and received signals. The changes will be generated by the Doppler effect and are used to determine the target's distance and size. The frequency bandwidth of FMCW radar could vary between 1 MHz and several gigahertz, defining the achievable detection range and size of the target.

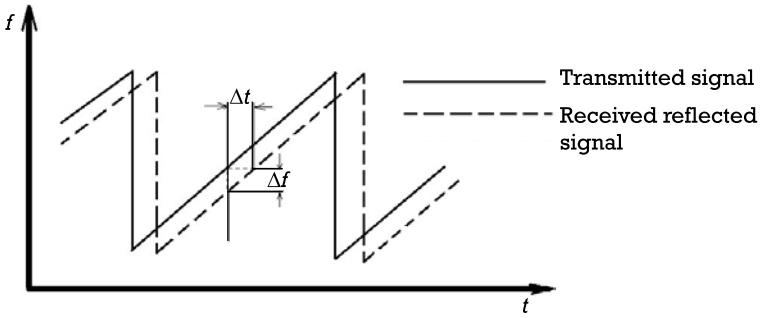

Figure 5.7 Transmit and received waveforms in FMCW radars.

The relations between the bandwidth, transmit power, and FMCW radar performance are illustrated in Table 5.2 [8].

From a C-UAV perspective, the FMCW radar could detect DJI types of UAVs (for example, 30 × 30 cm or 60-cm range resolution) at a maximum range of 500m, which is not fantastic as other types of radars could detect similar-size UAVs at a range in excess of a few kilometers. However, the advantages of FMCW radar are as follows [8]:

- The ability to measure very small ranges to the target;
- The ability to measure simultaneously the target range and its relative velocity;
- Very high accuracy of range measurement;
- A lower risk of hazardous radiation due to significantly reduced peak transmit power.

5.2.2.7 Passive Radar

These systems represent a special class of covert radar systems that detect and track targets by utilizing reflected signals from noncooperative transmitters, such as base stations (BS) of cellular networks and commercial broadcast transmitters, such as frequency modulation (FM) radio, digital audio broadcasting (DAB) radio, and terrestrial digital video broadcasting (DVB-T) TV stations. Passive radars could be considered also as a special case of bistatic radar, in which a transmitter is a noncooperative third-party transmitter. Figure 5.8 illustrates a passive radar system in which reflected signals from the noncooperative transmitter of the cellular BS are processed by the two radar receivers (A and B). It should be noted that in order to

Table 5.2
Bandwidth-Typical Range-Resolution Relationship for FMCW Radars

Bandwidth (MHz)	Range Resolution (m)	Maximum Range (km)
1	150	75
2	75	37.5
10	5	7.5
50	3	0.5
65	2.5	1.2 (note: with higher transmit power)
250	0.6	0.5
8,000	0.035	0.009

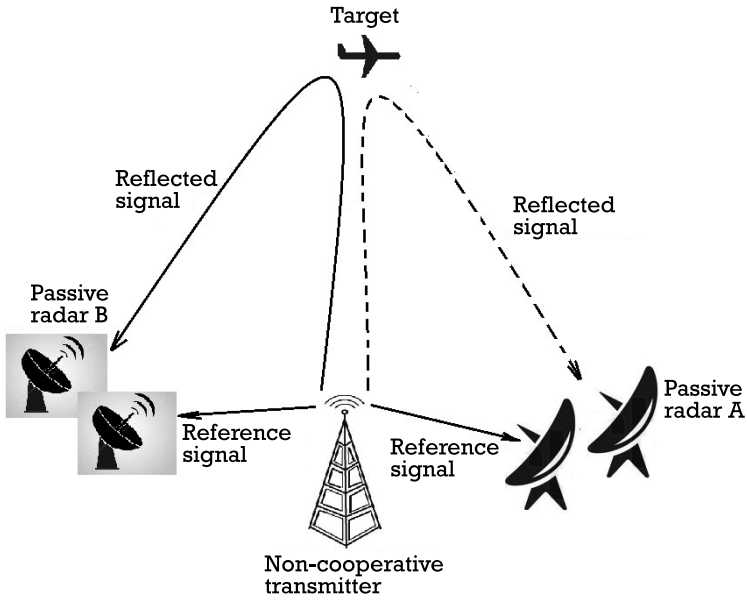

Figure 5.8 Example of a passive radar system.

process the reflected information accurately, each radar receiver must utilize a reference signal which is usually obtained via a separate line-of-sight (LOS) link between the noncooperative transmitter and the receiver. The accuracy of passive radar increases with the number of receivers in the system and strongly correlates with the deployment geometry as the distance of the receiver from the transmitter determines the level of external noise against which the targets must be detected.

A passive radar system utilizing one transmitter and only one receiver will be significantly less accurate compared to other types of radars. However, the detection range of these radars is significant as a passive radar using signals from high-power FM radio stations could achieve up to a 150-km detection range while utilizing low-energy signals from the cellular BS could provide a range of a few tens of kilometers.

5.2.2.8 Monopulse Radars

These use the phase antenna array to split the transmission beam into the two separate but overlapping lobes that have slightly different angles, as shown in Figure 5.9.

Furthermore, these lobes are polarized separately and are then rotated as in conventional conical scanner. Accordingly, there are two different reflected signals that are received separately. By comparing both the

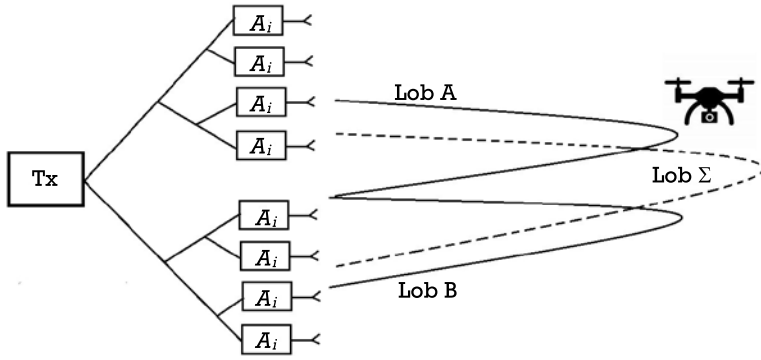

Figure 5.9 Concept of monopulse radar.

amplitude and the phase of these returned signals and calculating their monopulse ratio [9], it is possible to determine general direction of the target. If the lobes are closely spaced, this signal can produce a high degree of pointing accuracy and monopulse radars provide accuracy of up to 0.006°, which is equivalent to accuracy of about 10m at a distance of 100 km [10]. Monopulse radar is highly resistant to jamming, as to jam a monopulse system, a target would need to transmit a signal, which will duplicate both the polarization and timing of both lobs. Because the target receives only one lobe, precise polarization could never be exactly duplicated.

The performance of monopulse radars makes them a good candidate for C-UAV systems; however, their cost is often prohibitively high for the majority of C-UAV solutions.

5.2.2.9 Pulse Doppler Radar

As the name suggests, pulse Doppler radar is a radar system that uses a combination of techniques from pulse radar, continuous-wave radar, and Doppler radar to calculate the target's velocity. Pulse Doppler radars were originally developed for use on fighter aircraft to mitigate the effects of ground reflected signals. By taking into account Earth's movements and filtering out these reflections, pulse Doppler radars selectively excludes low-velocity reflections from the terrain and have look-down/shoot-down capabilities.

In addition to airborne and medical applications, pulse Doppler radars are widely used as meteorological radars, primarily for determining the speed of wind by detecting the movement of precipitation in the atmosphere.

In C-UAV applications, pulse Doppler radars can be used as airborne radars for the detection of UAVs in the designated airspace or as a ground-

based radar for the detection of LALE, MALE, and HALE UAVs. A typical block diagram of the pulse Doppler radar is shown in Figure 5.10.

In this configuration, the pulse Doppler radar will operate in two modes:

- *Scan mode (or detection mode):* In this mode, pulse Doppler receiver scans the airspace and applies the receiver frequency filtering, amplitude thresholding, and ambiguity resolution to all received signals. Once a reflection has been detected and potential target has been identified, the pulse Doppler radar automatically switches to tracking mode.
- *Tracking mode:* In this mode, the radar compares the difference between the measurements of the Doppler velocity against a predefined threshold. If the difference is less than the predefined threshold, the target will be locked, which eliminates the need for human intervention and significantly reduces the operational cost.

The performance of pulse Doppler radars strongly depends upon the pulse repetition frequency (PRF) so that these radars are classified as per their PRF, as shown in Table 5.3 [11].

As follows from Table 5.3, the selection of a radar's PRF depends upon the application. For example, if the priority of the C-UAV system is to detect rogue drones as early as possible, then a low PRF should be selected. However, if the priority is on accurate measurements of the velocity of the target UAV, then a high PRF should be selected.

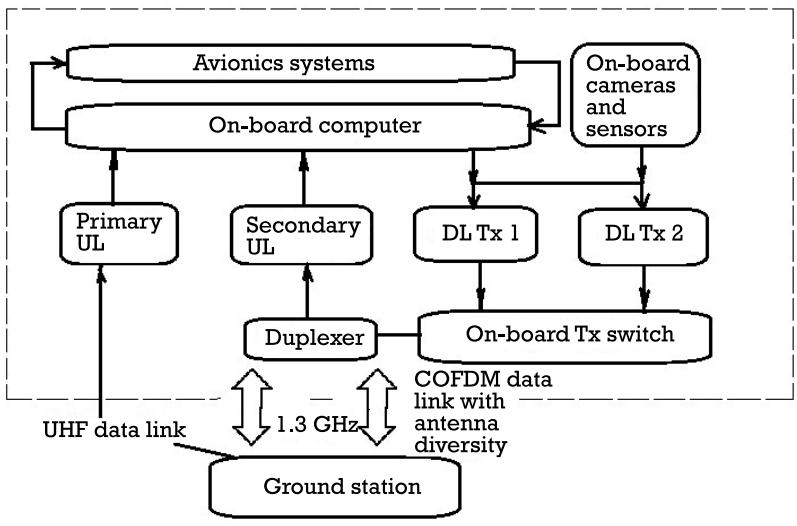

Figure 5.10 Block diagram of the pulse Doppler radar.

Table 5.3
Classification of Pulse Doppler Radars

Type or Characteristics	Range Measurements	Doppler Measurements
Low PRF	Accurate	Highly ambiguous
Medium PRF	Ambiguous	Ambiguous
High PRF	Highly ambiguous	Accurate

5.2.2.10 Synthetic Aperture Radar (SAR)

This is a class of radar that uses microwave signals to create two-dimensional (2-D) or three-dimensional (3-D) images of objects of interest [12]. Usually SARs are airborne radars that use the motion of the aircraft (or satellite) over a target region to provide high-resolution reconstructed images. SAR can be considered as a large aperture radar consisting of only one small-size antenna that moves over large distances collecting reflected signals at different locations. The distance traveled by the SAR carrier (aircraft or satellite) while the target area was in the view of the SAR is equivalent to the size of the antenna and is called synthetic aperture. Figure 5.11 illustrates the principle of the SAR operation [13].

The image resolution increases with the size of the synthetic aperture, while the synthetic aperture is usually larger for distant objects. Therefore, SARs are mainly used for military surveillance, remote Earth sensing, ocean current monitoring, and planetary observations.

Theoretically, it is possible to use SAR for the protection of large critical infrastructure objects against the rogue UAVs. All that is required is a small

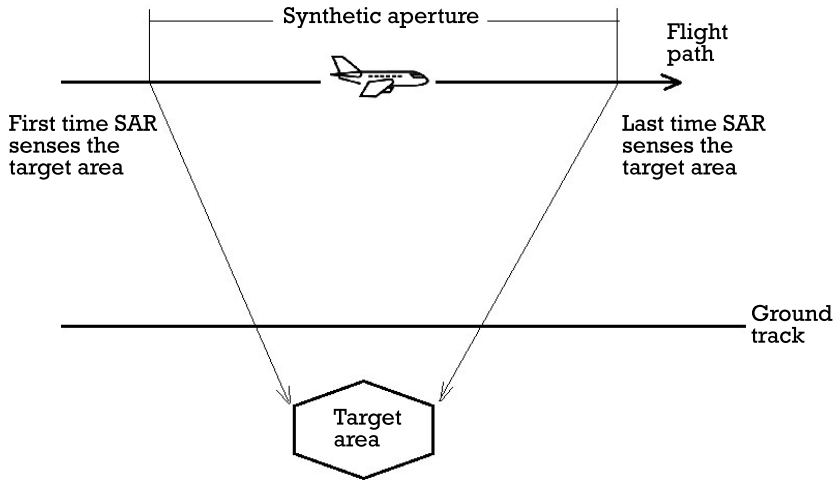

Figure 5.11 Principle of SAR operation.

antenna flying fast above and along the perimeter of the critical infrastructure and analyzing reflections of the transmitted coherent signals. The detection process will consist of two steps:

- *Calibration of the area of interest:* In this phase, a SAR image of the object will be created.
- *Monitoring and detection:* Any new object (including UAVs) that is not included in the calibrated image will be detected and classified.

Such a solution could probably provide one of the best C-UAV systems. Unfortunately, both capital expenditure (CAPEX) and operational expenditure (OPEX) of will be prohibitive for C-UAV applications.

5.2.3 Radars in C-UAV Systems

Considering the wide use of radars in aviation industry, it is not surprising that radars were the first sensors to be used for detecting rogue UAVs. Manufacturers of radars quickly identified an opportunity and applied the existing radars for the detection of UAVs. Almost every radar manufacturer announced the capability to detect UAVs efficiently, although the results were not always what the market needed as usually the manufacturers were facing one of two problems:

- The proposed radar was good in detecting various UAVs; however, it was too expensive for most civilian applications.
- The proposed radar was reasonably priced; however, its detection range and detection capabilities were not sufficient for noncivilian applications.

This led to the creation of two groups of products addressing different market segments:

1. Military grade 3-D radars with long detection range and baseline cost in excess of £1 million;
2. Civilian radars with short to medium detection range and a baseline cost around £150,000.

The radars that are within the first group have emerged from the military environment and a good example of such a radar is the C-UAV radar produced by RADA Electronic Industries from Israel [14].Their Tactical Multi-Mission Hemispheric (MMH) radars are software-defined, configurable

radar platforms that offer good C-UAV performance. The key characteristics of RADA's radar technology are:

- Pulse Doppler, software-defined radars;
- Armored, active electronically scanned array (AESA) antenna, GaN technology;
- Extremely high elevation coverage;
- Nonrotating, solid state radars;
- Digital: beam-forming, receivers, pulse compression;
- Compact and mobile, for tactical applications;
- High reliability.

It is not surprising that RADA's MMH radars have been selected by various defense establishments around the world.

Another C-UAV radar from the first group is GAMEKEEPER-16U a holographic radar developed by a Cambridge, United Kingdom-based start-up Aveillant [15], which was bought by Thales [16]. The Holographic Radar system differs fundamentally from both mechanically scanned radars and from electronically scanned systems. Holographic Radar floodlights a volume of interest on transmit and forms multiple simultaneous receive beams that fill the illuminated volume [15]. By focusing on targets continuously and for long periods, it achieves good detection performance against multiple targets. In addition, it produces a rich data set relating to individual targets, and after advanced signal processing, it generates very high levels of target discrimination and low false alarm rates. Like any other radar, it locates and tracks targets, but its very high Doppler resolution allows measurements of target movements.

The GAMEKEEPER-16U radar requires only a very narrow bandwidth compared to traditional radars and is able to detect, track, and classify small UAVs in 3 dimensions to a range of 5 km, providing the location and velocity of every object detected within its field of view.

As most of the radars from this category are evolving from the defense environment, it is not surprising that their technical details are restricted, and interested reader is advised to approach manufacturers directly for more detailed information.

A good example of a radar from the second group is the ELVIRA radar produced by Robin Radars in Netherlands [17]. With its pedigree from the bird detection in airports, the ELVIRA is a purpose-built drone detection radar, specifically designed to meet challenges caused by growing threats

from rogue UAVs. ELVIRA combines smart software with bird detection radar, specifically built for drone detection and tracking. ELVIRA can provide unlimited coverage by combining multiple radar devices into an integrated radar sensor network providing scalability, flexibility, and reliability. With the help of the dedicated graphic user interface (GUI), the outputs from multiple radars are incorporated into one unambiguous picture, meaning that a single drone causes a single alarm.

ELVIRA supports both fixed and nomadic installations. For fixed installations, it could be operational within minutes, while its nomadic version can detect UAVs within 60 seconds of stopping the vehicle.

ELVIRA is supported by the simple application programming interface (API), so that its tracks and alarms can be easily integrated with other sensors and third-party C2 platforms. To provide a visual picture of the target in order to take further action, ELVIRA can be equipped with a high-resolution pan-tilt-zoom (PTZ) camera for visual confirmation of the target.

Classifying and, most importantly, differentiating between drones and birds or other moving objects are critical features in preventing false-positives. Whereas other systems require a combination of multiple sensors to go from the detection to the classification of targets, ELVIRA combines detection and classification in a single sensor. This saves precious time in the decision-making process. The main technical specifications of ELVIRA radar are shown in Table 5.4.[2]

5.2.4 Summary

Radar sensors are essential in building a C-UAV system, especially for airports or large critical infrastructure in rural areas. The advantages of using radars in C-UAV systems are as follows:

- Radar can detect drones at a long range, providing early alerts.
- Radar can operate in adverse meteorological conditions where other sensors (e.g., optical) cannot.
- Radar signal can penetrate insulators, such as rubber and plastic, to capture the necessary data.
- Radar can provide accurate velocity and the exact position of an object.

However, radars alone cannot guarantee 100% UAV detection accuracy due to their intrinsic limitations:

2. We are grateful to Robin Radars (Netherlands) for showing these details.

Table 5.4
Main Technical Characteristics of the ELVIRA Radar

Technology	FMCW Radar
Operating frequency	9,650 MHz (X-band)
Power output	4W/36 dBm
Instrumented range	5 km
Detection range for 3-kg drone	3 km
Classification range for 3-kg drone	1.1 km
Main antenna beamwidth	10° × 10°
Azimuth coverage	360°
Elevation coverage	10° (−5° to +17° adjustable)
Azimuth resolution	1°
Range resolution	3.2m
Track while scan	Yes
Rotation/scan speed	45 rpm/1.3 seconds for 360°
Classification method	Micro Doppler
Dimensions	900 mm diameter × 1,000m height
Weight	72 kg
Communications	ETHERNET, 1000Base-T
Ingress protection	IP63

- Radars require a direct LOS to UAVs that they are trying to detect. A noncooperative UAV can bypass a C-UAV system consisting of only a radar by flying low and hiding behind the trees and the surrounding buildings.
- They work well in open areas but generate many false alarms in build-up areas.
- They struggle to detect hovering UAVs.
- They struggle to detect small and nano-UAVs.
- They require labor-intensive installations.
- Direction accuracy is dependent upon the size (and cost) of the radar (to generate accurate directions less than 0.5°) and a significant increase in cost is required).
- This is an active system that requires permissions to operate from radio agency.

- The cross-section of most UAVs is almost identical to that of birds, so some radar systems could produce a high level of false-positive signals when differentiating UAVs from birds.
- Even if a UAV is detected by the radar system, it will struggle to identify or classify the UAV.
- Radars in principle cannot detect the pilot of the UAV.

Therefore, most C-UAVs utilize other detection sensors in conjunction with radars, aiming to improve efficiency and accuracy of the UAV detection.

5.3 RF Detection Sensors

RF detection of UAVs is based on the interception and analysis of various signals exchanged between the UAV and a ground station. In general, the RF detection systems are classified as active or passive. Most of the known RF detection systems are designed as passive and rely on the detection and analysis of the uplink control signals transmitted by the ground station and/or the downlink telemetry and video signals transmitted by the UAV. Active systems operate like radars and combine a passive RF detection system with a dedicated transmitter whose sole purpose is to illuminate the drone and generate reflections of the transmitted signals from the drone.

As described earlier, various drones operate on different frequencies, but most commercial drones operate in Industrial, Scientific, and Medical (ISM) frequency bands of 433 MHz and 2.4/5.8 GHz. Simple power detection in these bands will not work due to presence of other legitimate users in the same geographical area. Therefore, most of the modern RF detection systems provide the detection and identification of the special unique signals generated by the UAV or data protocols implemented in a UAV. In [18], the authors described three different concepts for RF detection of UAVs:

- *UAV detection by analyzing the reflections from the propellers:* In this RF detection system, the drone is detected based on the signature of the signal reflected from its propellers, which could be observed by an off-the-shelf receiver (e.g., Wi-Fi receiver for detection of commercial micro-UAVs and mini-UAVs). The reflected signals will be modulated by the rotation speed and size of the propeller and delayed proportionally the distance between the UAV and the receiver station. Therefore, by analyzing the modulation and latency of the received reflected signal in both time and frequency domains, it is possible to identify the type of drones or at least its size. For example, the propeller of the Be-

bop AR Drone rotates with variable speed between 7,500 and 10,500 RPM, generating clearly visible signature of the drone in the frequency band less than 100 Hz [19]. Practical measurements described in [19] showed that the duration of each reflected signal varies from 1.4 ms to 2 ms correlated with the rotation speed of the drone's propeller in the time domain, and this signal can be used to develop an algorithm for drone detection. As expected, the reflection capability also depends on the drone orientation and often the signal is not fully reflected after passing through the drone propellers. Such RF detection systems are in early stages of their development and are expected to be very efficient when detecting drones flying in automatic mode with no communications with the ground station. However, at this stage of development, it works efficiently when the distance between the drone and the detecting system is less than 3m, indicating a long and challenging path towards the system that could be used in real practical scenarios.

- *UAV detection by analyzing the vibration patterns of the drone:* In these systems, the RF receiver analyzes the received signals, compares them with the existing library of signals (passive RF detection systems) or a transmitted signal (active RF detection systems), and is looking for changes in the signal. These changes can be detected by measuring the received signal strength (RSS) and phase (ϕ) modulations caused by drones' vibration [19]. This concept could be explained by the following simple equations.

  Let d be the distance between the drone and the ground station and Δd be the distance variation caused by the drone's vibrations; then the received signal strength (RSS) of the signal can be estimated from the well-known path-loss equation:

$$RSS = \gamma G^2 (d + \Delta d)$$

where $0 < \gamma < 1$ is the reflection capability of the drone's body, and the gain G is the attenuation gain of signals due to round-trip propagation. If we assume $\Delta d = 0$ for perfect drones with no vibrations, then we can assume that the RSS of such a perfect drone in perfect propagation conditions (no multipath, no deep fading) will be constant. Therefore, in perfect conditions, the fluctuation of the RSS will be caused by the change of Δd or drones' vibrations. In nonideal conditions, there will be additional variations of RSS due to propagation effects. However, for desired drone detection ranges ($d > 1$ km), the $\Delta d/d$ ratio is expected to be very small (approximately 10^{-3}% or less) and significantly smaller compared to RSS variations caused by propagation effects. Therefore, these small variation patterns could be used to detect the

drone and estimate the distance to the RF sensor. The accuracy and efficiency of such a detection will depend strongly on the receiver sensitivity and the noise level caused by other wireless systems operating in the area. For better resolution of distance variation detection, it is also possible to analyze phase variations of the received signal. This could be achieved using the following equation [19]:

$$\varphi = \frac{2\pi \times distance}{wavelength} = \frac{2\pi \times (d + \Delta d)}{\lambda}$$

where ϕ is the phase and λ is the wavelength of the received signal. Then the detected variations of ϕ could be used to analyze patterns of Δd and to detect the drone. As mentioned above, this principle is extremely useful in detecting drones flying in automatic mode; however, today, the detection range of RF detection systems utilizing this concept is not enough to be implemented in practical systems, although research in this area continuously promises more interesting results.

- *UAV detection by analyzing communication links between the drone and the ground station:* In these RF detection systems, a decision is made as a result of analysis of the uplink signals transmitted by the ground station and/or the downlink telemetry and video signals transmitted by the UAV. These RF detection systems are designed utilizing knowledge of the transport layer of the communication links between the UAV and the ground station, including the knowledge of the system topology and structure. This is achieved by building a library of signals for various drones and the better is the library the better will be the performance of the RF detection system. Passive RF detection systems that rely on these libraries first analyze control signals used by major drone manufacturers, then determine the distinctive features of these signals, and finally look for signals with those distinct features [20].

However, this raises a valid question: If most of the drones communicate with their ground station in 2.4/5/8-GHz frequency bands and utilize Wi-Fi signals, how could the RF detection system distinguish between a hovering UAV and a Wi-Fi access point (AP) operating in a nearby office?

The answer to this question is also simple: Even though communication link between the UAV and the ground station uses the same physical layer signals as in conventional Wi-Fi systems, there are certain differences in the transport layer that could be utilized for efficient RF detection. For example, in conventional consumer Wi-Fi systems, the exchange of beacons between the AP and peripheral devices (mobile phones, tablets, laptops, TV sets)

happens at a frequency of 10 Hz (or every 100 ms) [21]. However, most of the UAVs exchange beacons with the ground station at a frequency of 30 Hz [22–24]. This higher-frequency exchange is required to provide precise flight status data (which is changing rapidly) and to receive the flight control commands from the ground station. Furthermore, this is done in order to achieve robust and reliable communication between the UAV and the ground station, ensuring that the signals from surrounding Wi-Fi apps are not interfering with the UAV operation. Therefore, the RF detection system monitors communication channels and, in addition to measuring the RSS in 2.4/5.8-GHz bands, also observes the signal at frequency band less than 100 Hz. The analysis of these signals and comparison with signals from the system library allow for more efficient drone detection at distances in excess of 1 km.

A good library allows a user to detect and identify the airborne UAV in real time based on its data signals [18]. A typical example of such a system is the AeroScope family of RF detection systems, offered by DJI [25]. Leaving aside discussions about the business model in which a drone manufacturer also produces systems for detecting these drones, we need to emphasize that this system will achieve reliable detection and identification of the drones only if these drones are included in the database (i.e., DJI drones in the case of the AeroScope systems). Even if a good signal library is established and maintained, it is not enough for the development of the efficient RF detection system. There are three main reasons:

- The library can only be used when signals have been detected, which means that the sensitivity of the receiver and the ability to operate in a noisy environment are as important as the quality of the library [20].
- The UAVs operating in an autonomous mode and the Kamikaze UAVs [26, 27] do not maintain communication links with the ground station as they execute a flight plan or attack targets after the coordinates are entered into the UAV navigation system or based on a target image uploaded to the control system.
- UAVs used for malicious or illegal purposes will likely be homemade or hand-modified, so they will not match existing signal libraries [20]. We participated in trials where the RF signature of the off-the-shelf DJI Phantom UAV was modified in a particular way and the DJI AeroScope RF detection system failed to detect it even though the drone was maintaining all communication links with the ground station. Therefore, the detection of nonstandard drones in urban environments may not be successful.

Detecting the drone may not be sufficient in many practical applications. For example, if an RF detection system utilizes omnidirectional antennae, it will detect the drone but the direction of the drone or its angle of arrival (AOA) will not be known, making it difficult to apply an efficient countermeasure. Therefore, once a UAV is detected, is it is essential to determine the direction from which the classified signal is received and provide bearing of the detected drone, enabling a more efficient countermeasure.

Direction finding (DF) or radio direction finding (RDF) techniques were originally introduced in the early twentieth century, almost at the same time as the first radio communication systems become operational. One of the first RDF systems was developed in 1910 by W. G. Wade of the National Bureau of Standards in the United States, who used a large multiloop antenna to perform RDF. These systems were used extensively during World War II and the Cold War to locate unauthorized transmitters and radio operators. Before the era of GNSS, RDF was the main tool assisting pilots and sea captains in navigating their vessels. Even today, with the universal availability of GNSS, RDF is still used in aviation and maritime industries. Most of the technologies for RDF for UAVs were originally developed for passive detection and location of mobile phones. However, RDF systems for UAVs required additional development to incorporate specific features, such as simultaneous operation in multiple frequency bands and the requirement to detect and locate both the UAV and its pilot.

Direction finding refers to the use of specialized instruments, antennas, and methodologies to determine the physical location of a source of RF energy or targets. Accuracy requirements vary depending on application, but, for C-UAV applications, accuracy of less than a few degrees is a common requirement. UAVs may be stationary or moving (at various rates of speed) and, in the worst-case scenario, noncooperative. As can be seen in Figure 5.12, the principle of RDF is similar to the triangulation concept described earlier when explaining GNSS. However, unlike the triangulation technique, which provides the exact geographical coordinates of the object of interest and requires signals from a minimum of three satellites, RDF determines only the direction or bearing of the transmitter (in our case, the UAV transmitter) and the distance to the transmitter. It requires only two received antennae (although using more than two received antennae helps to improve the accuracy of direction and determines the location of the UAV). These receivers must be geographically separated, as the larger the distance between the received antennae, the higher the accuracy of measurement.

To explain the RDF concept, let us imagine a scene from a World War II movie in which the good guys are trying to capture the bad guys, who are using a temporary radio communication session to transmit critical

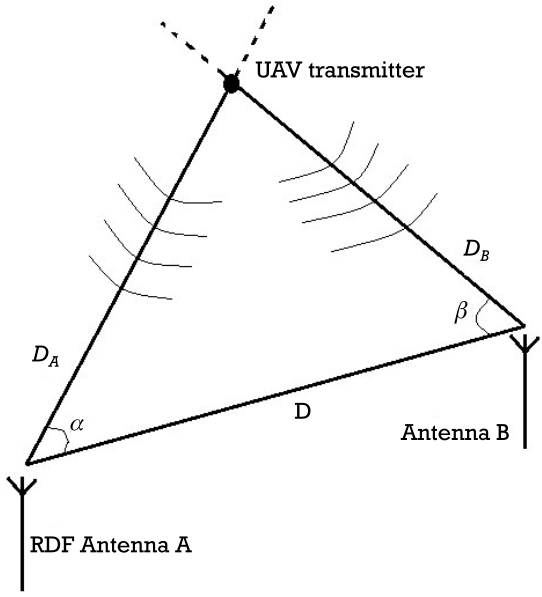

Figure 5.12 The concept of RDF.

information to their headquarters. The good guys are usually based in vehicles monitoring the signal strength, which is coming from the rotating antenna on the roof of the vehicle. The angle α is obtained for the highest level of the signal received in vehicle A. Accordingly, angle β is measured for the highest level of signal received in vehicle B. Knowing α, β, and distance D between the vehicles A and B, it is possible to calculate the distances D_A and D_B between the transmitter and vehicles A and B, respectively:

$$D_A = \frac{D \times tg\beta}{cos\alpha \times (tg\alpha + tg\beta)} \quad D_B = \frac{D \times tg\alpha}{cos\beta \times (tg\alpha + tg\beta)}$$

The typical block diagram of the RDF system is shown in Figure 5.13.

In Figure 5.13, various antennae are used for signal measurements in different frequency bands (for example, to apply RDF to commercial UAVs antennae operating in 433 MHz, 2.4 GHz, and 5.8 GHz will be required) in different locations. In modern RDF systems, mechanically scanning antennae are no longer used due to low accuracy defined by the mechanics of the scanning mechanism and cost. Instead, all existing RF detection systems utilize antenna array systems, which provide higher accuracy with reduced complexity and cost.

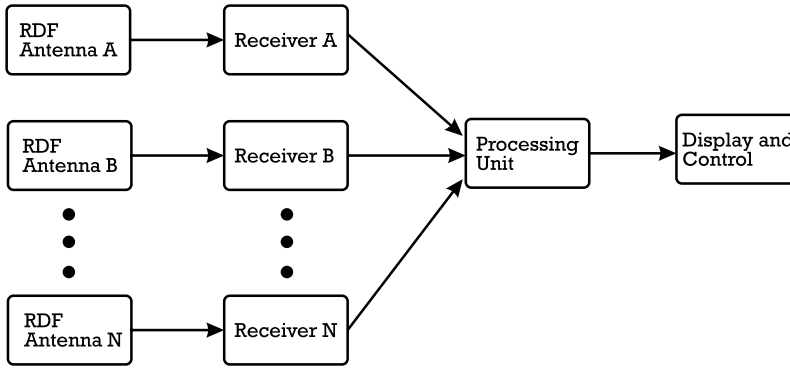

Figure 5.13 Block diagram of the RDF system.

The above example of the RDF system that we described is also known as the RDF system that measures the AOA. The system generates bearings for each of the installed receiver stations, which are defined as AOA. The AOA RDF system measures the angle(s) at which a signal arrives at an antenna array: not the phase or time differences of the signal at different elements. The criteria for confirming the signal arrival at an antenna is the maximum power of the incoming signal at the antenna. Therefore, AOA is also known as the maximum power of arrival (POA) technique.

AOA is a very straightforward RDF methodology, as there is no requirement for time or phase alignment and frequency comparison. It utilizes simple receivers and does not require a complex calculation of bearing. The accuracy of AOA systems increases with the increased number of distributed antennae. These systems work efficiently on all types of signals but are highly susceptible to multipath; a clear LOS is often required for satisfactory results.

Multipath is the phenomenon caused by reflections of radio signals from various objects located in the vicinity of the receiver in general or RDF receivers in particular. In the presence of multipath, the transmitted signal reaches the antenna by more than one path. Since these signals have different propagation paths, they arrive to the receiver antenna at different time instants with different phases, resulting in variations of signal levels, also known as fading. In the extreme case of multipath, the signal could take two different paths and arrive 180° out of phase, canceling each other out. In reality, this is not a practical concern, especially as the number of bearings taken from multiple locations increases.

Depending on frequency band, multipath appears as a result of atmospheric ducting, ionospheric reflection and refraction, and reflection from terrestrial objects such as mountains and buildings [28]. For frequencies

that are used for communication between the UAV and the ground station, the main cause of multipath is the reflection from water and buildings. The principle of multipath is explained in Figure 5.14.

When it comes to drone detection in open areas, such as airports, large critical infrastructure (e.g. nuclear power stations), or open-air events (musical festivals), this is not a dramatic problem as in these conditions multipath is minimized due to clear LOS visibility between the UAV and the RDF receiver.

However, in an urban environment, multipath is the biggest issue in the RF detection of UAVs and direction finding. Coupled with interference from other transmitters operating in the vicinity of the receiver, the performance and accuracy of AOA RDF systems in an urban environment dramatically reduces as each received signal generates a false-positive target alarm, indicating virtual UAVs and requiring a manual check of all detected targets. One of the best ways to overcome multipath is to take many bearings from many unique locations: many being on the order of hundreds to tens of thousands [29]. Obviously, this creates two challenges:

- *Computation:* Triangulation does not benefit from an extremely large number of bearings.
- *Complexity and cost:* The procuring, setting, and operation of such a system will require a lot of planning and will result in a high cost (including the cost of operations), which most likely will not be acceptable to the user.

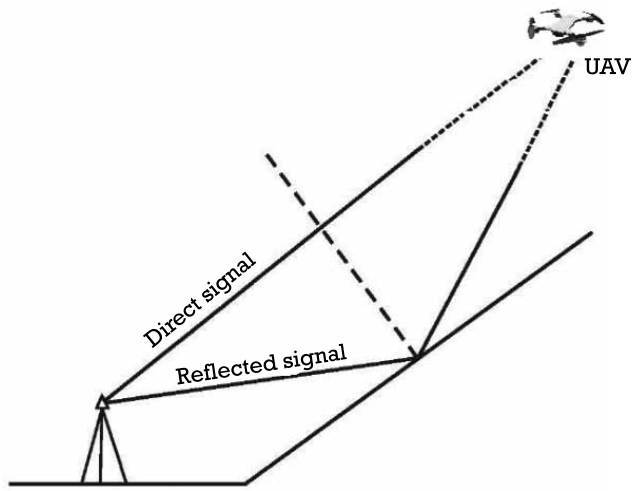

Figure 5.14 Concept of multipath.

Another technique for RF detection and location of the UAVs is based on the principle of time difference of arrival (TDOA), which allows mitigating some of the effects of multipath. As shown in Figure 5.15, in TDOA, a minimum of three receivers at different locations receive a signal from the target (UAV).

As the paths between the UAV transmitter and the receivers are of different lengths, there are differences in the time of arrival at the different receiver locations. These time differences can be represented as hyperbolae that cross at the location of the transmitter of interest. The block diagram of the TDOA system is very similar to the block diagram of the AOA system shown previously. However, in the TDOA system, all receivers are connected to a master station over a data link that transmits time-stamped digitized intermediate frequency (IF) from the remote receiver to the master station. At the master station, a cross-correlation function between all received signals is calculated and this calculation yields the estimation of the time difference between the received signals [29]. Once the time difference, Δt, between the received signals is known, the TDOA processor then computes and plots hyperbolae representing this distance between the UAV and various receivers. The intersection of multiple hyperbolae yields the estimated UAV location.

In practice, the TDOA measurement results typically are accurate to within a 1-km range; however, the performance and accuracy depend strongly on the geographical location of the receivers [30]. Therefore, to provide the most efficient TDOA system, some pre-knowledge of the transmitter location is essential. This obviously creates challenges for C-UAV system operators, as rogue UAVs could appear from all possible locations. However, with good planning and clearly defined requirements and security threats, this problem can be solved, especially for large critical infrastructure objects, such as airports, where receivers are installed at the perimeter of the no-fly zone.

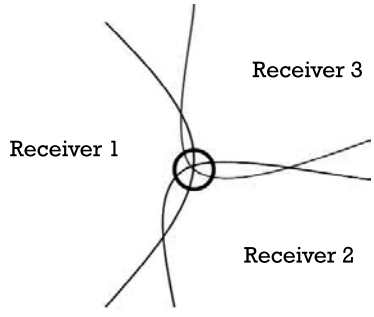

Figure 5.15 The concept of TDOA.

There are numerous UAV RF detection systems that are advertised as the best on the market with "better than 1° accuracy in direction finding" and "effectively unlimited range" [20]. However, these claims need to be taken lightly, as most of the results are obtained in ideal laboratory conditions or in low RF emission environments. We attended a great number of demonstrations where the excellent performance of RF detection systems demonstrated was downgraded dramatically as soon as other sources of RF emission were switched on (i.e., radars, numerous Wi-Fi apps, jamming devices). However, we also observed some really stable and impressive performances from RF detection systems, and it is not surprising that these are the systems that are already installed in various critical infrastructure locations around the world. Next we present a very brief description of these systems; however, this description should not be taken as the comprehensive review of RF detection systems or as the recommendations.

5.3.1 SkyArcher (ST Engineering, Singapore)

The SkyArcher Drone Detection System is a multisensor integrated system that uses signal detection, direction finding, and visual analytics to automatically detect, classify, and track commercial drones. The RF signal detection provides an indication of the direction of drone controllers (i.e., drone operators) and target drones, coupled with visual analytics for the identification, classification, and tracking of the target drones. The RF signal detection provides an indication of the direction of drone controllers (uplink signal) and target drones (downlink signal). It also identifies the drone model based on the Drone Remote Control Libraries. Table 5.5 shows the RF detection sensor parameters.

The overall SkyArcher system is shown in Figure 5.16.

The SkyArcher system has been installed in a number of critical infrastructure locations in the Far East since 2016 and has shown good results despite operations in extremely challenging conditions (temperatures up to +55C, high humidity, and a high RF noise environment).

5.3.2 SKYPERION (METIS Aerospace, United Kingdom)[3]

SKYPERION is an RF multisensor solution that provides the operator with a timely, high-confidence, actionable understanding of UAV activity. The sensors and their detection techniques ensure a high probability of interception across a wide range of targets, whether they are UAVs or other possible threats to the area to be protected. SKYPERION is designed to integrate into

3. We would like to express our gratitude to METIS Airspace Ltd. (U.K.) for providing materials related to the SKYPERION system.

Table 5.5
Parameters of the SkyArcher
RF Detection Sensor

Parameter	Performance
RF detection frequency range	20 MHz–6.0 GHz
Number of libraries	15*
Geolocation sector coverage	5° to 15°
Detection range in LOS	1 to 2 km

*This number was correct at the time of this writing. ST Engineering constantly updates and increases the number of libraries.

Figure 5.16 The SkyArcher system installed in the Far East. (We would like to express our gratitude to ST Engineering (Singapore) for providing materials related to SkyArcher system.)

a configurable and flexible network of deployed sensors through a single, easy-to-operate software interface, where all the sensors contribute to the final decision-making process. The relevant information is presented to the operator in a configurable means to allow decisions to be made in a clear and distinct manner.

SKYPERION provides the user with the capability to search, detect, identify, track, and report unauthorized UAVs. The system can operate in all weather conditions during the day and the night. The capability has been designed for minimal operator interaction, with the aim to allow operation with a 75% distracted operator during standard operations as well as being interoperable with other C-UAS sensors. The SKYPERION architecture allows both fixed and nomadic installations and supports spiral upgrade development. Figure 5.17 illustrates current SKYPERION installations in various critical infrastructure sites.

The SKYPERION software interface provides a simple-to-operate user interface that integrates the sensors deployed into a single solution. The

(a) (b)

Figure 5.17 (a) Fixed and (b) nomadic SKYPERION installations.

software is fully configurable to suit the needs of the operator in the field, but with a two-level operation, a more expert operator can access more detailed information if required.

SKYPERION can also detect, track, and identify most drone controllers. Its enhanced capability upgrade provides the ability to record, display, and output the individual hop parameters for direct sequence spread spectrum and frequency hopping spread spectrum (DHSS/FHSS) drone controllers such as DJI/Futaba drone controllers. With time synchronization, this will allow a partner RF mitigation system to surgically jam the drone control signal limiting fratricide to the RF spectrum.

The key features of the SKYPERION software include:

- Real-time spectrum monitoring;
- Multimission capability;
- Scalable from one to many sensor nodes;
- Wired (Cat5 and fiber) and wireless node network;
- Multiformat spectral displays;
- 2-D mapping;
- Automated detection using AI and parametric detection capabilities;
- RF signal parameter output for mitigation capabilities.

These features offer the operator several benefits including improved situational awareness, increased operational agility, and real-time information

sharing of the activity in their area of interest. In addition to the real-time operational activities, the software can offer post-mission data analysis and signal identification capabilities by use of its record function.

SKYPERION offers the customer a cost-effective solution utilizing a minimum of two RDF sensors for geolocation, with the capability to add more as well as the ability for integration into a larger, multilayer C-UAS system if required to provide tailored coverage. The performance of the SKYPERION solution is driven by several parameters including range, transmitted power, terrain masking, and RF noise levels. The RDF sensors clearly indicate the location of the UAV by the intersection of the two lines of bearing from each sensor. The main parameters of SKYPERION are summarized in Table 5.6.

In summary, SKYPERION is a well-established and proven RF detection and tracking system with the following key benefits:

- Conducting detection, identification, and geolocation of multiple UAV systems simultaneously across multiple RF bands;
- High probability of detection;
- Early detection of UAV (prior to takeoff);
- Automated detection and geolocation tools;
- Detection of the UAV's radio control unit;
- Low false alarm rate;
- Day and night and all-weather operations;
- Operations;
- 360° azimuth coverage.

5.3.3 Drone Hunter DHS-PRO (Fortunio, Hungary)

The DHS-PRO system is a proprietary solution which is not based on spectrum analysis of communication and control signals. Instead, the system detects signal generated by the UAV propulsion system. It is a reliable and cost-effective UAV detection system with almost no false alarms. The system is particularly efficient for detecting UAVs flying in autonomous mode (without communication with the ground station) and is combined with a variable power jammer, which will be described later. The system allows a fully automatic operation with no dedicated operator, which significantly reduces operational costs.

Table 5.6
The Main Parameters of SKYPERION

Detection/Classification Specifications	Value
Detection Range UAVs: rural	>2.5 km
Detection range UAVs: urban	1.5–2 km
Detection range controllers: rural	>0.8 km
Detection range controllers: urban	0.4–0.6 km*
Simultaneous UAV detections	4 UAVs tested, >10 UAVs theoretical
UAV detection	UAV and/or transmitting element controller unit
Minimum automatic parametric detection signal-level UAV	5 dBm (2 × standard deviation) above RF noise level**
Minimum automatic parametric detection signal-level controller	8 dBm above RF noise level**
UAV detection speed	Up to 50 m/s
UAV initial detection time	90 frames/0.8 second (parametric detect)
Detect methods	Masking: fixed and custom (pattern of life/new drones), parametric AI
Background masking	None, partial, full custom masking across spectrum
Data logging	Full selectable and autonomous if selected
Azimuth monitoring	360°
Azimuth error	±5° RMS
Elevation	Surface to +90°***
Compass accuracy	±0.5° (1σ) for pitch <60°
Compass resolution	0.01°
GPS positional accuracy	<2.5m CEP, 50% typical <5.2m CEP 95% typical
Frequency range (standard)	400 MHz to 6 GHz
Polarization	Circularly polarized antennas
Maximum instantaneous bandwidth	100 MHz
Scan rate	>400 GHz/sec
Deployment	Distributed receiver network capability, so multiple sensors (unlimited) can be deployed, suitable for harsh environments, mobile, portable or permanent mount options
Operator functionality	
UAV positioning	UAV azimuth (line of bearing), UAV GPS coordinates, UAV distance
UAV mapping	Map overlay with UAV positions
Recording	24-hour recording, event replay, full data rate stream to host if selected
Telemetry logging	All logs/events recorded

*Subject to LOS to the target and maximum power transmission from the controller, indicative of DJI Lightbridge 2 (Phantom 4 and Inspire) in open conditions. Dependent on other interfering signals such as Bluetooth. **Based on DJI Phantom 4 (setting configurable for environment). ***The azimuth error will increase above +60° elevation.

The system can be installed as a fixed permanent network around the desired protection area or as temporary nomadic perimeter protection unit for ad hoc operations (military exercise, sporting or public event). Its performance and validity are verified in a numerous practical installations in Europe and the Middle East (see Figure 5.18).

5.3.4 AIRFENCE (Sensofusion, Finland)[4]

The AIRFENCE 6.0 is a proven, integrated RF system that allows reliable UAV detection, tracking, and mitigation (in this section, we cover performance related to RF detection while performance related to jamming will be covered in another section). The system operates in the frequency band from 300 MHz to 6.0 GHz; it is developed based on highly efficient low noise power architecture and, as a result, offers a detection range of up to 10 km for DJI-type drones. AIRFENCE offers extremely a low detection time (about 1 second once the drone is within the detection range). A flexible system architecture allows AIRFENCE 6.0 to be used as a standalone unit or in conjunction with other sensors as an integral part of a larger C-UAV system. The standalone mode is typically used for mobile installations on vehicles, ships, manned/unmanned aircraft, and VIP (very important people) convoys. No external connection is required when used as a single sensor, although AIRFENCE could be easily connected to the existing sensory C-UAV network.

For fixed installations, AIRFENCE requires a dedicated server that could be arranged in two ways:

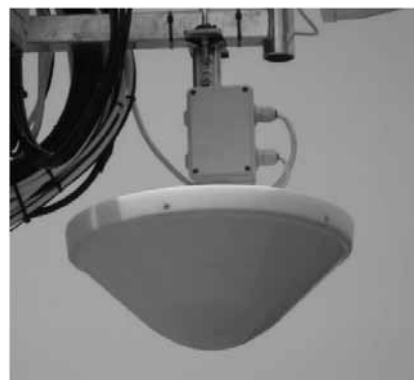

Figure 5.18 Drone Hunter System installed in Europe. (We would like to express our gratitude to Fortunio Ltd. (Hungary) for providing materials related to the SkyHunter system.

4. We would like to express our gratitude to Sensofusion (Finland) for providing materials related to the AIRFENCE system.

- *AIRFENCE sensor network, hosted by Sensofusion:* In this case, AIRFENCE is connected to the dedicated Sensofusion servers via the internet and Sensofusion ensures the 24/7 operational capability including the latest software updates. Typical application environments include airports, prisons, industry sites, and warehouses.
- *AIRFENCE sensor network, hosted by the customer:* Such an AIRFENCE installation in the customer environment is typically required when operation has a classified status (e.g., military, soldier of fortune (SOF), police). All sensors are connected to the AIRFENCE server, hosted by the end customer.

In the detection and tracking mode, AIRFENCE is implemented as a passive RF detection system suitable for both fixed and mobile installations. This is achieved through a special design of a directional antenna, which incorporates three individual antennae with the following parameters:

- *Antenna 1:* 6-dBm direction finding antenna in 2.4/5.8 GHz;
- *Antenna 2:* 3-dBm omnidirectional antenna in 433 MHz;
- *Antenna 3:* 3-dBi omnidirectional antenna in 915 MHz.

Once a UAV is detected in a predefined geographical area, an SMS mobile notification or email is sent to the authorized personnel. In parallel, an active RF jammer is activated and the UAV detection log is created for future forensic use and prosecution.

AIRFENCE 6.0 is IP-rated, weighs less than 10 kg, and could be installed in less than 10 to 15 minutes. Its performance is proven in a number of installations in Europe and around the world.

5.4 Optical Detection Systems[5]

To cover all eventualities [about drone detection] there needs to be a suite of sensors and, ultimately, they have to be able to detect drone optically.

—Captain Tim Pottage,
the representative of the British Airways Pilot Association [1]

5.4.1 Types of Optical Detection Systems

As all UAV pilots and operators of C-UAV systems know, a micro-UAV or mini-UAV is difficult to detect visually, especially while in motion. The

5. We would like to express our gratitude to Denis Kolev of Rinicom Ltd. (United Kingdom) for providing materials related to AI-based EO/IR detection and classification.

probability of visual detection without previous knowledge of the UAV position at distances above 100m is very small, while at distances in excess of 300m, it is almost impossible. In [31], Farlik described the results of dedicated experimental trials of various visual UAV detection sensors.

5.4.1.1 Visual Detection by Humans

The following are methods of visual detection by humans:

- *Binoculars LEICA 7 × 42:* With the preliminary localization by human sight, detection was possible up to around 200m. Tracking of the localized UAV without a tripod was possible at a distance up to 1.2 km.
- *TZK 10 × 80 air defense military binoculars:* With a known location, it was possible to detect the UAV with binoculars and track the UAV by the main objective lens at a distance up to 1.2 km.
- *ReTOB:* This professional device for aerial target detection was used by skilled professionals. In the preliminary localization of the UAV (e.g., provided by the radar), it was possible to detect and track the UAV at a distance >1.5 km.

5.4.1.2 Infrared (IR) Sensors

The detection in the IR spectrum has serious constraints due to well-known physical principles and a strong influence on detection range by the environment. The IR sensor measures the contrast of the thermal sign of the object and the background. When applied to the detection of UAVs, an IR sensor will measure the thermal signature of the motors and propellers and the entire UAV or background sky. The accuracy of measurement depends on UAV motor temperature, the color of the UAV, the IR camera angle of view, the IR camera temperature (cooled or uncooled), wavelength, the distance between the IR camera and the UAV, and the structure of the UAV. The typical results for detection of TAROT F650 (650 × 650 mm) UAV by FLIR A40 microbolometer (320 × 240 lines resolution) are shown in Table 5.7, while the results for the DJI Phantom (350 × 350 mm) indicate that the range will be proportionally less.

To achieve the desired range, military-grade, cooled thermal imaging cameras are used, but the cost of these IR cameras rises dramatically with improved resolution and added cooling options (we do not know a good IR sensor solution that will cost less than £200,000) and cooling also adds dramatically to the operational cost. Therefore, only a high-end, military-grade C-UAV system utilizes IR sensors, while most civilian C-UAV systems rely on radar and RF detection in dark conditions.

Table 5.7
Characteristics of FLIR A40 Microbolometer

Operation	Range (m)
Detection	<300
Recognition	<70
Identification	<30

5.4.1.3 EO Sensors

Until recently, C-UAV systems had utilized EO/IR sensors, which were guided by other sensors (radar, RF), primarily for providing visual images of the drone and its payload, and recorded images for forensic investigation and eventually for prosecution.

As with all conventional optical systems, it was anticipated that the performance will suffer in dark and foggy conditions and detection capability will be constrained by the availability of high-spec lenses and the LOS vision of the UAV. For example, even on high-resolution EO cameras with a standard horizontal field of view used in industry (ranging from 20° to 45°), the linear size of the DJI UAV is just few pixels at distances in excess of 200m. This makes these UAVs undistinguishable from the noise or any other moving object (like birds or airplanes in the background). In order to identify the object as a drone, the field of view should be very small, which makes it hard to capture a maneuvering high-speed object such as a drone.

However, despite all these drawbacks, several C-UAV systems with EO/IR sensors were installed at various critical infrastructure sites around the world. Unfortunately, all the anticipated drawbacks of EO/IR systems appeared during the operation of these systems. Worst of all, new unexpected drawbacks transpired as these EO/IR systems were generating a high false alarm rate when used for the detection of the drone and the operation of EO/IR systems in conjunction with other sensors required continuous involvement of the operator, significantly increasing the operational cost.

5.4.2 Optical Detection with AI

A novel approach to optical UAV detection, classification, and tracking has been developed by Rinicom and is protected by a U.K. patent application [32]. Unlike conventional systems, this system, called SkyHunter, utilizes two EO/IR cameras in conjunction with two corresponding AI algorithms. The system utilizes the deep learning approach for image processing combined with the availability of the general-purpose graphic card processing units (GP-GPU) and super high-resolution machine vision camera mod-

ules. As shown in Figure 5.19, the detection and identification of UAVs in SkyHunter are split into two main stages:

- *Preliminary detection:* The preliminary detection of distant objects is achieved by static high-resolution cameras. By applying methods such as background subtraction and multiple object tracking, a set of moving objects is extracted. Detected objects are marked as potential targets (zoom requests) using statistically fitted classification algorithm, based on trajectory features.
- *Classification:* After an object is detected, accurate bearings are provided to a PTZ camera that is pointed at the object for a few seconds, provides images for further classification using deep learning-based recognition algorithm, and then returns to the standby position ready for the next object to be classified.

Such an approach allows the simultaneous detection of multiple drones (practically unlimited numbers) at extremely large distances utilizing relatively simple and inexpensive camera modules. In addition to the detection

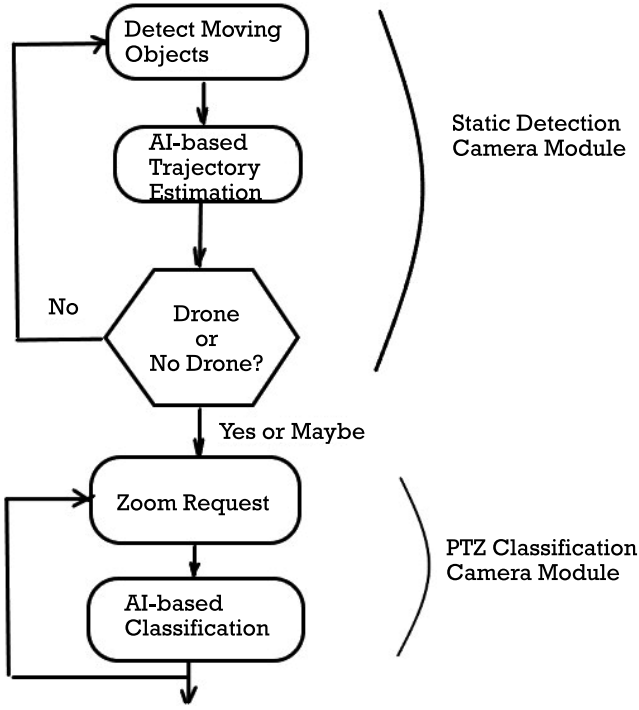

Figure 5.19 Workflow of the SkyHunter EO/IR system.

and classification, the system provides very accurate (less than 0.1°) UAV geographical angular positioning and rough coordinates' estimation and continuous tracking. All the data, including the detection and recognition of data and images of detected and recognized objects, are stored and shared with the C2 platform. The joint software and hardware architecture of the system is presented in Figure 5.20.

In this configuration, the system is designed as the multimodule system, which processes the information from multiple sensors. A typical SkyHunter installation consists of the following submodules:

- *Detection camera module (DCMs):* This is composed of several static high-resolution cameras, where each camera is connected to a separate processing board (GP-GPU or just a powerful CPU), which performs the preliminary detection algorithm part. These modules are referred to as DCMs. Each DCM sends the obtained information and position for each detected object for each processed frame to the dispatch and control service. The position of each object, its identification, and other temporal characteristics of the object are encoded in the object descriptor.
- *Dispatch and control service (DCS):* This receives the information from all attached DCMs, converts the received objects position into a global coordinate system, and orders the detections into a prioritized queue for processing by the recognition camera module. From the recognition module, the DCS receives the classification results. The DCS sends all available information to the information processing service. The DCS

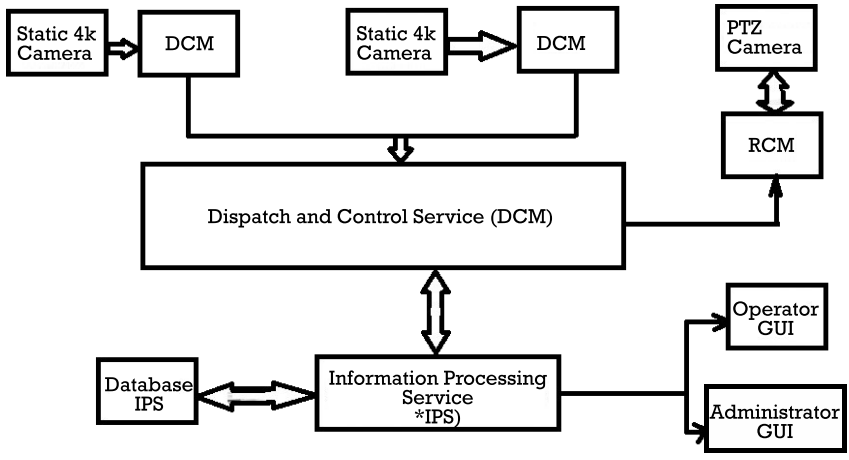

Figure 5.20 SkyHunter joint software and hardware architecture.

analyzes the data received from different DCMs and merges the detections, related to the same real-world object, captured by several DCMs (this algorithm is further denoted as a handover).

- *Recognition camera module (RCM):* This takes the candidate targets from the prioritized queue organized by DCS. The RCM controls a PTZ camera, so that it follows the selected potential target and performs the optical classification. The tracking is performed using the object positioning obtained on DCM. As the RCM performs a deep neural network classification, it is suggested it to be installed on a GP-GPU platform. The RCM sends the classification results for each processed object to the DCS.
- *Information processing service (IPS):* This receives the descriptors and classification results from (possibly) multiple DCSs and stores them in the database.

5.4.3 Detection Algorithm Overview

The detection range of the DCM significantly depends on the parameters of the camera used. The smaller field of view and the larger the resolution of the image, the higher detection distance that may be achieved. More precisely, the following equation approximates the size of the drone in pixels at given distance for specific image parameters:

$$n_d = \frac{l_d N}{2L \tan\frac{\beta}{2}}$$

Here n_d, l_d are the pixel and linear size of the drone correspondingly, N is the horizontal size of the image in pixels, L is the distance to the drone, and β is the horizontal field of view. Thus, assuming that 3 pixels are enough for detection (this fact is supported by numerous experiments), the detection distance for DJI Phantom (~30 cm linear size) for a 42° field of view (FOV) and a 4 Mpix camera is around 500m; for a 30° FOV and the same camera module, the detection range is more than 700m.

$$b_t = (1-\alpha) b_{t-1} + \alpha I_t$$
$$s_t = (1-\alpha) s_{t-1} + \alpha (I_t - b_{t-1})^2$$

where b_t is the background mean, s_t is the variance, and I_t is the image at moment t. The main challenge in the processing is driven by the fact that

the size of the drone in pixels is very small, which does not allow us to use any filtering techniques. The foreground is determined by the following thresholding:

$$f_t = \left(I_t - b_{t-1}\right)^2 > \mu_{t-1} s_{t-1}$$

A set of connected components is extracted from the foreground image f_t: $C_t = \left\{c_t^1, \ldots, c_t^l\right\}$, which are to be associated to the set of tracked objects $O_{t-1} = \left\{o_{t-1}^1, \ldots, o_{t-1}^m\right\}$. In a general case, $m \neq l$.

Multi-object tracking is done by bank Kalman filtering with the association performed using a simplified Hungarian algorithm [33]. The visible variables of the Kalman filter are given by the position of the blobs and their speed. The hidden variables define the position of the object and the object speed. Blobs are associated to the objects by maximum-likelihood association rule, formalized as an optimal assignment problem.

For each object for each moment of time (each processed frame), a vector of features is extracted, which includes trajectory-dependent characteristics, such as speed, speed variance, acceleration, connected component average size, and angular speed variance. Based on the extracted feature vector, a classification is performed using bagged decision trees [34] and the least absolute shrinkage and selection operator (LASSO) regression [35]. The classification model is trained using semi-supervised learning methods.

If the per-frame classification frequency exceeds the given threshold, the object is marked as a potential target or zoom request.

The DCM sends the information about all available potential targets to the DCS each frame. The information contains enough information for the RCM to rotate the PTZ camera to the object with high precision and follow the target until it is classified or lost.

An important characteristic of the DCM is the number of frames processed per second. This parameter influences the detection quality, as a lower number of frames complicated the association of objects and adaptive estimation of the background. The best quality is achieved usually if this number is higher than 12 to 14. In order to achieve this number using CPU processing with high-resolution cameras (such as 12 to 20 MP), a low-level optimization should be performed, such as vectorized number processing (SSE, AVX). At the same time, GP-GPU platforms achieve much higher numbers, which makes them preferable.

5.4.4 Classification Algorithm Overview

The RCM solves two main problems:

- Object tracking based on the information received from DCS (DCMs);
- Object classification.

In order to properly track the object, the RCM must synchronize three data streams:

- Stream of descriptors for the zoomed object from the DCMs;
- Stream of the PTZ camera position information;
- Stream of frames (images).

In general, this is necessary to know for each descriptor what was position of the camera was and which frame corresponds to the described object position. Thus, it is possible to estimate how to rotate the camera to track the object and whether the object is present on the image. The camera could be navigated only by the information from the DCM descriptors. The angular positioning accuracy of the objects obtained from DCM is very high, due to the high resolution of the camera. Additional image tracking by the detection technique could be used, but not as a main driver for the navigation, as these approaches are much less reliable. This is partially explained by the poor quality of the image-based object tracking for small objects from moving camera (with no background). However, DCM-based navigation requires the PTZ camera to be placed close to the static camera, so that the transformation of the angular coordinates of the object may be obtained through rotation. Large displacement between cameras may lead to incorrect navigation and the correct rotation of the PTZ will depend on the distance to the object, which is unknown in the general case.

For object classification, a spatiotemporal faster region-based convolutional neural network (R-CNN) is used. For each frame, the neural network outputs the possible positions of the objects with the detection confidence. The detections are aggregated over time using a statistical technique or by an additional time-recurrent layer. The network could be trained to distinguish different UAV types. The block diagram of the classification algorithm is shown in Figure 5.21.

Figure 5.22 shows SkyHunter screenshots with the classification of a UAV.

The SkyHunter system and its AI module are shown in Figure 5.23.

The described approach cardinally changes the perception on the use of EO/IR systems in C-UAV operations. First, this approach allowed unpresented optical detection performance with low-cost camera modules. For example, the typical SkyHunter detection range for DJI drones (30 cm × 30 cm) is in excess of 1.5 km, while the classification range with simple

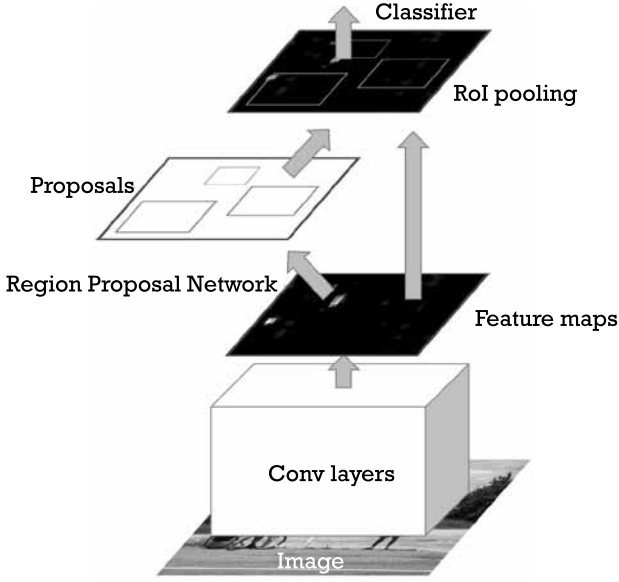

Figure 5.21 Faster R-CNN.

PTZ camera (30 times zoom) is in excess of 1 km.[6] Most importantly, when integrated with other sensors and C2 platforms, SkyHunter dramatically reduces the number of false alarms (both false-positive and false-negative) and allows automated operation without the involvement of the dedicated operator.

5.5 Acoustic Sensors

Similar to other C-UAV sensors, acoustic sensors also evolved from military developments where they were used for a long time for detecting snipers and other similar applications. In simple terms, a C-UAV acoustic sensor is an array of microphones that pick up noise generated by the propellers and motors of UAVs and then compare the received signals with signals in a database of drone acoustic signatures. The database of acoustic signatures is supported by a signal processing module that uses simple algorithms (similar to direction-finding in RF detection, as described previously) to calculate the azimuth and eventually locate the sector in which the drone is operating. Although acoustic sensors do not perform well in noisy environments

6. These parameters were correct at the time of this writing. Rinicom is constantly improving the performance of its algorithms, which results in the increases of detection and classification ranges.

Figure 5.22 SkyHunter GUI screenshot for: (a) non-UAV classification and (b) UAV classification.

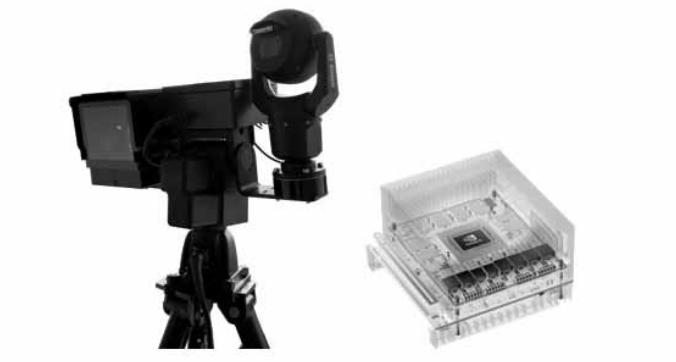

Figure 5.23 SkyHunter optical and AI modules. (We would like to express our gratitude to Rinicom Ltd. (United Kingdom) for providing material related to their patent and sharing supporting images.)

(for example, urban or airport runway), they have certain advantages, in particular when used in conjunction with other detection sensors:

- They can be very efficient in mountainous or highly urbanized areas where the terrain or obstacles (like hillsides or tall buildings) might block LOS and eventually make other sensors (radars, optical) less efficient.

- Acoustic sensors are passive and do not require any regulatory approvals as they do not interfere with other legitimate users.

As often happens in life, where our advantages are often our biggest flaws, reliance on acoustic signatures (with all the benefits explained above) is the biggest flaw of acoustic sensors, as UAVs are becoming more silent as the technology evolves. In addition, the detection range of acoustic sensors in a particularly noisy environment often is not enough for many practical C-UAV applications.

The most common type of acoustic sensors for C-UAV applications is long-range acoustic sensors [36]. They have a narrow 30° beam that can provide up to 1-km detection range with over 450m above the ground at a maximum length. Each acoustic sensor also includes a 600-cm dish that is mounted to the base station masts of standard cell antenna, making the installation of these systems challenging, especially if permission from the owner of the tower is required.

References

[1] Pottage, T., *Commercial and Recreational Drone Use in the UK*, the House of Commons Science and Technology Committee Report, 2015, p. 47.

[2] 42 Solutions, "Merlin," 2019, https://www.42solutions.nl/index.php/merlin/.

[3] 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, July 22, 2004.

[4] Air Traffic Control Association (ATCA), 2018, https://www.atca.org/uploads/National%20Security%20-%20When%20Time%20is%20of%20the%20Essence.pdf.

[5] Britannica, "Ground-Probing Radar," *Encyclopaedia Britannica*, 2010, https://www.britannica.com/technology/radar/Ground-probing-radar.

[6] Hülsmeyer, C., "Hertzian-Wave Projective and Receiving Apparatus Adapted to Indicate of Give Warning of the Presence of a Metallic Body, Such as a Ship, or a Train, in the Line of Projection of Such Wave," Patent No. 13170, applied June 10, 1904, granted September 22, 1904.

[7] Chernyak, V., *Fundamentals of Multisite Radar Systems: Multistatic Radars and Multiradar Systems*, Amsterdam, The Netherlands: Gordon and Breach Science Publishers, 1998.

[8] Wolff, C., "Frequency-Modulated Continuous-Wave Radar (FMCW Radar)," *RadarTutorialEU*, 2002, https://www.radartutorial.eu/02.basics/Frequency%20Modulated%20Continuous%20Wave%20Radar.en.html.

[9] Barton, D., et al., *Monopulse Principles and Techniques*, Norwood, MA: Artech House, 2011.

[10] Barton, D. K., "Development of the AN/FPS-16 Instrumentation Radar," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 26, No. 4, 2011, pp. B1–B16.
[11] O'Donnell, R., "Airborne Pulse Doppler Radar," *IEEE New Hampshire Public Lecture*, 2009.
[12] Kirscht, M., and C. Rinke, "3D Reconstruction of Buildings and Vegetation from Synthetic Aperture Radar (SAR) Images," *Proc. of IAPR Workshop on Machine Vision Applications*, 1998.
[13] Stimson, G., *Introduction to Airborne Radar*, 2nd ed., Raleigh, NC, SciTech Publishing, 1998.
[14] RADA Electronic Industries, "Tactical Radars for the Maneuver Force," 2019, https://www.rada.com/capabilities-3/land-radars-2.html.
[15] Aveillant, "Our Technology," 2018, http://www.aveillant.com/technology/.
[16] Thales, "Thales Completes the Acquisition of Aveillant, World Pioneer in Holographic Radar Technology," November 28, 2017, https://www.thalesgroup.com/en/worldwide/defence/press-release/thales-completes-acquisition-aveillant-world-pioneer-holographic.
[17] Robin Radar Systems, "Countering Drones at Airports: What to Keep in Mind When Evaluating Solutions," White Paper, February 5, 2019.
[18] Nguyen, P., et al., "Investigating Cost-Effective RF-Based Detection of Drones," *DroNet'16*, Singapore, June 26, 2016.
[19] Julio, "Parrot Bebop Quadcopter Review: A (Near) Flawless Drone with the Sky Controller," *FPV Drone Reviews*, February 5, 2016, https://www.youtube.com/watch?v=Vnlp2mwivsk.
[20] Edge, A., "Drone Detection: Myths and Reality," CRFS, September 23, 2019, https://www.crfs.com/blog/drone-detection-myths-and-reality/.
[21] Geier, J., "802.11 Beacons Revealed," April 17, 2003, www.web.archive.org.
[22] Piskorski, S., et al., *AR Drone Developer Guide: Parrot*, 2012.
[23] Clarke, R., "Understanding the Drone Epidemic," *Computer Law & Security Review*, Vol. 30, No. 3, 2014, pp. 230–246.
[24] Andre, T., et al., "Application-Driven Design of Aerial Communication Networks," *IEEE Communications Magazine*, Vol. 52, No. 5, 2014, pp. 129–137.
[25] DJI, "DJI AeroScope," 2018, https://www.dji.com/uk/aeroscope.
[26] Au, C., "Taiwan Develops Anti-Radiation 'Kamikaze' UAV," *Shephard News*, June 24, 2019, https://www.shephardmedia.com/news/uv-online/taiwan-develops-anti-radiation-kamikaze-uav/.
[27] Mizokami, K., "Kalashnikov Is Getting into the Business of Self-Destructing Drones," *Popular Mechanics*, February 20, 2019, https://www.popularmechanics.com/military/aviation/a26414352/kalashnikov-kub-bla-drone/.
[28] Fertig L. B., et al., "Knowledge-Aided Processing for Multipath Exploitation Radar (MER)," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 32, No. 10, 2017, pp. 24–36.
[29] Denisowski, P., *Introduction to Radio Direction Finding Methodologies*, Munich, Germany, Rohde and Schwarz, 2002.
[30] International Telecommunication Union (ITU), *Spectrum Monitoring: Handbook*, Geneva: ITU, 2011.
[31] Farlik, J., "Multispectral Detection of Commercial Unmanned Aerial Vehicles," *Sensors (Basel)*, Vol. 19, No. 17, April 2019, p. 1517.
[32] Rinicom, "Method and Apparatus for Detecting and Classifying Drones," U.K. Patent Application No. 1905256.2, 2018.

[33] Kuhn, H. W., "The Hungarian Method for the Assignment Problem," *Naval Research Logistics Quarterly*, Vol. 2, 1955, pp. 83–97.
[34] Quinlan, J. R., "Induction of Decision Trees," *Machine Learning*, Vol. 1, 1986, pp. 81–106.
[35] Santosa, F., and W. W. Symes, "Linear Inversion of Band-Limited Reflection Seismograms," *SIAM Journal on Scientific and Statistical Computing*, Vol. 7, No. 4, 1986, pp. 1307–1330.
[36] AntiDrone, "Acoustic Sensors," 2019, https://anti-drone.eu/products/acoustic-sensors/.

CHAPTER

6

Contents

Countermeasures

6.1 Introduction

C-UAV systems are developed and installed in order to provide a technological foundation for countering drones, which is a complex, multistep process involving interactions between several distinct systems and between those systems and the human operator(s) [1]. As mentioned in previous chapters, typical neutralization techniques include:

- Jamming;
- Spoofing;
- Hacking;
- Laser gun;
- High-power microwave;
- Water cannons;
- Shooting nettings;
- Interceptor drones;
- Falcons;
- Guns;
- Missile systems.

However, like UAV detection sensors, there is no single solution that will be ideal for all possible threat scenarios. Therefore, when considering the selection of a countermeasure, the following factors need to be considered:

- Disturbing communication systems in the surrounding area;
- Disturbing navigation and other electronic system in the protected area;
- Collateral damage created by the selected countermeasure;
- Range;
- Time to reload;
- Accuracy;
- Ease of use;
- Organization fit;
- Asymmetric warfare;
- Compliance with the law and regulations.

Furthermore, the selection of the most appropriate neutralization tool for specific security threat caused by a UAV is only one part of the solution. To ensure that the installed C-UAV system delivers the required levels of protection once a drone is detected, a clearly defined counter-drone neutralization chain must be established.

6.2 The C-UAV Neutralization Chain

The end users do not really need C-UAV sensors and neutralization techniques. What they really need is a comprehensive solution to ensure that the security and safety threat from rogue UAVs will be reliably mitigated if and when it happens and perpetrators are punished. Therefore, specifying requirements and procuring a C-UAV system is only the first step but certainly not the solution. As mentioned above, the solution (i.e., mitigation of security and safety threats from UAVs) is usually provided by establishing the C-UAV neutralization chain. A block diagram of this C-UAV neutralization chain is illustrated in Figure 6.1.

As follows from Figure 6.1, the chain starts with the detection and location of the UAV, utilizing sensors that are integrated in the C-UAV system. The detection could be achieved by a single sensor (for example, radar or RF detection) or multiple sensors fused together in the C2 platform. The

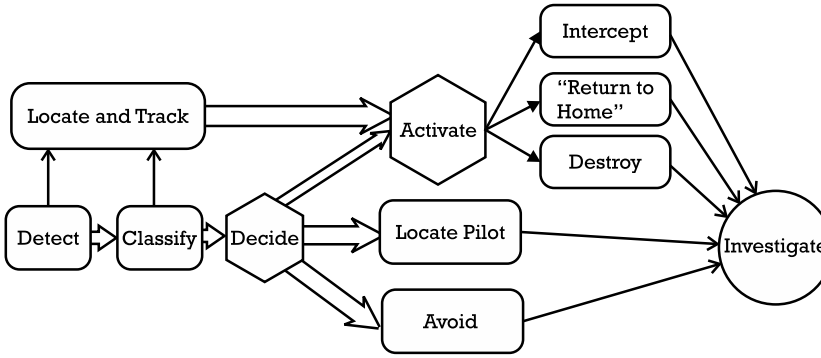

Figure 6.1 A C-UAV neutralization chain.

benefits of the multisensor comprehensive approach were explained previously, but it is important to emphasize that, as various sensors provide different information, their fusion usually produces a more comprehensive picture. For example, the RF sensor may detect the pilot while the optical sensor may help to identify if the UAV is carrying a payload. Once a UAV is detected, it needs to be classified, usually with EO/IR sensors and the embedded AI module, and as soon as a UAV is classified and identified as a rogue UAV, it needs to be tracked continuously.

Once a drone is identified as a rogue drone, an alarm is raised and a decision must be made as to how to respond to the alarm. In most of the C-UAV systems currently installed around the globe, this decision is made by a human operator who usually has a variety of options of how to respond with the help of supporting information from the C2 and situation awareness platforms. C-UAV system operators usually have a very short time to choose the most appropriate neutralization measure. For example, if the DJI INSPIRE drone is detected at around a 2-km range and is classified as a UAV at around a 1.5-km range, it could reach the object in less than 50 seconds (if traveling at a full speed of 94 km/h). As at least half of this time needs to be allocated to the activation of neutralization measures, this means that the C-UAV operator will have less than 30 seconds to make potentially life-critical decision. Furthermore, it is expected that drone velocity will be constantly increasing, building up pressure on C-UAV operators.

Typically, the C-UAV operator will choose one of the following options:

- *Activate one or a few neutralization tools:* These include jamming, spoofing, kinetic, interceptor drones, laser guns, snipers, eagles, and water cannons (the full list is given at the beginning of Section 6.1). It has to be emphasized that, particularly in civilian environments, mitigation

should be considered as a last-resort measure as C-UAV teams may have a very limited window of time to make this decision.

- *Locate the pilot and stop the flight:* This is feasible only with an RF detection sensor and usually is applied in scenarios where the drone is perceived as not dangerous or life-threatening (for example, illegally flying paparazzi or television or amateur drones trying to get exclusive pictures).
- *Do nothing with the drone:* In some cases, it will be safer to do nothing with the drone and instead focus security efforts on actions of possible targets. For example, if a yacht with celebrities on-board detects a paparazzi drone, it is easier to ask everyone just to leave the deck and put clothes on (or maybe even to take them off, depending on individual preferences and agenda) instead of trying to jam or shut off the drones, which, depending on the country of location, could create legal problems for the operators of the C-UAV system.

Let us assume that a decision is made to mitigate the drone. As follows from Figure 6.1, at this stage, the C-UAV operator has a number of options at his or her disposal:

- *Intercept:* This option includes various tools ranging from jamming to spoofing and interceptor drones with nets. It is based on neutralizing one of the key functions of the UAV, such as navigation, control and communications, propellers or engine
- *Force the UAV to return to home:* This option is usually realized with jamming or spoofing techniques. However, some modified drones could have a target location programmed such as "Home," so this option needs to be exercised cautiously and for the best effect, in conjunction with other options.
- *Destroy:* This option should be considered as the last resort and includes actions by snipers, a strong electromagnetic pulse, and water cannons.

Even though a drone is destroyed, the job of the C-UAV operator is not complete. In all cases, the drone or the remains of the drone will be landing on the ground. Depending on the neutralization technique used, this could result in a wide range of effects; there the intercepted UAV needs to be retrieved and isolated. If the drone is potentially armed, an explosive ordnance disposal team may be called in to assess and, if needed, disable the device [1]. Unarmed drones must likewise be treated with caution as they

may carry chemical or biological compounds. Furthermore, even if a UAV is not armed, its lithium-ion battery may pose a risk of combustion.

Once the drone is neutralized and safe to approach, the C-UAV operator must engage with forensic investigators, who should follow internal procedures to ensure that the integrity of the system and the potentially valuable data it carries are not compromised [1].

6.3 Neutralization Tools

The market is not short of neutralization solutions, and a very detailed analysis of the existing products was presented in [1]. Taking into account the historical perspective and current prevalence of jamming systems (both RF and GNSS) in the military domain, it is not surprising that jamming is the most common neutralization technique; 259 C-UAV systems employ some form of signal jamming as a standard feature. Jamming is the most widespread but is not the only tool available for UAV neutralization: 31 systems have a spoofing capability, 18 involve lasers, 27 employ nets, and eight take the form of a sacrificial collision drone [1]. In the rest of this chapter, we will provide an overview of the most widely used neutralization techniques.

6.3.1 Jamming

The basic concept of jamming is very simple: understand through which frequency users communicate and create a signal with significantly higher power on the same frequency that acts as a noise and significantly reduces the signal-to-noise ratio (SNR), making communication impossible. If the exact frequency not known or is changing constantly (for example, as in frequency-hopping systems), then generate a high-power signal in the whole band. While this approach may work in extreme battlefield conditions, it is not suitable for C-UAV applications:

- The continuous jamming of GNSS or control and video data link frequencies (which mainly operate in license-free SIM bands, 2.4 GHz and 5.8 GHz) will affect the performance of other legitimate devices operating in the same area, potentially creating an even higher security risk than a UAV.
- Continuous jamming in the wide band will require a significant amount of power and potentially could become a health hazard for the operators of the C-UAV system.

Therefore, jamming in the C-UAV system is realized differently, mitigating the above-mentioned drawbacks by utilizing data available from the detection sensors, as shown in Figure 6.2.

As follows from Figure 6.2, the C-UAV jamming component will be activated only when a drone is detected and classified. Then the information from the RF detection sensor or from the C-UAV drone library will be extracted to specify active data links and their exact frequencies. In parallel, the C2 platform should provide drone location and bearing so that jamming could be achieved on a multiple frequency bands and focused on a UAV with directional antenna and for a short time, minimizing the negative effect on legitimate users of the frequency band. Figure 6.3 shows the typical output from the multichannel jammer.

A good example of a jammer operating according to the described protocol is a Department of Homeland Security (DHS) jammer integrated in the RF detection system manufactured by FORTUNIO in Hungary [2]. The jammer can operator as a standalone module covering a certain area or in combination with other jammers providing full dome-jamming coverage. The specification of this jammer is shown in Table 6.1.

The jammer was evaluated by the Hungarian Radio Certification Authority, which concluded that the system is compliant with the 2013/35/EU Directive and that "beyond the distance of 20 cm from the device there are no adverse health effects from the RF exposure emitted by the DHS."[1]

A jammer integrated with the RF detection system is also produced by a Helsinki, Finland-based company Sensofusion [3]. The RF detection sensor of the system, called AIRFENCE, was described earlier. The operation algorithm is explained in Figure 6.2, and the main technical characteristics are shown in Table 6.2.

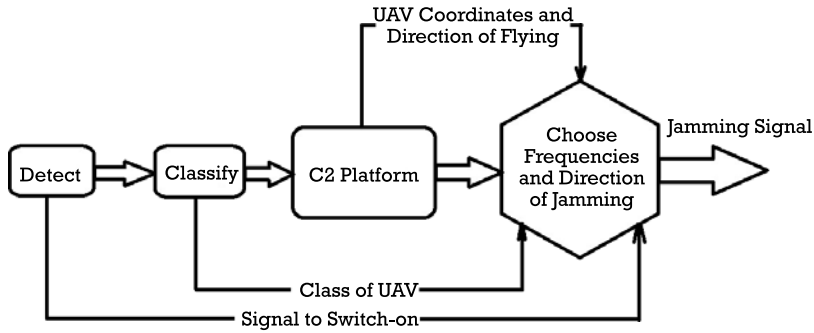

Figure 6.2 Flowchart of the operational procedure of a C-UAV jammer.

1. The authors are grateful to FORTUNIO for sharing this information.

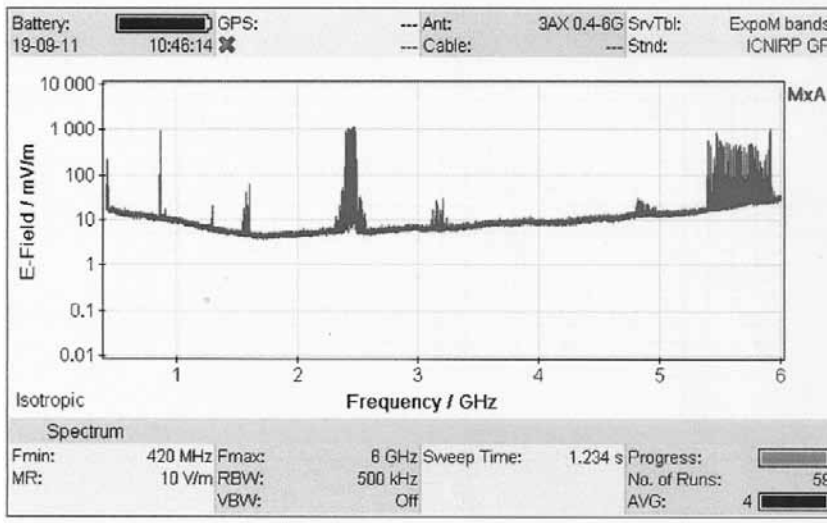

Figure 6.3 Spectral output of a multichannel RF jammer. (We would like to express our gratitude to FORTUNIO (Hungary) for providing this supporting illustration.)

Table 6.1
Specification of the RF Jammer from FORTUNIO

Parameter	Value
Size	221 × 161.5 × 30 mm
Weight	≤1 kg
Operation voltage	DC 12V to 24V
Power consumption	≤1.5A
Operating frequency bands	2,400–2,483.5 MHz, 5,725–5,875 MHz
Output power (EIRP)	2,400–2,483.5 MHz, ≤28 dBm (631 mW), 5,725–5,875 MHz, ≤28 dBm (631 mW)
Jamming type	Full dome protection

A variety of jammer options is offered by the U.K.-based Drone Defence [4]. The Paladyne E1000MP series of drone RF jammers are designed to be a backpack-mounted, man-portable, and future-proof system to disrupt the control signals, video data links, and GNSS signals on the majority of commercial drones. Once the drone is detected, the Paladyne E1000MP is activated manually or automatically, forcing UAV to perform "return to home" or land or drift harmlessly away. The Paladyne E1000MP has a total output of more than 100W and five channels that cover the most popular

Table 6.2
Main Technical Characteristics of AIRFENCE Jammer

Parameter	Value
Frequency range	300–6,000-MHz ultrawide band
Antenna type	Omnidirectional antenna for countermeasures suitable for all weather conditions; the antenna is designed for fixed and mobile installations
Weight	2,000g
Dimensions	250 mm × 65 mm (H × W), NATO standard mount
Required safety distance for personnel	1m (3 ft) from the omnidirectional antenna
Angle of radio emissions	The same from all directions when the omnidirectional antenna is in use
Security	Connection is encrypted with TLS; the TLS certificate is additionally signed with GPG

commercially available UAVs, such as the DJI and 3DR multicopters. Its operational range is up to 1 km, and the system supports both omnidirectional and narrow beam directional antennae for distributed or targeted jamming.

The SkyFence jammer uses multiple, low-powered radio transmitters that are strategically placed around the protected site [4]. SkyFence is fully programmable and can be activated via a suite of sensors or human input. It is an RF jamming system that disrupts control and GNSS signals and prevents drones from flying into a predefined protected area. The system is all-weather proven and can be configured horizontally or vertically depending on the operational requirements. For example, a "gold" deployment setup is capable of creating a 3-km safety bubble, with three to four Drone Defender teams on the ground patrolling the perimeter.

Another example of the RF jamming system is the Drone Counter Measure System integrated within the SkyArcher C-UAV system developed by ST Electronics in Singapore [5]. The SkyArcher system offers a variety of effector options to meet different requirements for any environment and operates according to the algorithms described in Figure 6.4.

The key features of the system are summarized in Table 6.3.

A very similar approach to jamming is also implemented in the SkyNet Detect system developed by the U.K.-based Kirintec Ltd. [6]. Their KT 950-186 patented system is integrated with optical sensors from Rinicom [7]. With an impressive 9-km range, the system is capable of neutralizing both single UAVs and swarms of UAVs. Available as both the man-portable and fixed systems, Table 6.4 shows the main technical characteristics [6].

The jamming module switches on when a target is detected but before it is classified as a UAV. If the classification shows "Not UAV" results, the system switches off. If the classification shows the "UAV" result, jamming stays

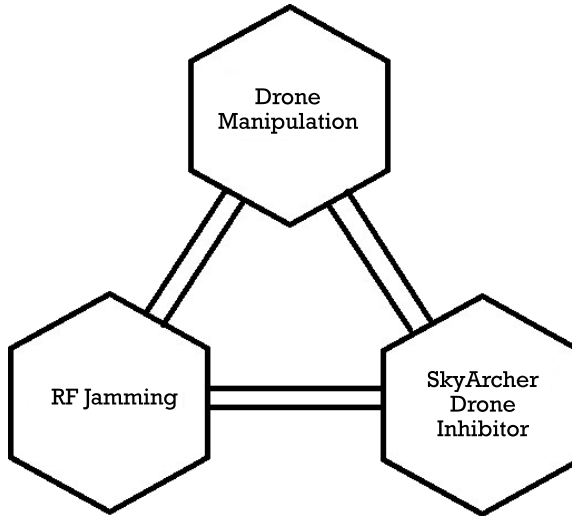

Figure 6.4 The SkyArcher neutralization algorithm.

Table 6.3
Main Technical Characteristics of SkyArcher Jammer

Parameter	Value
Frequency range	Band 1: 2.4–2.5 GHz, Band 2: 5.725–5.85 GHz, Band 3: 1.559–1.61 GHz
Effective range	300m; options for up to 2 km available
Deployment	Suitable for deployment by a single effector or a combination of effectors
Programmability	Frequency band selectable
Ambient temperature rating	0°C to 40°C
Storage temperature	–10C to 70°C
Humidity	Up to 85%, noncondensing
Compliance	Complies with IEEE C95.1-2005 (HERP)
Weight	Mechanical data gun weight 3-kg backpack, integrated battery 11 kg
Design	Ergonomically designed (suitable for left and right-handed users)

on until the target is neutralized. The system also has options for integration with RF detection and radar sensors.

6.3.2 Jamming Systems from Russia

Russia always had very strong jamming capabilities, in particular for military applications. Therefore, it is not surprising that a number of state-of-the-art

Table 6.4
The Main Technical Parameters of SkyNet

Parameter	Value
System frequency range	20 MHz–6 GHz
RF power output up	Up to 80W
Operating temperature range	–20°C to +60°
GNSS jamming	Yes
Weight	28 kg (62 lbs) excluding batteries
Environmental	IP65
Voltage in	12–35V
Programmability	Yes
Build-in self-test	Yes

solutions to combat the C-UAV problem were developed in Russia. Unfortunately, not much information is available in relations to C-UAV systems for civilian applications, as most of the publicly announced C-UAV systems in Russia are for military applications. One such a solution is a new mobile anti-drone warfare complex named the Repellent. The system is designed specifically for military applications and can suppress and destroy miniaturized enemy drones no larger than a few dozen centimeters and no heavier than a few kilograms [8].

Repellent-1 was created by engineers from the Moscow-based JSC Scientific & Technical Centre of Electronic Warfare (STC-EW) Design Bureau. The system is capable of automatically detecting and neutralizing enemy drones at distances of over 30 km (although range is impressive the size of detected drones is not specified), suppressing their control sensors via powerful jamming or through directed interference to the drones' satellite navigation systems [8].

Repellent-1 utilizes RF sensors to detect enemy drones' control signals to detect them across long distances at any time of day or night and under any weather conditions, including the extreme conditions of the Arctic. The complex is designed to operate in temperatures below –45°C with strong winds or at up to 50°C.

The Repellent-1 system is mobile, allowing it to defend advancing military units on the battlefield, as well as stationary objects such as military bases and airfields. The system is operated from a workstation in the control cabin on the back of the truck, situated next to a collapsible telescopic mast, the data from which is fed into the control cabin. The upper section of the mast contains the heart of the complex: RF detection and jamming equipment, together with a panoramic camera. On two monitors, personnel can observe the local RF environment, as well as any counter-jamming systems

that are aimed against it. Repellent-1's control cabin life support systems are designed to protect personnel from small-caliber fire, as well as chemical and biological attacks.

Another interesting anti-drone jamming system from Russia is developed specifically to mitigate MALE and HALE UAVs. The operation protocol is like the algorithm presented in Figure 6.1 but with innovative difference. First, the system detects large UAVs using a suite of detection sensors. Once the UAV is detected and classified as a foe, the UAV interceptor is launched and directed to the zone of enemy cruising and starts jamming its datalink. This allows for the neutralization of large UAVs with relatively low power at long ranges minimizing potential collateral damage to its own infrastructure.

6.4 Interceptor Drones

Interceptor drones are getting more popular as a neutralization tool for countering rogue drones. As with sensors, there is no single solution that will work in all scenarios; hence, there is a large variety of interceptor drones being introduced to the market. One such an example is the AeroSnare drone capture system introduced by Drone Defence [4]. AeroSnare is an easy-to-use, low-cost device that provides a basic drone capture capability for police and security forces who already operate their own drones. AeroSnare uses a weighted drag line that is slung underneath the interceptor drone (note that the company claims that it could be any drone, but it has been specifically designed for the Mavic and DJI M200 series).

The interceptor drone then flies over the hostile drone with a view to entangling the drone's propellers in the drag line. Once the offending drone is entangled, it stalls and falls out of the sky, and the process activates the magnetic release function in AeroSnare, which, in turn, quickly (sub-1 second) deploys a parachute, so the hostile drone descends slowly with little force (sub-69 joules for drones under 2.6 kg), allowing it to be captured and analyzed for further forensic investigation.

A novel approach to interceptor drones was released and patented by Lockheed Martin Corporation [9]. The patent relates to UAVs having a deployable net capture apparatus to enable, while in flight, the nondestructive interception and entanglement of a threat unmanned aerial vehicle. The patented net capture mechanism designed specifically for interception of nano-UAVs and micro-UAVs and is mounted on a larger UAV. The deployable net capture mechanism includes a deployable net having a cross-sectional area sized for intercepting and entangling the threat UAV, and a deployment mechanism capable of being mounted to the interceptor. The deployment mechanism includes an inflatable frame or a rod for positioning

the net in a deployed position. The system is designed as a net capture mission package, which is to be interchangeably mountable on any suitably sized and powered UAV.

One of the most advanced and efficient interceptor drone solutions is the DroneHunter system developed by Fortem Technologies Inc. from the United States [10]. DroneHunter is a military-tested UAV that provides perimeter-intrusion detection and protection by autonomously patrolling an airspace and towing away rogue drones from the sky.

The DroneHunter is equipped with Fortem TrueView radar [11], which provides detection, classification, and monitoring during the day and night and in all ground and weather conditions, including smoke, clouds, fog, and smog. DroneHunter includes an autonomous guidance system and an open command-and-control platform to detect, identify, and tow away hostile drones within a secured, geofenced perimeter. DroneHunter notifies authorized personnel of potential aerial threats in real time, and the command center ground station provides monitoring and manual intervention override options to meet situational requirements.

DroneHunter is using proprietary AI algorithms and operates autonomously. The system's Netgun captures its target and can be configured for single or multiple shots. For higher-speed targets, the system autonomously blocks fast-moving drones before they reach restricted areas or no-fly zones. Once a UAV is detected and captured in the net, DroneHunter can tether and return or safely discard the captured UAV in a safe dedicated area. The key parameters of the DroneHunter are shown in Table 6.5.

The DroneHunter system has been recognized as one of the best on the market as NATO selected DroneHunter for its terrorism defense program using counter-UAV technologies.

6.5 Lasers

Similar to jammers, laser UAV neutralization techniques have emerged from military applications and have two main advantages:

- Lasers are very precise.
- Lasers have virtually unlimited supply of ammunition providing that they are powered by adequate power source.

Laser weapon systems already work on land, in the air, and at sea, providing 360° coverage and can be scaled up or down as per mission requirements. They can be installed quickly and seamlessly on a variety of fixed

Table 6.5
Technical Characteristics of DroneHunter

Parameter	Value
Airframe	800-mm class high strength airframe weather-resistant construction
Motor	6 brushless high torque motors
Velocity	High speed 33 m/s (74 mph)
Tow capacity	High tow capacity 25 kg (55 lbs)
Navigation	Advanced autopilot utilizing Fortem-developed flight computer
Communication link	1.83-GHz control link, telemetry status, and FPV video to the SkyDome ground control, which does not use Wi-Fi frequencies
Encryption	AES-128 encrypted link, unique keys per installation
Dual net launcher	Inert gas propelled high speed at 90 mph net launch, computer-optimized autonomous net launch timing, snap-off, snap-on net cartridge system for easy reload, optional electronic tether release for secondary target acquisition
Capture range	Computer-optimized capture range between 6 ft (2m) and 25 ft (8m), 10.5 ft (3.2m) net for the capture of large intruder drones
Control	Man-in-loop override or man-in-loop manual authorize options

and mobile platforms and could be easily integrated with the overall C-UAV concept described above.

One of the first laser systems specifically developed for C-UAV applications is the Advanced Test High Energy Asset (ATHENA) syst em, which was originally designed to combat small boats, rockets, and mortars. The ATHENA system utilizes a 30-kW Accelerated Laser Demonstration Initiative (ALADIN) laser weapon. To achieve the desired maximum power, the system combines the power of three 10-kW fiber lasers into one 30-kW beam. If required, the system can also operate at 10 or 20 kW. However, only 30 kW is sufficient to ensure damage against UAVs and their fall out of the sky [12].

Recently, Raytheon announced the release of the high-energy laser weapon for C-UAV applications, which has the following features [13]:

- High survivability;
- Efficient heat removal and thermal management;
- Modular, low-maintenance design;

- Automated queuing from the full spectrum of electro-optical/infrared sensors;
- Reliability through proven manufacturing experience.

Unfortunately, very limited information is available at this stage, which is understandable taking into account the pedigree of this product.

6.6 Spoofing

A UAV is considered captured by spoofing when the third party takes control of the UAV by changing the UAV's position and velocity and the direction of movement. During postcapture control, the spoofer controls the true state of the UAV, resulting in the UAV changing its original flight plan without raising alarms [14]. On December 5, 2011, the U.S. spy Lockheed Martin RQ-170 Sentinel (UAV) was lost near the city of Kashmar in Iran. The captured UAV was shown on Iranian state television and the Iranian government announced that the UAV was brought down by its cyberwarfare unit, which commandeered the aircraft and safely landed it. The true story is still not known as Iranian television showed an essentially intact UAV while the drone was flying using encrypted military GPS, which is practically impossible to spoof. In any case, the drone was never returned, and it is highly likely that Iran produced its latest UAVs based on the captured RQ-170.

The first spoofing of the civilian UAV was demonstrated in 2012 by a research team from the University of Texas at Austin (UT-Austin) [15]. The team used a Hornet Mini UAV used extensively by law enforcement agencies in the United States. The Hornet Mini's navigation system is using civil (unencrypted) GPS and information from an altimeter, a magnetometer, and an inertial measurement unit [16]. Once the UAV was hovering 50 ft above the ground at the test site, a spoofer on a hilltop about a half-mile away was activated, sending GPS-like signals toward the UAV, aligning them with authentic signals at the UAV's GPS antenna. The power of the spoofing signal was increased gradually eventually overriding original GPS signals and taking control of the UAV. The team managed to instruct the UAV to lower its altitude and safely landed it. The results of this work were published in [14] and explained in [17], discussing both covert and overt spoofing strategies. This experiment raised serious concerns about safety of UAVs and, at the same time, stimulated a wide range of activities aiming to develop spoofing capabilities for both the civilian and military applications.

There are quite a few publications claiming successful low-cost implementation of the spoofing on the civilian UAV [18]. Interesting results are

presented in [19], which not only claims successful spoofing but defines conditions for achieving such a spoofing:

- The waypoint of the UAV is assumed to be known for experiments and assessments.
- The GPS receiver on the UAV is assumed to be known.
- Reference trajectory predefined in the flight plan is assumed to be known.

However, despite these preconditions, which are not always feasible in a real field environment, the effect of the spoofing signal on the autonomous UAV has been verified and assessed through the experimental results [19, 20].

The authors attended a couple of demonstrations where spoofing capabilities were demonstrated in the controlled laboratory environment with a priori information about the UAV that was known to the spoofers. However, at the time of this writing, we cannot name a fully working spoofing system that can operate in field conditions without a preliminary knowledge of the spoofed UAV.

6.7 Guns

Apart from the conventional guns, which will not be considered here, there are specially designed C-UAV guns. However, the range of these guns is relatively low (a few tens of meters) and they are usually considered as the last resort.

A typical example of such a gun is NetGun X1, developed by Drone Defence [4]. The NetGun X1 is a simple-to-use, cost-effective, active deterrent that allows law enforcement officers to capture unwanted drones up to 15m. The gun has two different types of capture net (Mesh Net and Spider Net), allowing the user the choice depending on the situation that is faced.

- *MeshNet* has an effective range of up to 10m and the net area is 9 m2 (3m × 3m). Its deployment time is 1 second and net velocity is 10 m/s.
- *SpiderNet* has an effective range of up to 15m and the net area is 2 m2 (1.5m radial). Its deployment time is 1 second and the net velocity is 10 m/s.

Another example of an anti-UAV gun is a SkyWall Auto gun developed by OpenWorks Engineering Ltd. in the United Kingdom [21]. SkyWall is an

autonomous system that is remotely operated and rapidly captures multiple targets in accurately delivered nets, deployed in conjunction with electronic countermeasures for a layered defense, or in environments where an electronic attack cannot be used [21]. SkyWall can be used as a standalone drone capture system or can be integrated with a drone detection and a security system to offer a highly capable and easy-to-operate counter-drone solution. A single SkyWall Auto system can protect a high-value asset or multiple systems can be networked and deployed to protect a large site.

SkyWall Auto launches a projectile up to the target drone after the system has autonomously acquired and tracked it using proprietary AI technology. The system can be permanently installed on a building or vehicle mounted for a mobile deployment. The above-described features of the system minimize the risk of any collateral damage and help to keep the UAV intact or with minimum damages, allowing forensic investigation and identification of the operator.

6.8 Effectiveness

Similar to UAV detection systems, no neutralization technique can guarantee 100% effectiveness. A number of C-UAV exercises in the United Kingdom, United States, and Europe confirmed that UAVs are "very resilient against damage" and concluded that most of the C-UAV neutralization systems need further development [1]. More specifically, every neutralization technique has its drawbacks, while almost all drone neutralization techniques can generate dangerous outcomes in certain circumstances:

- RF jamming systems are useless against UAVs flying without an active RF link and using non-GNSS navigation. Furthermore, most of the RF jammers have an effective range of a few hundred meters and require a line of sight to the UAV. In many operational scenarios, this is not sufficient, as allowing a UAV to approach to a few hundred meters could generate serious security threats. Jammers that can operate at long ranges and beyond the line of sight are, by definition, significantly more powerful, and even though they use directional jamming, they pose a high risk of interference to legitimate navigation, communication, air traffic management, and life support systems.
- All kinetic systems are not very efficient in neutralizing UAVs drones that are moving fast and/or are in unpredictable trajectory. UAVs that have their flight interrupted by kinetic systems may fall to the Earth, causing significant adverse effects. Even net-based interceptor systems with a parachute may cause significant damage if the parachute fails

to open correctly or if the interdiction occurs at low altitude. In some cases, if the net misses a UAV, it could be very dangerous to bystanders or other legitimate equipment.

- Long-range effectors such as lasers and high-powered microwaves could pose a serious threat to aircraft operating above a targeted drone [1].

Therefore, similar to the detection sensors, the most efficient neutralization could be achieved through a layered approach, when the C-UAV operator has a suite of neutralization tools available and chooses the most suitable for the particular scenario.

6.9 Legality

n most Western countries the use of C-UAV systems is regulated by national laws and regulations and in the majority of cases there is significant ambiguity concerning the operation of C-UAV systems. At the time of this writing, several international and national regulatory and legal activities were ongoing, aiming to define rules and boundaries for legal operation of C-UAV systems. However, as this needs to cover all aspects of very complex legal and regulatory challenges that involve a great number of stakeholders with different interests, this work may not be completed for some time. There are various reasons for this, but one of the main reasons is that the C-UAV technologies are subject to numerous overlapping laws that were drafted to address other challenges, long before the C-UAV appeared [1]. Adding to this ambiguity is the fact that different agencies are moving with different speeds as airspace regulators are the most active, while other government agencies are still discussing foundations for the comprehensive C-UAV policies. As mentioned above, in most Western countries, the use of the C-UAV systems is either illegal or questionable and is based on individual permissions given to certain authorities rather than regulated by the legal framework.

In the United Kingdom, intercepting, shutting down, or countering a UAV in any way is considered as a violation of provisions in the Aviation Security Act and the Criminal Damage Act. Correspondingly, jamming a drone is likely to be considered a violation of the Wireless Telegraphy Act 2006, which has a purpose to "consolidate enactments about wireless telegraphy." In addition, jamming also violates the Electromagnetic Compatibility Regulations. To make things more complicated, laser-based UAV neutralization systems most likely will be violating the 2016 Air Navigation Order.

Similar and sometimes even more complex situation is in the United States, where the Wiretap Act forbids the interception of electronic communications. This means that not only all UAV jamming systems violate this act but even simple RF detection systems that only detect and track a drone by using information from its communication links might violate this law [22], while spoofing systems may contravene the Computer Fraud and Abuse Act [23]. Currently, UAVs are classified as aircraft, all UAV neutralization techniques also violate the U.S. Aircraft Sabotage Act, which imposes heavy fines and even prison sentences for setting fire, damaging, destroying, disabling, or wrecking any aircraft in U.S. airspace [24].

An intermediate solution to the use of C-UAV systems has been found in the United States by granting special authority to mitigate drones to the Department of Defense, the Department of Energy, the Department of Justice, and the Department of Homeland Security [25]. There are ongoing discussions regarding extension of this authority to other federal and regional agencies, but no timeline has been provided yet.

Certain common detection systems may also not always be legal [26]. The Federal Aviation Administration (FAA) has stated, as recently as May 2019, that it "cannot confirm the legality of any UAS detection system." For example, certain types of radar could, according to the FAA, "require Federal Communications Commission (FCC) or National Telecommunications and Information Administration (NTIA) authorization and interagency coordination," and the use of any type of detection system at any U.S. airport could implicate various sections of the U.S. Code and a number of FAA orders [27].

In Europe, C-UAS sensors that collect personally identifiable information may implicate the General Data Protection Regulation (GDPR) [28]. To address these and other issues, the project ALADDIN (Advanced hoListic Adverse Drone Detection, Identification and Neutralisation) was initiated by the European Commission (EC) through the Horizon 2020 research and innovation program [30]. The aim of ALADDIN was to assess relevant C-UAV technologies, threat trends, regulations, and other societal, ethical, and legal issues to improve the law enforcement agencies' capabilities in mitigating the rogue UAVs threat. An analysis of the legal implications of the C-UAS in Europe was presented in a number of deliverables that are publicly available in [30–33].

References

[1] Michel, A. H., *Counter-Drones Systems*, 2nd ed., Report from the Center of the Study of the Drone at Bard College, December 2019.

[2] FORTUNIO, 2019, http://fortunio.hu/.

[3] Sensofusion, 2019, https://www.sensofusion.com.

[4] Drone Defence, 2018, https://www.dronedefence.co.uk/.

[5] ST Engineering, "SkyArcher Counter Drone System," Singapore, 2014.

[6] Kirintec, 2018, https://www.kirintec.com/.

[7] Rinicom, 2019, https://rinicom.com/.

[8] "Tiny Spy Drones No Match for Russia's 'Repellent-1' Mobile Anti-Drone Complex," *Sputnik International*, December 29, 2016. https://sputniknews.com/military/201612291049110110-repellent-anti-drone-complex-development/.

[9] Lockheed Martin, "Unmanned Aerial Vehicle (UAV) Having a Deployable Net for Capture of Threat UAVs," U.S. Patent No. 9896221, July 2015.

[10] Fortem Technologies, "The DroneHunter," 2019, https://fortemtech.com/products/dronehunter/.

[11] Fortem Technologies, "TrueView Radar," 2019, https://fortemtech.com/products/trueview-radar/.

[12] Keller, J., "Air Force Shows Counter-UAV Laser Weapons Based on Fiber Lasers That Can Defeat Threat of Drone Swarms," *Military & Aerospace Electronics*, November 19, 2019, https://www.militaryaerospace.com/unmanned/article/14072287/laser-weapons-counteruav-fiber-lasers.

[13] Raytheon, "Counter-UAS," 2019, https://www.raytheon.com/capabilities/products/counter-uas.

[14] Kerns, A. J., et al., "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, July 2014.

[15] "Researchers Use Spoofing to 'Hack' into a Flying Drone," *BBC News*, June 29, 2012, https://www.bbc.co.uk/news/technology-18643134.

[16] "UAVs Vulnerable to Civil GPS Spoofing," *Inside GNSS*, July 16, 2012, https://insidegnss.com/uavs-vulnerable-to-civil-gps-spoofing/

[17] SPOOF, 2012, https://www.youtube.com/watch?v=6qQXVUze8oE/.

[18] Huang, L., and Q. Yang, "Low-Cost GPS Simulator – GPS Spoofing by SDR," *DEFCON 23*, August 2015.

[19] Seo, S. -H., et al., "Effect of Spoofing on Unmanned Aerial Vehicle Using Counterfeited GPS Signal," *Journal of Positioning Navigation and Timing*, Vol. 4, No. 2, June 2015, pp. 57–65.

[20] Guo, Y., et al., "Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation," *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 7, July 2019.

[21] OpenWorks Engineering, "SkyWall Auto," 2018, https://openworksengineering.com/skywall-auto/.

[22] U.S. Congress, "National Defense Authorization Act for Fiscal Year 2018," Section 1602, 115th Congress, 2018, https://fas.org/sgp/news/2017/06/dod-uas.pdf.

[23] "Computer Fraud and Abuse Act (CFAA)," Internet Law Treatise, 2009, https://ilt.eff.org/Computer_Fraud_and_Abuse_Act_(CFAA).html

[24] U.S. Congress, "S.2623 - Aircraft Sabotage Act," 98th Congress, 1984, https://www.congress.gov/bill/98th-congress/senate-bill/2623.

[25] "Blue Ribbon Task Force on UAS Mitigation at Airports Final Report," Blue Ribbon Task Force on UAS Mitigation at Airports, October 2019, https://uas-mitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf.

[26] Dermody, J. R., "Letter from John R. Dermody, P.E., Director, Office of Airport Safety and Standards," U.S. Federal Aviation Administration, July 19, 2018, https://web.archive.org/web/20190110160243/https://www.faa.gov/airports/airport_safety/media/counter-uas-airport-sponsor-letter-july-2018.pdf.

[27] Dermody, J. R., "Letter from John R. Dermody, P.E., Director, Office of Airport Safety and Standards," U.S. Federal Aviation Administration, May 7, 2019, https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf.

[28] Sarma, D., and P. Quinn, "D3.1 – Data Protection, Social, Ethical and Legal Frameworks: Advanced hoListic Adverse Drone Detection, Identification Neutralisation Program, Diginext," February 2018, http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN_D3.1_DataProtectionSoEL_Framework_V1_0_PU.pdf.

[29] ALADDIN, "Project," 2017, https://aladdin2020.eu/project/.

[30] "D3.1 – Data Protection, Social, Ethical and Legal Frameworks," 2017.

[31] "D3.1 – Data Protection, Social, Ethical and Legal Frameworks," 2018.

[32] "D3.1 – Data Protection, Social, Ethical and Legal Frameworks," 2019.

[33] Rupprecht, J., "7 Big Problems with Counter Drone Technology (Drone Jammers, Anti Drone Guns, etc.)," Rupprecht Law, P.A., 2018, https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems.

CHAPTER

7

Contents

Standardization and Regulatory Activities on C-UAV Systems

At the time of this writing, no international standards existed describing the appropriate design and use of C-UAV systems. A wide variety of C-UAV products currently available on the market is relatively new, and many of the products, including those mentioned in this book, have not yet had time to mature. The security threats caused by rogue UAVs had have the highest impact on military and on the aviation industry so far. Therefore, it is not surprising that military and aviation industries initiated relevant standardization activities, aiming to harmonize existing solutions and to develop the most appropriate C-UAV system for different scenarios.

7.1 C-UAV Standardization by NATO and EDA

Both the North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA) have long recognized threats from rogue UAVs and have initiated a number of activities to regulate and mitigate these threats. Both organizations, due to their nature, although different, contribute to air superiority in the case of military incidents and produced their respective priority plans. A brief outline of these plans is presented in this chapter.

The EDA has produced the state of play for Anti-access and Area Denial (A2AD) for rogue UAVs [1].[1] This plan emphasizes that the development of a minimum level of protection of European Union (EU) armed forces against mini-UAVs threats is a major short-term challenge and recommends the following way forward:

- Coordinate and exchange information on the national C-UAV capabilities and plans.
- Importantly, develop standards for C-UAV capabilities.

For medium-term activities, the EDA formulated the challenge of systematic deployment of a high-level protection of deployed European armed forces against mini UAVs threats and recommended the following ways forward:

- Establish user groups for existing C-UAVs operated by several member states.
- Jointly develop the European C-UAV systems based on harmonized requirements.

The long-term challenge is identified as continuously adapting member states' C-UAVs capabilities to the quickly changing capabilities of mini-UAVs and their potential malicious use within an operational environment always more dependent on the electromagnetic spectrum. The EDA also recommended that, to address this challenge, member states should coordinate the development of relevant technologies to cope with the evolution of the mini-UAVs threats to the armed forces.

1. We are grateful for the insights provided by Dion Polman (from the European Defence Agency) during a presentation on EDA-C-UAS activities.

While formulating these challenges, the EDA welcomed the announced inclusion of a category dedicated to the C-UAS within the European Defence Industrial Development Programme (EDIDP) [2]. However, the EDA also emphasized that all future C-UAV systems must have civilian-military dual-use capability and produce a minimum adverse impact on other systems, including other defense systems, mobile phones, or even heart pacemakers.

At the time of this writing, the NATO Standardization Committee was planning its C-UAV standardization activities, which will be focused into two areas: operational and technical.

Activities within the operational scope will be focused on the definition of a doctrine and the development of the C-UAV concept of operation (CONOPS), providing recommendations for interoperability between allied forces and other relevant activities.

Activities within technical scope are divided into several parallel and correlated activities, such as:

- Establish a NATO C-UAV Standardization Subgroup open to industry, which would aim to select or create appropriate standards.
- Demonstrate compliance with these standards through a Technical Interoperability Exercise coordinated by the NATO Communications and Information Agency (NCIA). The final aim would be to set up a 2-week exercise in 2021 in a laboratory environment, in which data sharing and interoperability will be tested in a number of scenarios.

The initial focus of the standardization subgroup will be on three main areas:

- *Architecture:* It is recognized that a distributed architecture would be the ultimate solution for a comprehensive C-UAV solution; in this scenario, special attention should be focused on sensor fusion and resource management.
- *Intra C-UAS system interfaces:* This is the definition of standard interface control documents (ICDs) between sensors, command and control, and effectors.
- *Integration of the C-UAS system with other systems:* This is the definition of standard ICDs to communicate both with other C-UAS systems, in a mesh architecture, and with other systems (i.e., ground-based air defense (GBAD)).

7.2 Standardization in EUROCAE and RTCA[2]

In aviation, Air Navigation Service Providers (ANSPs) are responsible for providing safe, secure, and efficient management of airspace assigned to a particular ANSP. These include [3].[3]

- Preventing collision between aircraft;
- Providing advice on the safe and efficient conduct of flights;
- Conducting and maintaining an orderly flow of air traffic;
- Notifying the concerned organization and assisting in search and rescue operations.

Romek [3] and Lele and Mishra [4] emphasized that UAV activities in civilian air space could lead to the both security and safety threats. More specifically, UAVs' unlawful interference with airport infrastructure is considered as a security threat while UAVs' threats to air traffic in the landing and take-off areas are considered as safety threats. This classification is important from an operational point of view and should be incorporated into the operational procedure of the C-UAVs' systems installed to protect the civilian airspace.

In [3], it was recommended to define a 3-mile zone from the end of the runway as the critical area that needs to be protected by the installed C-UAV systems. The reasons for choosing the 3-mile range are as following:

- In this area, aircraft fly at the slowest speed.
- In this area, aircraft fly low and within reach of many commercially available UAVs.
- In this area, aircraft have limited maneuverability.
- In this area, aircraft are always at the same point each time that they approach the runway, making it easier to attack.

Therefore, considering the roles and responsibilities of ANSPs, Romek [3] also recommended that ANSPs should take additional responsibilities for:

2. We would like to express our gratitude to Alain Vallée from EUROCAE (France) for providing this material.
3. We would like to express our gratitude to Czeslaw Romek from Polish Air Navigation Services Agency for sharing this material.

- Checking and advising on technical specifications of active C-UAV systems, ensuring compatibility with the existing legacy communication, navigation, and surveillance (CNS) systems;
- Developing and implementing procedures with the operator of the C-UAV system when a UAV is detected.

In recognition of the growing threat to the aviation industry from the UAVs and in response to several high-profile cases when rogue drones caused significant monetary and reputation damages to the biggest airports in the world, the aviation industry initiated standardization activities to ensure that the aviation industry in general and airports in particular are prepared to address safety and security threats caused by UAVs. The importance of having a consolidated and regulated approach to the C-UAV challenge in aviation is emphasized by the International Air Traffic Association (IATA). It was shown in [5] that, in addition to safety and security threats, rogue UAVs flying in civilian airspace create sufficient financial damages.[4] For example, on May 9, 2019, a drone sighting in the vicinity of Frankfurt Airport resulted in 135 flights being canceled, 42 flights being diverted, and many flights being delayed, with an estimated cost of €1,000 per minute. A drone sighting at Gatwick Airport in December 2018 led to the cancellation of more than 1,000 flights, resulting in a total cost of approximately €64 million.

When it comes to security threats from UAVs, the presentation [5] emphasized that, according to the regulations, airport security is the task of airport managers or owners or national authorities, not the ANSP. Therefore, these stakeholders must have legal, technical, and financial tools specifically customized to these tasks. While emphasizing that the C-UAV systems being used for the protection of military and critical infrastructure sites (naval bases, nuclear power plants, government buildings) also could be used in airports providing that they are compatible with legacy systems, [5] stated without any ambiguity that, very importantly, RF jamming and shooting down countermeasures are not allowed in airports. To address the problem, [5] recommended joint standardization activities to be managed between the major aviation standardization bodies such as EUROCAE (European Organisation for Civil Aviation Electronics) and Radio Technical Commission for Aeronautics (RTCA).

In January 2019, the RTCA in the United States was requested by the U.S. government agencies to form a committee aiming to develop standards for Counter-UAV, with emphasis on UAV detection. RTCA immediately

4. We are grateful to Manfred Mohr, from the International Air Traffic Association (IATA), for sharing this information.

began consultations with its members and the U.S. government and, in June 2019, met with various stakeholders and identified the scope and timeline of the new standard. The new group, called the Counter UAS Special Committee SC-238, was established. In December 2019, RTCA approved the formation of the SC-238 and call for participation sent to all interested stakeholders. At the time of this writing SC-238 had a number of working meetings despite COVID-19 situation and first draft was sent to RTCA members for comments. For more details, readers should see the RTCA website [6].

In parallel, RTCA engaged with EUROCAE, aiming to harmonize U.S. and European standardization activities. Both the RTCA and EUROCAE emphasized the increased frequency of sightings of unauthorized UAVs in both civilian and military airspace and acknowledged disruptions of airport operations with significant economic losses. This has a negative impact on the safety and security of the air transportation system and airspace around airports or any type of airspace that needs to be protected. It was agreed that the standardized C-UAV system should provide:

- Detection and reporting of any unauthorized UAV activity, at the earliest possible stage;
- Neutralization or disruption of UAV component(s), in accordance with national regulations.

As a result, in November 2019, a joint EUROCAE/RTCA standardization committee, called Working Group 115 (WG-115), was established. The aim of WG-115 is to develop standards to support the safe and harmonized implementation of counter-UAV systems into airport and air navigation service provider (ANSP) systems.

The scope of the WG-115 is limited to surveillance, interoperability, and interfaces with stakeholders involved in the C-UAV domain: ANSP, airports, U-space service providers, surveillance systems manufacturers, law enforcement agency (LEA), and pilots. More specifically, WG-115 focus is on the detection and surveillance capabilities around the airfield, but C-UAV system should be capable to be extended to operations in other environments, such as urban areas. The initial system configuration for developing the standard is shown in Figure 7.1.

The scope of WG-115 activities does not include the topic of cooperative target detection, but interaction with information from cooperative sensors will be included in the overall system assessment. In addition, the interoperability of the neutralization capabilities with the airport and ANSP systems will be addressed.

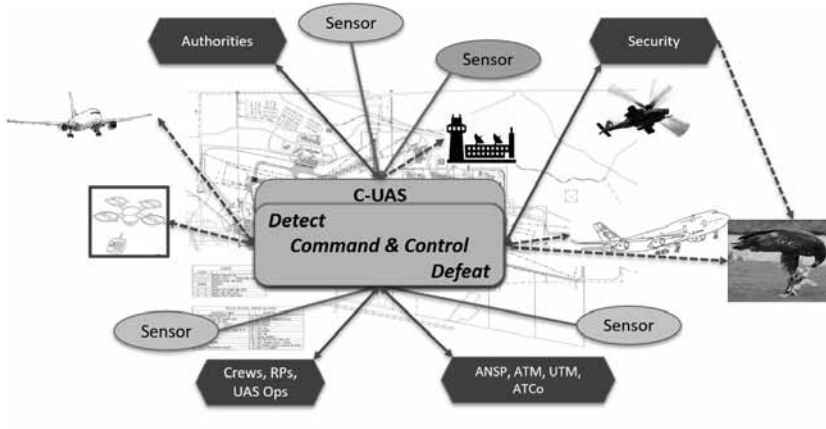

Figure 7.1 The proposed C-UAV system configuration in the EUROCAE WG-115 standard.

In December 2019, the kickoff meeting of WG-115 was held in Paris, where participants agreed that the focus of further action would be around the following main areas:

- Define the requirements' specification for counter-drone measures, including operational procedures and technical solutions that are interoperable and compatible with the existing infrastructure.
- Clarify the confusion about the actual scope of the UAV neutralization and provide a comprehensive description of the challenge that will permit requirement specifications for countermeasures to be developed.
- Encourage a close dialogue between authorities and the developers of countermeasures aiming to meet end users' performance requirements.
- Exchange good practice and experiences across sectors and continents, covering areas such as legislation, setting of standards, testing of different solutions, and operational routines or practice.

The EUROCAE WG-115 issued the Operational Services and Environment Definition (OSED) document, which provides the basis for assessing and establishing operational, performance, and interoperability requirements for the counter-UAV systems integrated into airports and ANSP systems. The scope is limited to surveillance, interoperability, and interfaces with stakeholders involved in the C-UAS domain, with focus on detection

and surveillance capabilities around the airfield, considering also interoperability of defeat capabilities with the airport and the ANSP systems. The WG-115 was scheduled to produce the first draft of the standard after this book will be published, so the interested reader should go to the EUROCAE website for more details [7].

7.3 Conclusions

In this part, we described various challenges of C-UAV systems, emphasizing that an effective solution of the C-UAV problem requires a complex approach, covering counter-drone technology as well as safety, practicality, policy, and legality. We show that there is no single sensor solution that will perform well in all scenarios and emphasize that every detection sensor has its drawbacks. For example:

- Radars struggle to detect nano-UAVs, micro-UAVs, and mini-UAVs, especially if they are flying at a low altitude.
- EO/IR sensors struggle in adverse weather with low visibility and NLOS.
- RF detection sensors do not perform efficiently in an urban environment with a high level of radio interference or when drones fly in the automatic mode.
- Acoustic sensors have a limited range and require significant planning for installation, while their efficiency is reduced with quitter drones being introduced to the market.

Table 7.1 provides detailed summary of advantages and drawbacks of all types of sensors considered in this chapter and illustrates the benefits for integrated approach.

We emphasize that, in order to ensure efficient operation, the developed C-UAV system must include classification of UAVs, operate in the automatic mode, and generate low levels of false-negatives and false-positives. This is achievable only with the incorporation of advance AI and ML learning algorithms, which allow a significant reduction of the operational costs of C-UAV systems.

We also show that almost all drone neutralization techniques can be dangerous or illegal in certain circumstances; therefore, the selection of the most appropriate countermeasures must be made quickly, taking into account various factors, such as potential collateral damage, legislation, or impact of not taking any neutralization measures.

Table 7.1
Detection Capabilities of Various Sensors

Application/Sensor	Radar	EO/IR	RF Detection	Acoustic	Integrated System
Detection	👍	👍	👍	👍	👍
Tracking and Location	👍	👍	👍	👎	👍
Identification	👎	👍	👎	👎	👍
Distance Range	👍	👎	👍	👎	👍
Autonomous Target	👍	👍	👎	👎	👍
Hovering Target	👎	👍	👍	👍	👍
Environmental and Congested Spectrum	👍	👎	👎	👎	👍
Need for a Dedicated Operator	👎	👍	👎	👎	👍

Like detection systems, no interdiction system is 100% effective and all neutralization systems have specific drawbacks [8]:

- RF jamming systems have no effect against drones that operate without an active RF link.
- Many signal jammers have a limited effective range of a few hundred meters, meaning that the system must be very close to the intruding drone to successfully mitigate it, and are not effective without a direct line of sight to the drone. Jammers that are capable of operating at long ranges and beyond the line of sight must be significantly more powerful, but more powerful jammers also pose a higher risk of interference to legitimate communications.
- All kinetic systems may struggle against drones that are moving quickly or in unpredictable patterns. (When they do work as intended, they may destroy components of the drone that are necessary for forensic investigations.)
- Spoofing systems, meanwhile, are technically very difficult to build and implement, while their efficient use today requires a priori knowledge of drone details. Therefore, spoofing systems may not be universally effective against all types of drones. A UAV with encrypted

navigation or communication links, for example, could be resistant to spoofing attacks.

References

[1] Pullman, D., "European Defence Agency," *Drone Intrusion and Surveillance Conference*, Brussels, October 3–4, 2019.

[2] European Commission, "2019 Calls for Proposal: European Defence Industrial Development Programme (EDIDP)," March 19, 2019, https://ec.europa.eu/growth/content/2019-calls-proposals-european-defence-industrial-development-programme-edidp_en.

[3] Romek, C., "Airport Airspace Protection," *Drone Intrusion and Surveillance Conference*, Brussels, October 3–4, 2019.

[4] Lele, A., and A. Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles. *Journal of Defence Studies*, Vol. 3, No. 3, July 2009, pp. 54–65.

[5] Mohr, M., "The Unique Challenges of Countering Drones at Airports: To Protect Our Passengers, Crew and Aircraft and How It Will Be Financed?" *Drone Intrusion and Surveillance Conference*, Brussels, October 3–4, 2019.

[6] RTCA, 2019, https://www.rtca.org/.

[7] EUROCAE, 2019, https://eurocae.net/.

[8] Michel, A. H., *Counter-Drones Systems, 2nd ed.*, Report from the Center of the Study of the Drone at Bard College, December 2019.

CHAPTER

8

Contents

A Strategic Approach to Counter Rogue Drone Threats

8.1 Introduction

UAVs have been commercially available for decades, but until lately, the unique challenges of operating aircraft remotely have meant that there have been relatively few users of such systems outside of specialist military operators and skilled model aircraft pilots. Advances in key technologies now mean that, in recent years, remotely piloted aircraft have become increasingly available, increasingly capable, and increasingly easy to use [1]. The proliferation of the commercial use of drones has created a new, innovative, and exciting addition to the aviation industry with boundless possibilities. Inevitably, this technology comes with risks. Careless and inconsiderate drone users can cause a nuisance and pose a safety risk to others. Ignorance is not an excuse, but the reckless use of drones raises concerns for citizens' privacy and public safety. There are also those who would more deliberately use drones for criminal acts, whether that is to facilitate organized

crime, to disrupt national infrastructure, or to commit acts of terrorism. Major incidents involving the malicious use of drones has highlighted that tackling hostile drone threats is a real challenge. Governments across the world are seeking ways to reduce the likelihood of such incidents, as well as amplifying their ability to respond should further incidents occur.

It is clear that the scale of the challenge in preventing rogue drone incursions and malevolent attacks is much wider than any one government department. There is clear international consensus that there is no technological silver bullet suitable for use against all drones under all circumstances, and as drone technology advances, the nature of the threat will change [1]. Tackling malicious drone use requires a comprehensive and layered strategic approach to be put in place by government and implemented across the full local, regional, and national apparatus of the state. This strategic approach must blend technological innovation with legislation, regulation, and education. Developing counter-drone solutions will not solely reside in one nation; it is a global phenomenon requiring greater collaboration, including the sharing of knowledge, expertise, and best practices. It is also a problem that cannot be solved by authorities alone; at-risk sectors within private industry must now increasingly consider their vulnerability to malicious drone use and how they should best mitigate it safely and legally. Technological countermeasures will need to coevolve with drones and within the legal and regulatory frameworks that govern their use.

Some governments have recognized the scale of threat vectors from contemporary drones, developing a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones. This recognition is now turning into positive state action, taking a full-spectrum approach to deter, detect, and disrupt the misuse of drones, which acknowledges the need to build strong relationships with industry to ensure that their products and services meet the highest security standards. Moreover, as demonstrated during the global COVID-19 pandemic, governments are empowering their police and other operational responders to enforce the law through access to counter-drone capabilities and legislation. Lessons from the police use of drones during the pandemic reinforced the need for public dialogue about the police and wider proliferation of drone use in society, addressing the privacy and surveillance concerns of citizens' fundamental rights. Governments need to strike a balance between ensuring that a robust security posture is in operation to keep citizens and their economy safe, while recognizing the benefits of the legal uses of drones and allow themselves to reap the fullest rewards of incorporating drone technology into society that is accepting of the sudden changes. This chapter will therefore focus upon the challenges to secure society's acceptance of increasing drone use. It will also examine the key considerations for creating an

effective counter-drone strategy and the practical guidance to ensure the successful implementation of counter-drone policies, practices, and procedures. Finally, this chapter will explore the international dimensions of UAV regulation, legislation, and enforcement, alongside the requirements for training and continued research, innovation, and development in the C-UAS domain.

8.2 Social Acceptance

The continued proliferation of drone use increasingly depends upon society's acceptance of this disruptive technology. Industry forecasts anticipating the exponential global growth of the drone market are not guaranteed, despite the wealth of positive benefits that UAVs are bringing and will continue to bring to both public and private sectors. The case to darken the skies of our towns, cities, and urban areas with thousands of buzzing drones delivering parcels and increasing the footprint of state surveillance has yet to convince all citizens, community groups, and civil rights campaigners that this is entirely a good idea. Government policymakers and drone industry aerospace professionals must not underestimate the deep-rooted invasions of privacy that some private citizens feel when a drone is sighted near or above their property. In July 2015, William Merideth, aged 47, went outside to investigate at his home in rural Bullitt County, south of Louisville, Kentucky, in the United States, following reports from his children that they had seen a drone while they were playing in the backyard [2]. When the drone turned and flew back over his property, Merideth admitted to grabbing his shotgun and firing into the air, sending the $2,500 camera-equipped machinery to the ground [2]. The DJI Phantom 3 drone shot down by Merideth belonged to his neighbor, who filed a complaint to police, leading to Merideth's arrest and felony charges. Dubbed the "drone slayer" by the media, Merideth denied the charges insisting that he had every right to protect his property [3]. Merideth stated [2]: "I had no way of knowing if it was a predator looking at my children. I was completely justified in protecting my family." After reviewing testimony in court in October 2015, Judge Rebecca Ward ruled that Merideth was right to protect his family and property, stating [3]: "I think it's credible testimony that this drone was hovering for two or three times over these people's property, that was an invasion of their privacy and they had the right to shoot this drone. I'm going to dismiss this charge." The "drone slayer" case highlighted the unsatisfactory legal territory that surrounds the use of drones near private property and provided an example of the actions citizens will take to protect their privacy from what they believe is a rogue drone incursion and breach of their most fundamental human right.

The British government's Department for Transport and Ministry of Defence commissioned research during 2016 to open public dialogue on the use of drones in the United Kingdom. It explored the public's understanding of drones, attitudes towards current usage, and public expectations, aspirations, and concerns about future usage. Experts and stakeholders, including drone operators, aviation authorities, and academics, also participated in the dialogues to listen to and support informed debate. The results of the research provided a rich source of evidence-based data, providing information upon which to build the foundations of a framework for future drone use. At the start of the dialogue, participants on the whole had low awareness and knowledge of drones, with military drones and high street toys being the main types of which the participants were aware. Participants often had little or no knowledge of commercial applications and high-level associations with drones tended to be somewhat negative, linked to concerns about privacy and surveillance, safety and misuse, and fear of the unknown [4]. Different attitudes emerged towards different groups of potential drone users. The general public were seen as the highest-risk group and most likely to cause accidents and incidents when operating drones, due to low awareness of regulations, lack of training, and the growing accessibility of drone technology. Participants were particularly concerned about children and teenagers who were expected to be less likely to read instructions and more likely to take risks and use drones unsafely. By the end of the dialogue, four key public priorities emerged with relative consistency, illustrated in Table 8.1.

The findings of the study largely reflected the broad outcomes of similar consultations and research conducted by public authorities and academia. The public participants in the U.K. study suggested four common strategies that could be used across the areas to mitigate their concerns, which are described in Table 8.2.

Recognizing the pace of change in the drone industry, participants of the U.K. study ultimately wanted greater controls on public access to the introduction of drone technology, believing that this would be an important first step in reducing risk and future-proofing drone policy. However, the sudden size, scale, and scope of the global coronavirus pandemic during 2020 brought the social acceptance of drones in society to the forefront, testing governments' ability to delicately balance the provision of safety and security to the public while preserving citizen privacy, civil liberties, and fundamental human rights. To enforce new emergency powers for public gatherings, social distancing curfews, and quarantine rules, police forces across the world utilized specially modified drones to prevent the rise of COVID-19 infections. Learning from police strategies in other jurisdictions to effectively manage public lockdowns, police forces adopted the

Table 8.1
Public Priorities for the Use of Drones in the United Kingdom

Public Priority	Description of Public Concern
Anonymity and traceability	Participants were worried about the current difficulty of identifying the user if they encountered a drone or a negative incident occurred. Participants were also concerned about not knowing the purpose of a flight or how any data collected would be used. This led to concerns about accountability for accidents and enforcement of regulations.
Safe use by operators	Participants were concerned by injuries caused by drones crashing or falling from height, accentuated by the perceived difficulty of flying them, and the fact that public users were unlikely to have had training.
Quality of materials	Participants expressed safety concerns that were often in part driven by anxieties about the potential for subpar safety standards; in particular, participants worried about whether quality of materials would be sufficient to avoid preventable injury or accidents (e.g., in relation to inexpensive, smaller, imported drones, homemade machines built by hobbyists, and the eventuality that drones become outdated in terms of safety mechanisms or overall quality such as battery life).
Misuse of drones	Participants were particularly concerned about hacking, terrorism, stalking, and surveillance from the start of the dialogue process; participants often acknowledged that many forms of technology can be misused and that these were not necessarily drone-specific issues.

Source: [4].

use of their drones as part of a new tactical menu of options. At the beginning of the public lockdown measures in the United Kingdom in March 2020, Northamptonshire Police Chief Constable Nick Adderley said that he planned to increase the force's number of drones from two to eight as using drones would be a "cost-effective way" to pass on information to the public [5]. The drones would be equipped with speakers in order for them to transmit messages, providing health warning updates and enforcing new emergency police powers [5]. The decision in the United Kingdom to use drones to prevent the spread of COVID-19 followed the use of police drones in China, Spain, Belgium, and France. Local police in Italy were also permitted to use drones to monitor the movements of citizens, the Italian Civil Aviation Authority (ENAC) confirming their approval of the tactic after receiving requests for additional support from local police units who were struggling to monitor the movement of citizens on lockdown by traditional police use of CCTV, roadblocks, checkpoints, and increased high-visibility patrols [6].

In the United States, the Chula Vista Police Department in California also used drones equipped with cameras and loudspeakers to monitor the coronavirus shutdown, doubling its fleet of drones with new specifications to include night-vision cameras [7]. Spencer Gore, the chief executive of U.S.-based drone company Impossible Aerospace, said he was "working like

Table 8.2
Strategies to Address Public Priorities for the Use of Drones in the United Kingdom

Registration	Participants thought this would be a key starting point to address numerous concerns, notably anonymity, and enable users to be traced and held accountable and liable when things go wrong. The act of registration itself was also perceived to encourage more responsible behavior. However, participants acknowledged that registration alone may not enable someone to identify a user in the moment and set experts the challenge of finding solutions to this. The dialogue process also gave space for participants to consider the feasibility of this idea; despite potential barriers, they felt that sit was an important area for investment.
Mandatory Training	Participants suggested that mandatory training, particularly of public users, was seen as a potential avenue to reduce the likelihood of accidents if users were more aware of regulations and how to use their equipment safely. Participants suggested minimum requirements for public users such as online training at registration. They expected that more significant training would be required for commercial operators or anyone using heavier, more sophisticated drones.
Technological Solutions	Participants cited technology as a way to address safety concerns, particularly by the public and near airports. These included enforcing minimum safety standards, which would include safety features built into drones, notably blade covers and geo-fencing capabilities.
Education	Education and raising awareness were strategies commonly suggested across the areas by many participants to address unsafe use by making users more aware of regulations. This could also reassure the wider public by making them aware of drones and their capabilities and when and how to report incidents.

Source: [4].

crazy" to help equip law enforcement agencies across the United States with specialized drones [7].

However, not all residents in the United States were happy to see an increase in the police use of drones during the COVID-19 crisis, seen as an unwelcome introduction that impeded their freedoms, a view shared by many citizens across the world. In the suburban town of Westport, Connecticut, residents raised concerns over possible privacy violations as members of the public and the media observed police surveillance drones yelling at people not observing the 6 feet apart social distancing guidance [8]. The American Civil Liberties Union of Connecticut (ACLU-CT), a nonpartisan, nonprofit membership organization that defends, promotes, and preserves individual rights and liberties, described the police action as an avenue for privacy-invading companies to use the coronavirus pandemic to create a market for their surveillance products [9]. However, the Westport Police Department said that the drones would not fly over private yards or use facial recognition technology [8]. Westport first selectman Jim Marpe praised

the police department for adopting smart solutions in fighting the spread of the virus. He said the use of the surveillance drones was a pilot program to help flatten the curve of the COVID-19 virus infections to return the city to its regular routine, but he also expressed disappointment that many citizens opposed the use of the surveillance drones for whatever reason [8]. The extent of public concern and complaints made to authorities resulted in police pausing the use of drones until they carried out a full assessment of the drone's privacy impacts [8]. It is clear to see why police in Westport, Connecticut, and other jurisdictions across the world chose to utilize drones to enforce COVID-19 emergency measures as they offered a new tactic for policing public gatherings that could be operated remotely, they presented little or no risk of infection to their operators, they could be acquired cheaply and easily, and their operation could be mastered simply and safely.

The police use of drones to enforce emergency powers was another new and unprecedented measure to protect the public during the coronavirus pandemic. Despite being encouraged to socially distance to prevent and delay the spread of the virus, a mixture of complacency, naïveté, and irresponsibility, combined with the very human desire to venture outside, served to force many governments to take extreme, draconian but necessary measures to keep citizens safe, based on the best medical advice that they were receiving. However, some senior police officers recognized that how these draconian measures were being enforced had the potential to change the delicate relationship between citizens, their communities, and the police, as well as impacting the acceptance of future drone use. The police use of drones to enforce COVID-19 emergency powers also raised concerns among civil liberties groups who warned that during crisis events where political stakes are high, legislators fear being seen as lenient or indifferent and often grant the executive broader authorities without thorough debate, resulting in new, special provisions intended to be temporary, which, in reality, turn out to be permanent. The police use of drones during the COVID-19 pandemic across the world brought into sharp focus the need for regulatory frameworks and regulations to reassure the public about their safety and private concerns for the continued proliferation of the use of drones in society.

8.3 Counter-Drone Strategy

Effective counter-drone management is an issue of growing concern for government and all sectors as the number of aerial security incidents has grown globally. The primary focus of national and international counter-drone initiatives to date has been on developing a more effective drone safety ecosystem [10], in particular, the licensing and regulation of drone

use, educational programs, new legislation to tackle criminal activity, and engagement with the private sector to further develop counter-drone solutions. All of these initiatives are essential steps in developing a counter-drone security posture, but governments continue to grapple with the issue of drone technology proliferation and the related safety and security implications, while seeking to ensure that appropriate controls are proportionate and do not unnecessarily impede the development of a new market that has the potential of making a valuable contribution to a nation's economic well-being. Legislative and regulatory approaches to dealing with drones are important and need to progress, but what is evident, largely by its absence in contemporary counter-drone discourse, is the need to view counter-drone management in the context of broader organizational resilience planning, particularly concerning national security strategies and the protection of critical national infrastructure [10].

The concept of organizational resilience means much more than maintaining business continuity or crisis management, which is single and event-focused. The British Standards Institution defined it in the following terms [11]: "Resilience is a strategic objective intended to help an organisation to survive and prosper. A highly resilient organisation is also more adaptive, competitive, agile and robust than less resilient organisations. Organisational resilience is the ability of an organisation to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes." A resilience approach is especially important in the context of drone management due to the often rapidly changing threat and risk landscape attributable to the pace of evolving technological innovation. This necessitates that organizations regularly review their systems, processes, training, and equipment needs, making adjustments as and when needed, to ensure that they remain as fully prepared as possible to ensure the most effective responses to any drone-related incidents [10]. Failure to do so can result in unnecessary gaps and vulnerabilities developing, which can render an organization less resilient, often unnecessarily so, since there is no one-size-fits-all approach and technological innovation does not remain static.

A recurring theme across public and private sector organizations that have experienced or are most likely to have to deal with drone incursions and other incidents is their reliance upon often expensive and complex hardware and software counter-drone technological solutions. While counter-drone technology may be entirely appropriate to assist in the identification, detection, tracking, and defeat of drones, the technology is still very much developing in terms of its capability and is limited to its technical roles. The limitations of technological counter-drone solutions is evidenced by a catalog of high-profile incidents, where unsatisfactory responses have

failed to detect multiple rogue drone incursions and identify the pilot, resulting in far fewer arrests and convictions for those responsible of causing large-scale disruption to essential services. Important lessons for developing organizational resilience approaches continue to be gained by those organizations suffering drone-related incursions. Recurring themes have included:

- Complacency and inadequate preparedness resulting in less effective responses and greater damage and/or loss than might otherwise have been the case;
- Intelligence failings regarding the acquisition of new equipment by malicious nonstate actors, affecting preparedness;
- The need to assess, reduce, and manage risk better;
- The insufficiency of existing doctrine (including law enforcement and military), with accompanying lack of clarity regarding how to prioritize conflicts in stakeholder interests as well as to identify lead government departments;
- The limitations of equipment such as defense capabilities due to the speed with which militants can develop new drone capability compared with lengthy, complex procurement timelines [10].

There are a number of potential ways of mitigating or even preventing these issues. The first is by increasing organizational education on issues relating to drone threat versus perception: the ability to identify and distinguish between different types of drones, some of which may indeed pose a real threat to an organization, but the vast majority of which are unlikely to do so. Accurate drone threat recognition is immensely important, since a potential overreaction to risk may impact adversely upon an organization's business operations, resulting in significant reputational damage, commercial losses, or potentially costly and unnecessary deployment of police and/or military assets. The sense of panic that a drone incident can cause, including a thorough lack of understanding as to the real nature of any perceived threat, together with an accompanying need to be seen to be doing something in order to retain commercial and/or public confidence can also result in expensive, hasty procurement decisions that do not always represent the best use of limited available resources [10].

A further factor in developing a strategic counter-drone response is to be cognizant of the potential challenges and limitations associated with the procurement of counter-drone technology. When deciding if and what capability in which to invest, it is important for organizations to not only fully understand what types of drones they are most likely to encounter

and what their strategic, tactical, and operational goals in counter-drone responses are likely to be, but also whether any expensive investment is likely to become out-of-date quickly. With an increasing number of organizations responding to the growing security threat from drones, security managers have to chart their way through the muddy waters of which counter-UAS is right for their specific needs, which is not a simple process. To start with, they need to have a thorough understanding of their own particular threat landscape before they can begin to decide what kind of detection and mitigation technology will be fit for their purposes. Yousuf Malik, the principal consultant at Defence iQ, stated [12]: "The drone-detection technology solutions are complex. Take radar for example; you would need to understand technical terminology around range, output power, signal-to-noise ratio, Doppler effect, polarisation, beam-steering, frequency, interference, signal processing techniques and much more. Without this understanding, it is not possible to make an objective comparison between different systems." Avoiding costly mistakes in system procurement requires an understanding of different sensors, command and control, standards, and measurement of effects, among others. Potential customers for counter-UAS solutions have trouble understanding why apparently similar solutions vary so much in cost and must avoid making expensive mistakes by investing in a solution that appears to work well in demonstrations but often fails to deliver in the real world. To support the drone-detection procurement decision-making process, the following steps should be followed by all organizations to ensure the successful procurement and implementation of the right drone-detection system:

- Understand the broad drone threat landscape and identify the specific threats to your organization.
- Gain a scientific, nuanced, and unbiased understanding of the underlying technologies for counter-drone systems.
- Learn how to make an objective comparison between different counter-drone solutions free from vendor bias.
- Create a roadmap to clarify routes to vendors and procurement processes.
- Deepen your knowledge of upcoming standards to know what you can and cannot procure.

The complexity of drone-detection system procurement to underpin a counter-drone strategic response presents a real challenge. Given the rapidly evolving nature of the drone and counter drone sector, buyers should

adopt an "evergreening" technology strategy that ensures that the procurement of counter-technologies does not overcommit to responses with a short shelf life, but instead prioritizes flexible and adaptive solutions [10]. The procurement of the relevant technology is an important part of developing an effective counter-drone strategy. A tried and tested security strategy structure that can be adopted to counter-drones is the four-P model, first introduced by the U.K. government to devise a counterterrorism strategy following the tragic events of 9/11 [13]. It is a model now widely adopted and adapted by governments across the world. The four-P strategy, divided into four key pillars that provide the scope to reduce security threats, can be easily adapted for an effective counter-drone strategy [13]. The four pillars of a counter-drone strategy are:

- *Prevent:* To stop rogue drone incursions and related attacks;
- *Pursue:* To detect rogue drone incursions and related attacks;
- *Protect:* To strengthen protection against rogue-drone threats;
- *Prepare:* Where an attack cannot be stopped, to mitigate its impact.

The broad principles of the four-P structure ensures through Prevent and Pursue that countermeasures are designed to reduce the risk of drone attack while Protect and Prepare focus upon building capacity and capability to reduce vulnerability of attacks when they occur. By simultaneously tackling areas to reduce the risk and to minimize vulnerability, they collectively serve to reduce the overall threat from rogue drone incursions and all manner of identified attacks. Moreover, developing the four-P structure for a counter-drone strategy is easily understood as a logical narrative, being able to be translated into specific programs of action across organizations, and is capable of being updated and extended in response to developments in the threat and in drone technologies for countering it. Creating an effective counter-drone strategy within a four-P structure, being underpinned by a detailed knowledge of the drone threat landscape, should include the following developments:

- Building counter-drone capability within the organization, investing in developing counter-drone expertise within the security function;
- Engaging the technology landscape to understand the capacity and capabilities of new, emerging and existing technology systems;
- Integrating counter-drone plans, policies, and procedures within existing security operations and culture of the organization;

- Facilitating testing, training, and exercising of counter-drone responses to expose vulnerabilities and levels of preparedness;
- Coordinating education and awareness activities of the strategy across all organization departments to improve preparedness and resilience;
- Regularly communicating and updating counter-drone policy, plans, and procedures across all internal and external stakeholders [14].

The four-P model provides a valuable framework to build an effective counter-drone strategy, but since drone-related technological innovation inherently raises issues across the security, safety, and disaster risk paradigms, a failure to adopt a fully integrated approach, such as the identification of all relevant factors, can lead to flawed planning assumptions, resulting in less effective preparedness and response measures [10]. Counter-drone strategies must therefore be synchronized with existing security operations and embedded within the very culture of security practices to maximize its full potential. All counter-drone approaches will prove largely ineffective without fully understanding the issues, formulating a comprehensive strategy, deploying the appropriate equipment, and integrating that equipment into a coherent and comprehensive strategy.

8.4 Review and Reform

Reducing the risks posed by malicious illegal drone use will require organizations to invest their time and money to upskill personnel and devise effective counter-drone approaches. These approaches may require the procurement of technical counter-UAS and their effective operational implementation, which must yield a positive return on the investment, providing benefits that are proportionate to managing the identified risks. To ensure continued maintenance of security from all manner of drone threats, measures must also be put in place to analyze performance and regularly review risk assessments and operational delivery of counter-drone plans, policies, and procedures throughout the full life of the strategy. Regularly reviewing counter-drone measures to determine where and how to rebalance investments in drone security to keep them effective while providing value for money ensures that the organization remains able to reap the positive benefits of incorporating drone technology into their security operations. Due to the fast-evolving nature of drone and counter-drone technology, it must be the intention of security professionals to review and, if necessary, refresh counter-drone strategies regularly and in line with existing stress-testing security regimes to ensure high levels of preparedness and resilience.

There are also a number of other important self-help measures that an organization can take to make itself more resilient and less dependent upon a range of external actors and resources, while also meeting their legal due diligence obligations. This includes reviewing the extent to which any counter-drone technological solutions are fully embedded within existing organizational resilience approaches, including in terms of governance, accountability, integrated training, operational decision-making, and crisis management. Security professionals can also make adequate provision for effective knowledge management and transfer, especially since relatively few adequately trained counter-drone technicians currently exist to avoid the dilution or even loss of technological capability should technicians be unavailable [10].

Embedding a rigorous, proactive culture of review and learning following any incident to ensure that key lessons are identified, related modifications to existing approaches are made, and the organization continues to adapt and respond to the parallel evolving threat and risk landscape is also essential learning to improve counter-drone security postures. Such measures are aimed at assisting organizations not merely to survive, but rather to thrive should drone-related disruptions occur. All in authority would be wise to learn that responding to the threat of drones is ineffective without fully understanding the issues, formulating a comprehensive strategy, deploying the appropriate equipment, and integrating that equipment into a coherent and comprehensive strategy, including prevention, detection, evaluation, reaction, investigation, and review. All organizations that perceive that they are at risk from any kind of malevolent drone incursion or malicious attack must now act to identifying effective solutions to safeguard its infrastructure and personnel from the diverse rogue drone threat landscape, which is becoming increasingly aggressive.

8.5 Regulatory Frameworks

The increased use of drones for civilian applications has presented many countries across the world with regulatory challenges. Such challenges include the need to ensure that drones are operated safely, without harming public and national security, and in a way that would protect areas of national, historical, or natural importance [15]. Ongoing large-scale commercial investment has led to civilian drones becoming cheaper, able to operate over longer ranges, and capable of carrying ever-larger payloads. The pace of development has accelerated in recent years, with a vast range of models now available to the civilian customer. There are hundreds of models available, ranging in size, speed, weight, and payload capacity. There is no doubt that drones are here to stay and will continue to have an even greater

positive impact on society than has already been achieved. However, there will also be those hostile actors who embrace and embed drone disruptive technology into their illegal operations. Although there is still a large gap between the capabilities of military and civilian drones, commercially available drones are giving hobbyists, companies, and hostile groups access to capabilities previously only available to the military [16]. Given the speed of technological advancements in the drone sector and the new and creative ways in which hostile actors are finding nefarious uses for UAVs, law enforcement agencies and policymakers are endeavoring to respond appropriately to this continued development. The legislation governing the civilian use of drones is still evolving and regulators around the world are scrambling to keep up with new uses, capabilities, and drone technology.

Many nations have leaders in innovation and emerging technologies who are at the forefront of rapidly developing aspects of the growing drone market. Every national government is seeking to maintain and develop its own position as the place for technology companies to build their businesses, to invest in new innovation, and to use science and engineering to drive new technologies to reach their full potential to amplify their economic well-being. It is therefore vital that all governments seek to balance maintaining and developing their leading positions in aviation safety and security while supporting the development of the emerging drone industry [17]. Although the first duty of government is to keep its citizens safe, and in order to do so must ensure the safety, security, and accountability of the drone industry, it also seeks to harness the benefits that drones, used in a safe way, can bring to its economy. Balancing the competing demands of security and economic prosperity has resulted in approaches to drone regulation that differ dramatically across the globe, where the elements of regulation are largely the same from country to country, but with wide ranges on the level of restrictiveness of each regulatory element that is often dictated by whether a country favors the promotion of new technology or a safety-first approach [18]. It is not within the scope of this chapter to detail all the current rules and regulations currently in operation across the world, primarily because of the increasing volume of laws and also the regularity at which existing provisions are updated to keep pace with new threats and technological developments.

8.6 International Challenge

As UAV technology becomes more advanced, more approachable, and more affordable, troves of recreational and commercial drone pilots are entering the drone industry [19]. Due to a sharp increase in drone use internationally, countries are struggling to incorporate drones into their aviation

regulatory frameworks [18]. The first challenge in devising UAV regulations is to define what a drone actually is. Unfortunately, there remains no international consensus at this time of a detailed definition of a UAV suitable for the purposes of international law, as every country has each own variation. However, there are common aspects of drone definitions operating across the world today using the term "drone" to refer to a small unmanned aircraft, whether they are remotely piloted or autonomous. Other common legal descriptions of drones includes that they can be fixed-wing, rotary-winged, or a combination of both [1]. Some legal definitions of drones state that they may be controlled remotely or use satellite navigation systems or other methods to fly autonomously or semiautonomously and that traditional radio-controlled model aircraft are also classed as drones for regulatory purposes [1]. Defining what a drone is, and therefore what a drone is not, is essential in law to ensure that related regulations are fit for the purpose for which they are intended. The rapid rise of drones and the frequent introduction of new technologies and capacity continue to challenge the relevance and currency of existing drone regulations as they quickly become outdated and require regular review and reform.

For countries that have drone regulations, they typically incorporate four areas of regulatory requirements including: a pilot's license, registration of the drone, restricted zones, and insurance [18]. These regulatory requirements vary based on such parameters as drone mass, population density, altitude, and use cases. Even for countries with existing drone legislation, laws are constantly being reevaluated, with most drone-related laws being amended every 2 years. While drone laws almost always move toward a more permissive approach to regulation, the creation of new basic infrastructure may aid in the success of such a transition. Specialized training courses, pilot exams based on the type of UAV and the conditions under which it operates, and liability insurance to protect against accidents overpopulated areas are all mechanisms for ensuring the safety of the general population as usage laws become more permissive. In looking at the variation in the four components of regulations across countries, according to a commercial drone regulation study by the RAND Corporation [18], six broad approaches to national commercial drone regulation become apparent and they include:

1. *Outright ban:* Countries do not allow drones at all for commercial use.
2. *Effective ban:* Countries have a formal process for commercial drone licensing, but requirements are either impossible to meet or licenses do not appear to have been approved.

3. *Requirement for constant visual line of sight (VLOS):* A drone must be operated within the pilot's VLOS, thus limiting potential range.

4. *Experimental uses of beyond visual line of sight (BVLOS):* With certain restrictions and pilot ratings, exceptions to the constant VLOS requirement are possible.

5. *Permissive:* Countries have enacted relatively unrestricted legislation in commercial drone use. These countries have a body of regulation that may give operational guidelines or require licensing, registration, and insurance, but upon following proper procedures, it is straightforward to operate a commercial drone.

6. *Wait-and-see:* Countries have enacted little, if any, drone-related legislation and monitor the outcomes of other countries' regulations.

International standards to regulate certain aspects of drone operations are currently being considered by the International Civil Aviation Organization (ICAO). In 2011, the ICAO issued a circular titled "Unmanned Aircraft Systems (UAS),"[1] serving as a first look at the subject, the circular called on states to provide comments, "particularly with respect to its application and usefulness," in an effort to proceed with the development of [15]: "the fundamental international regulatory framework through Standards and Recommended Practices (SARPs), with supporting Procedures for Air Navigation Services (PANS) and guidance material, to underpin routine operation of UAS throughout the world in a safe, harmonized and seamless manner comparable to that of manned operations." To advance the international standardization of drones, the ICAO established DRONE ENABLE, a framework to bring nations together to discuss the challenges of UAV safety and security. DRONE ENABLE seeks to build international consensus and has held a series of symposia convened to address specific themes. In 2020, the fourth DRONE ENABLE symposium [20] was held with the theme of "Addressing Tomorrow's Challenges Today." The ICAO symposia bring together key stakeholders from industry, academia, government, and international organizations in the unmanned aviation sector to exchange best practices, lessons learned, research material, and challenges related to the introduction of UAS and UAS unmanned traffic management (UTM) [20]. All DRONE ENABLE symposia showcase the breadth of existing technologies and ongoing research and development and describe commercial

1. International Civil Aviation Organization, *Unmanned Aircraft Systems (UAS) ICAO Cir 328 (2011)* [Online] Available at: https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf (Accessed 15/5/20).

and noncommercial activities in this rapidly evolving sector of the aviation industry. The ICAO symposia also provide participants with valuable networking opportunities and all in the drone sector are encouraged to engage, contribute, and follow the development of the DRONE ENABLE symposia, which will serve to shape the future of drone flight at an international level. Understanding international drone legislation is critical to determine which countries will be the most open to the use of drones and what sort of precedent is set for late-acting countries to adopt legislation.

8.7 European Regulations

Efforts to harmonize the rules of drone operations are currently being undertaken by the European Commission (EC), which has introduced new regulations to integrate all drones, regardless of their size, into the existing European aviation safety framework [15]. The responsibility for the operation of civil drones in European airspace was transferred from the national aviation authorities to the EC in December 2018 [21]. Civil drones refer to all drone usage other than by the military, police, or emergency services. The European Union Aviation Safety Agency (EASA) was appointed by the European Parliament to propose to the EC the technical expertise to regulate drones below a maximum take-off mass (MTOM) of 150 kg [21]. The proposed regulations by EASA were unanimously accepted by the EC in 2019, followed later that same year by the publication of the new European regulations for using civil drones, being the responsibility of each member state's Civil Aviation Authority to implement the regulations which was completed during July 2020 [22]. The new regulations aim to create a level playing field in Europe and will remove most drone operations from the aviation domain in terms of regulation. Current manned aviation regulations are rule-based and have proven to be insufficiently flexible for the rapidly changing drone market and so the new European regulations provide a blueprint for other jurisdictions across the world to see if they provide the necessary safety measures to reduce the risk of rogue drone threats [21]. According to the EC Commissioner for Transport, Violeta Bulc, the new rules under Commission Delegated Regulation (EU) 2019/945 and Commission Implementing Regulation (EU) 2019/947 ensure that [22]: "The EU will now have the most advanced rules worldwide. This will pave the way for safe, secure and green drone flights. It also provides the much needed clarity for the business sector and for drone innovators Europe-wide." The laws form part of EASA measures to regulate drones, alongside projects to create a UAV traffic management system across the EU called U-Space, a term adopted to describe the management of unmanned aircraft traffic to ensure the safe interaction with other entities using the same space in any

location, not just urban areas [23]. Despite new laws and safety measures, the adoption of drones as a tactical attack planning option for terrorists to cause mass disruption, damage economic stability, and threaten European security remains a concern. Reinforcing this threat, in August 2019, EU Security Commissioner Julian King warned that drones could be used for acts of terrorism, stating that [24]: "Drones are becoming more and more powerful and smarter which makes them more and more attractive for legitimate use, but also for hostile acts." The warning followed the publication of a leaked secret report in December 2018 from France's Anti-Terrorism Unit (UCLAT) to the country's Special Committee on Terrorism. The report warned of [24]: "A possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents." The introduction of new drone regulations across Europe, given the safety and security concerns, is timely.

The new European drone regulations are risk-based and divide the operations, whether commercial or recreational, into a low-risk category (open category) and a medium-risk category (specific category) [21]. The high-risk operations will remain in the manned aviation domain under the certified category. The open category places very few demands on the drone pilot or operator and implies a buy-and-fly approach [21]. Pilot qualification can be as simple as an online exam, although the drones themselves will require having a EC-approved product certification. Many of the current routine commercial drone operations will be possible in the open category as long as they do not take place over or near people. All other operations, unless high-risk, are performed in the specific category. For this category, a risk assessment must be carried out by the operator with associated mitigation measures implemented and approval requested from their national aviation authority. The new European regulations are far-reaching and will bring changes to the whole drone industry, although, given the scale of the changes, there will inevitably be a period of uncertainty as the new rules come into force. However, the implementation of the new regime does create a much-needed European-wide structure, bringing uniformity to the former fractured and outdated regulations that differed in each country across Europe.

The development of drone regulations in Europe continue to advance through EASA, which, in April 2020, published the first view worldwide on the use and control of drones in an urban environment, balancing the desire to maximize the commercial and convenience benefits of drones against the need to ensure the safety and privacy of citizens and the potential environmental impact on our cities. The challenge of integrating drones into urban environments is that these areas are already densely used by ground traffic, other types of air traffic, such as commercial airplanes, other civil aviation,

and police or hospital helicopter services, and also people, concerned about noise, privacy, and the possibility of low-level flights causing accidental injury. Patrick Ky, the executive director of EASA, stated [23]: "We are already starting to see an increasing number of complex flights undertaken by drones in various experiments across the globe. Also, as everyone is aware, many companies have commercial ambitions to use drones for deliveries or, looking further ahead, to offer services such as air taxis." EASA proposals have recommended the introduction of a regulatory framework that will allow such drone services to coexist with all the other activities in our urban environments. The aim is to ensure safe operations, while also creating the basis for a competitive U-space services market and establishing a level of environmental protection, security, and privacy that is acceptable to the public. The EASA proposal, presented to the EC as a basis for future legislation, laid down the first building block for the establishment of the U-space in Europe [23]. The initial scope is low-level airspace, densely populated urban airspace, and locations close to an airport, with no attempt made to cover the airspace in other areas. EASA expects to expand the scope as the market develops and experience is gained, providing evidence of how EU regulators are leading the global effort in finding workable solutions to tackle the increasingly problematic domain of drone regulation.

8.8 Enforcement

All in authority are acutely aware that regulations are only as effective as the enforcement regimes that support them. It is therefore essential that every element of a regulatory framework carefully considers the practical challenges of enforcing drone laws. Integral to the success of enforcing drone regulations, as well as preventing rogue drone threats and investigating incidents when they do occur, are capable, professional, operational first responders. Vital to any counter-drone approach, these responders will in many cases be police officers, who, depending on the incident, could be required to exercise a counter-drone response across any at-risk sector. Specific at-risk sites will have their own operational responders, including other public authority employees such as prison officers, or private sector employees responsible for safety and security in a variety of locations, such as privately operated prisons, critical national infrastructure, and crowded open-air public spaces [1]. To ensure that first responders understand their role and responsibility within drone regulatory frameworks, they must have at their disposal a full range of powers to act against malicious drone use and be empowered through training and, where appropriate, through access to counter-drone systems and the powers to use them. It therefore remains essential that all governments work to ensure that all responders

have access to training, technology, and legal powers appropriate to their roles and the drone risks they face, so that they can act confidently and decisively address drone-based threats.

In the United Kingdom, as police officers are responding to an increasing number of drone-related incidents, police officers have new powers to land, inspect, and seize an unmanned aircraft if an offense has been committed and a warrant is secured [25]. They also have stop-and-search powers around airports and prisons to help tackle illegal drone use. To support the police in their challenging role, drone users in the United Kingdom face receiving on-the-spot fines for certain offenses, such as failing to provide evidence that they have the correct permissions and exemptions if found to be flying their device too high or too close to buildings, or failing to provide evidence of competency or registration. The U.K. Transport Minister, Baroness Vere, stated [25]: "Drones have incredible potential, whether that's by transforming how we move goods around or saving lives in search and rescue missions. Most people using drones want to do so responsibly, and we encourage them to familiarise themselves with the law. We are confident these police powers will be used proportionately to both deter careless drone use and to tackle serious, malicious criminal activity." The United Kingdom's new drone provisions also allow the police and senior prison authorities to authorize the use of counter-drone measures to combat illegal drone use. Despite the new powers in the United Kingdom being welcomed by police officers, there remains a number of unique challenges that confront first responders when attempting to increase their awareness of drone and counter-drone issues. The perceived complexity of the subject, the technical skills required, and the nature of specialist aviation-related provisions are contributing factors, all of which will be required to be overcome if the new police provisions to enforce drone regulations are to be effective.

A major vulnerability of first-responder counter-drone efforts is the protection of public spaces alongside sites and sectors critical to a nation's infrastructure. Unfortunately, rogue drone incidents over recent years have exposed fault lines in multi-agency first-responder cooperation, coordination, training, awareness, and command and control processes to effectively respond to a rogue drone incursion. At present, first-responder agencies do not have the capacity or capability to effectively respond to a UAV terrorist attack on a public space, nor do they have a coherent or coordinated plan to implement in response to a UAV terrorist attack [26]. Therefore, all in authority must dedicate themselves to enhancing the coordination and cooperation between law enforcement, civil protection, and medical services through joint training and the collaborative development of a shared plan to institute to effectively respond to a terrorist attack using a UAV. Governments are working to ensure that they have nationally consistent principles

to prevent any gaps in response requiring multiple agencies. All governments must also now ensure operational responders know when and how to act, including the wide range of government organizations that play a role in responding to malicious and illegal drone activity [1]. A coordinated approach to enforcement of regulations is critical to maximizing the effectiveness of the response to rogue drone incursions. Further work will be required by authorities to ensure that drone legislation keeps pace with the evolving threat, is responsive to operational experience, and directly informs training and guidance for first responders. Governments must continue to develop proposals for inclusion in future legislation so that any drone legal framework within which operational responders must operate does not become obsolete or hamper their ability to respond to and investigate hostile drone activity. Moreover, the provision of police powers to enforce regulations, including to request evidence from drone users where there is reasonable suspicion of an offense being committed, provides confidence to the public that drone users are being monitored and brought to justice when their actions fall outside of the law, all of which serves to advance social acceptance for the future use of drones [17].

8.9 Balancing Act

Tackling malicious drone use requires a comprehensive and layered strategic approach to be put in place by government and implemented across the full local, regional, and national apparatus of the state. This strategic approach must blend technological innovation with legislation, regulation, and education. Developing counter-drone solutions will not solely reside in one nation; it is a global phenomenon requiring greater collaboration, including the sharing of knowledge, expertise, and best practices. Monitoring the evolution of international drone regulations, along with technology trends and security and safety incidents, provides insights into the ways that gradual or all-or-nothing approaches to regulation affect technology adoption and whether gradual approaches to introducing untested drone technology mitigates potential hazards [18]. Governments will seek to learn from each other to see which regulations actually work, compared to those that serve to restrict innovation and curb the progress of the drone sector in their jurisdiction. The challenge of preventing rogue drone threats is a problem that cannot be solved by authorities alone; at-risk sectors within private industry must now adhere to guidance provided by government. All commercial and private drone pilot enthusiasts must also play their part in keeping within the law while striving to set the highest professional standards. Drone enthusiasts should not hesitate to report other drone users who fail to comply with regulations as they jeopardize the future of drone

flight and risk committing offenses that provide evidence to regulators to strengthen their guidance.

To reduce the risk of drone threats, technological countermeasures need to coevolve with the advancement of drones and within the legal and regulatory frameworks that govern their use. Governments must work with manufacturers to introduce new technologies that will help in making sure drones are used in accordance with the law and encourage or even legislate for built-in security by design measures. This includes geo-fencing, where a drone can be automatically prevented from flying within protected areas through built-in software, and electronic projection, which allows the automatic identification of all airspace users including drones [17]. Many commercially available drones already include geo-fencing capabilities and governments across the world should amplify their efforts in engaging directly with drone manufacturers and industry on how these capabilities can be improved. This may include working with airspace managers and regulators to understand how robust data on permanent and temporary airspace restrictions, such as those around airports and other critical national infrastructure sites, can be made available in a format that manufacturers and technology developers can easily use to improve safety and help drone users fly in accordance with the rules [1]. Policymakers should also seek to pass stricter regulations limiting the capabilities of commercially available drones in the key specifications affecting hostile drone operations, especially payload capacity. Particular attention should be paid to limiting the attack and intelligence, surveillance, and reconnaissance capabilities of UAVs. Moreover, authorities must consider the licensing, registration, and introduction of unique serial number provision for each purchased drone registered by civilian operators of drones capable of carrying payloads [16]. Keeping people, property, and data safe from all manner of malevolent drone threats is a team effort requiring increasing levels of collaboration between authorities and industry. Ensuring the appropriate balance between maintaining safety and driving drone innovation to reap the economic rewards for the exponential growth in the drone sector in coming years requires higher levels of government and private industry engagement and cooperation.

Governments across the world will consider what further product standards or restrictions within the drone sector could reduce risks associated with the misuse of drones without disproportionately affecting legitimate users [1]. However, the best defense against the hostile use of drones is to employ a hierarchy of measures to counter the threat, which encompasses regulatory, passive, and active countermeasures [16]. Regulatory countermeasures can restrict the capabilities of commercially available drones and limit the ability of hostile groups and individuals to procure and fly drones [16]. The combination of these countermeasures, augmented by a

counter-drone strategy as an integral component of broader security operations, serves to support the prevention and detection of rogue drone threats to public safety and national security. Despite the increasing introduction and regular review of existing regulations, security policymakers remain concerned that the rapid growth of the drone industry continues to outpace the development of rules and regulatory systems to govern their use and, by extension, the powers for police and other civil authorities to effectively enforce drone laws. Regulations to prevent the misuse of drones will reduce the threat, but the uncomfortable truth is that they will not be able to prevent them all, given the hostile intent and creative ambitions of rogue actors who continue to seek new ways in which to adopt drone technology to advance their malicious operations. Given the scale and scope of drone technological advancements, the next generation of drones to be integrated with increasing levels of analytical computer power and artificial intelligence ensures that the threat from drones shall persist, remaining a major public safety and national security concern for the foreseeable future.

8.10 Counter-Drone Innovation

UAVs have earned their status as a contemporary disruptive technology, proving themselves to be an innovative development that has significantly altered the way that consumers, industries, and businesses across the world operate [27]. The proliferation of UAVs represents a disruptive technological innovation that continues to develop at an exponential speed and on a global scale. For drone and drone-detection companies, keeping pace and surviving in the new and dynamic disruptive technological evolution remain a significant challenge. However, simply surviving is not a recommended ambition, so how can individual drone sector organizations thrive in this environment? Darwinian business models provide an abundance of evidence that the strongest, or the most profitable, organizations are not the ones that survive, but rather the organizations that survive are the ones that are most adaptable to change [28], more specifically, adapting to change by actively embracing, encouraging, embedding, and creating an environment and culture of innovation to realize new ways of working faster [29]. Such innovations are driven by the possibilities offered by modern information technology and fundamental and applied scientific research that is influencing social reality, causing it to change at a high speed, and indicate that the twenty-first century will be characterized by the exponential revolution, more so than any previous decade. Disruptive social and technological innovations will occur at an ever-increasing speed, causing continuously, relatively fast, and drastic changes to society and the economy with impacts upon the UAV sector. This is not an era of change, but a change of eras.

In order to become agile and to remain successful, it is necessary for UAV companies to carry out activities that aim at influencing both the mindset and skillset of the drone sectors' most valuable asset: its people. The purpose of this chapter is therefore to provide guidance to adapt to change through innovation, including practical explanations of how to implement innovation. This chapter provides positive and practical steps to embed, and scale to any size of organization, a culture of innovation and an ecosystem where innovation can thrive, underpinned by acquiring, developing, and retaining the most talented professionals in the drone industry. Those leaders and key decision-makers in the drone sector who quickly learn that they are stronger when they work in partnership and realize that they can no longer solve many of the drone and counter-drone problems on their own will be better prepared to meet the challenges of tomorrow, reaping the rewards within a global drone market estimated to reach $14 billion over the next decade [30].

Moreover, those organizations that encourage and embrace breakthrough ideas and concepts from within and beyond their organizational boundaries will attract the most talented and creative people, encouraged by investment in their continued professional development through training and the workplace culture and environment that encourage autonomy to create and deliver. Organizations within the drone sector that adopt this approach will prove to be those that thrive and not merely survive.

8.11 Research to Reality

Despite new laws and safety measures, the adoption of drones as a tactical attack planning option for terrorists to cause mass disruption, damage economic stability, and threaten security remains a concern across the world. The terrorist use of UAVs has already materialized in theaters of conflict with devastating impact. Europol, Europe's leading law enforcement agency, has revealed that terrorist attacks across Europe have shown a recurrent targeting of public spaces and that terrorist organizations are using increasingly innovate techniques, which require an equally innovative approach by law enforcement to mitigate emerging threats, which includes those posed by the terrorist use of UAVs [31]. To develop an emergency service agency response to the hostile use of drones, the EC has invested in research projects to improve civil protection responses to secure public places against terrorist threats. A unique collaborative research and innovation project, funded by the EC Internal Security Fund for Police (ISF-P), is providing valuable training tools for first-responder agencies to improve responses to terrorist attacks on public space using drones [32]. Project DroneWISE, a 2-year action concluding in 2022, recognizes that the illegal use of UAVs is

a serious concern across the world as terrorists adopt drone technology and develop new and creative ways in which to deliver mass murder on an unimaginable scale [26]. The multidisciplinary consortium of partners delivering DroneWISE recognizes that recent rogue drone incidents have exposed fault lines in multi-agency first-responder cooperation, coordination, training, awareness, and command and control processes. By building on existing work and amplifying current action in this field, DroneWISE will deliver practical security solutions via training and strategies for first responders, civil authorities, and medical services to significantly improve the security of public spaces from UAV terrorist attacks [26]. The ethos of DroneWISE is to enhance the coordination and cooperation between law enforcement, civil protection, and medical services through joint training and the collaborative development of a shared plan to institute to effectively respond to the acute phase after a terrorist attack using a UAV. The combination of DroneWISE measures brings together multiple first-responder agencies to plan and prepare their responses. The collective impact of DroneWISE measures will serve to increase the preparedness of first-responder agencies to better coordinate their efforts, significantly improving the protection of public spaces and coordinated response and increasing resilience to all manner of terrorist attacks using UAVs.

The DroneWISE project will develop and deliver counter-UAV command training for all first-responder agencies, including tactical options and decision-making frameworks, supported by a counter-UAV command training handbook providing authoritative guidance for first responders. To address immediate and short-term vulnerabilities, the DroneWISE training will be delivered to first-responder practitioners across Europe during the project. The short-term needs of first-responder agencies will further benefit from the delivery of a counter-UAV command, control, and coordination strategy**,** providing a multi-agency command policy with decision-making models and a threat-and-risk matrix. To meet the medium and long-term needs of first-responder agencies, DroneWISE will deliver a counter-UAV train-the-trainers program to upskill and amplify first-responder training, and all training support materials will be made readily accessible via a counter-UAV online training portal. The combination of DroneWISE measures will serve to significantly improve the coordinated emergency responses delivered by the project consortium constituted of six partners representing five European member states, bringing forward a broad European perspective and representing the best expertise in their specific domain from government, academia, and private industry. As the coordinator of DroneWISE, the Department of Police from the University of Applied Sciences for Public Service in Bavaria provide operational and executive training to

police officers in Bavaria, which ensures unique and essential access to first responders at all levels for the project [33].

The inclusion of law enforcement agencies in contributing and coordinating large-scale international research and innovation projects provides evidence that senior police leaders are coming around to the idea that they themselves cannot begin to fully understand or tackle the complexity of contemporary security hazards. From combatting all manner of rogue drone incursions and drone-enabled terrorism, drug trafficking, and cybersecurity challenges, police officers are beginning to understand that collaborating with academic and technical experts can provide unique perspectives and practical solutions to address their policing challenges. Evidence of multidisciplinary collaborative research with active engagement and full integration of law enforcement agencies remains rare. For the most part, the field remained dominated by research on the police, designed, directed, and carried out by academic researchers. However, the desire of police officers and academics, alongside technicians and engineers from private industry, over recent years to work together has resulted in collaborative networks that are bringing about positive change. The DroneWISE consortium of partners embodies the new innovative and collaborative approach required to be replicated across the drone industry landscape. It includes the European Institute in Bulgaria, which is providing strategic security policy expertise [34], and the Centre for Security Studies (KEMEA) in Greece, providing academic rigor and direct access to the Hellenic Police of Greece [35]. The DroneWISE consortium is further complimented by RiniGARD in Croatia, which brings valuable drone and drone detection technical expertise, fused with first-responder operational experience providing essential industry insights to the latest technical developments of UAVs [36]. Saher-Europe in Estonia also adds substantial value to the DroneWISE partnership by unique first-responder strategy development and operational training expertise within the domain of counterterrorism and the protection of public spaces [37]. The University of Applied Sciences Velika Gorica in Croatia completes the DroneWISE consortium, which brings academic expertise in crisis management in the security domain, alongside essential training development, evaluation, and quality assurance skills [38]. The DroneWISE consortium has the perfect complementarity of skills, expertise, and operational first-responder competence, bridging the gap between government, academia, and private industry to bring innovative and collaborative counter-drone research to commercial and operational reality.

8.12 A Model Approach

An essential component of the DroneWISE project, and the wider success of the counter-drone industry, is the creation and continued development of effective counter-drone training to raise awareness of all manner of drone-related threats. Unfortunately, as a direct result of the criminal use of drones, police officers around the world have to investigate an acute rise in the number of incidents and crime reports involving drones purchased online, directly from stores or from a growing number of home-building enthusiasts. The rise in the reckless and malicious use of drones has forced governments and private industry to act, taking a series of measures to counter the risks posed to their workforce, data, disruption of essential services, and damage to premises. In direct response to the continuing security concerns posed by rogue drone activities, two-time Queen's Award winners Rinicom Ltd. joined forces with security innovators at Saher Ltd. (United Kingdom) to deliver drone detection and response training. Building upon a joint research and innovation initiative funded by the U.K.'s National Aerospace Technology Programme (NATEP), carried out in close collaboration with leading law enforcement agencies in the specialist drone detection domain, and including the National Police Air Service (NPAS) and the Police National Legal Database (PNLD) in the United Kingdom, the new and innovative training provides professionals with the knowledge and skills to increase operational and organizational resilience against rogue drone activity [39].

Designed and delivered by leading industry drone and law enforcement experts, the training is underpinned by the counter-drone training model of Detection, Evaluation, Neutralisation and Investigation (DENI), which provides the essential component parts to ensure a holistic response to counter all manner of drone threats effectively [40]. Using DENI as a curriculum development model for counter-drone training provides the training program with a framework to include measures to prevent rogue drone incursions and to prepare to respond and recover from attacks when they do occur. The unique model has informed interactive training that informs attendees of the threats from drone activities and how they can effectively respond to rogue drone incidents by working through a series of evidence-based scenarios most relevant to their area of responsibility. The training is aimed to provide all professionals, from security managers, police officers, and border authorities, with a detailed and holistic understanding of the threat posed by rogue drone activity and the effective measures available to manage and mitigate risk [41]. Following completion of the DENI model training program, courses attendees are able to:

- Demonstrate a comprehensive understanding of the drone threat landscape and the capacity and capability of drones and related technologies.
- Explain the relevant law, rules, and regulations relating to the illegal use of drones in their jurisdiction.
- Demonstrate a comprehensive understanding of drone detection technologies and the measures required to counter the threat from rogue drone activities.
- Design and develop a robust threat and risk assessment framework to manage and mitigate the risks from rogue drone activity.
- Demonstrate a practical knowledge of drone detection investigative techniques to identify rogue drone activity.
- Devise a comprehensive strategic response to drone threats demonstrating an ability to develop and integrate drone security policy, practice, and procedure into wider organizational resilience planning [40].

The completion of the DENI model training ensures that attendees are able to identify and assess security vulnerabilities and take positive action to safeguard against rogue drone activity by developing effective drone security strategies [40]. Moreover, the training program supports the drone-detection procurement decision-making process, ensuring that all organizations have the required knowledge and understanding that they require to assess and successfully procure and implement the right drone-detection system to meet their requirements [42]. This unique training appeals to security and police professionals, senior leaders, and operations personnel seeking further knowledge and expertise to enhance security measures and improve resilience. This training may also be of interest to technicians and attendees seeking enhanced operational expertise and awareness of threat and risk assessment, crisis management, response, recovery, and organizational resilience planning. The DENI counter-drone training model and program provide evidence of innovative multidisciplinary research and development through a collaborative approach. This approach recognizes that no single organization can keep citizens, civil authorities, or commercial companies safe from the increasing complexity of rogue drone threats [26]. The ethos of the DENI model is that organizations working jointly together are a more powerful agent for change, drawing upon their collective strength to make a real difference to counter malicious drone attacks.

8.13 Critical Success Factors

Innovation does not simply roll in on the wheels of inevitability; it is a continuous challenge that needs to be driven, programmed, and embedded within the very culture of the drone aviation sector. The pursuit of innovation to achieve the tripling of growth forecasted for the drone industry over the next decade must be relentless [41]. If UAV and related technology companies and service providers wish to seize a sizeable market share of this exciting opportunity, they, and the wider drone aviation sector and governments, have to deliver a step change in order to meet customer demands and expectations. The way to ensure that innovative approaches are delivered is to embed innovation within the operating culture of drone and drone-detection organizations, encouraged by governments, which provide incentives through research and innovation funds and introduce appropriate regulatory frameworks while increasing public consultation to amplify the social acceptance of drones by raising awareness of their positive attributes to the economy, environment, and increased efficiencies of commercial and emergency service operations. This can be achieved through various practical steps by introducing individual instruments as part of a wider innovation machinery across the full operating landscape of an organization. This may require the development of a bespoke innovation strategy and policy, reinforced by the inclusion of strategic innovation objectives.

Organizing an environment where innovation can thrive requires the removal of obstacles to creativity and reorganizing and appreciating colleagues' creativity and passion for their profession. Essential to the removal of obstacles to innovation at all operating levels are leaders; senior leaders in particular must become champions, ambassadors, and exemplars for innovation across the drone sector. Innovation in drone and drone detection requires the support of all leadership to create and encourage the innovation ecosystem. Leaders across the drone sector community must permit themselves and their colleagues to think beyond the confines of their cultural norms and traditional operational practices. Leaders must encourage the search for better ways and different ways of working and adopt a professional working ethos that promotes creativity, courage, and confidence. Adopting an innovative approach ensures that the drone sector is not only innovating in what it is delivering but also how it is delivering, all of which serves to create an effective innovation ecosystem, resulting in the acceleration and amplification of commercial opportunities to solve the most pressing drone and counter-drone challenges. Embedding an innovative approach will ensure that individual drone companies are better prepared today to meet the challenges of tomorrow, making a valuable contribution to the growth of the drone sector and, in return, reaping the financial re-

wards by providing unique products, systems, and services that transform business and tackle societal challenges around the globe.

As drone technology continues to rapidly evolve, the response to counter the threats that they pose must keep pace and understanding the threat and risks posed by drones remain important features of mitigating rogue drone incidents. Rogue drone incursions and malicious attacks that continue to occur with alarming regularity provide evidence of the persisting threat from actors with hostile intent, including those committed and motivated activists, willing to pursue their political, ideological, or environmental cause through illegal rogue drone direct action [43]. Despite the amplification of countersurveillance and counter hostile reconnaissance measures, all in authority must acknowledge that the widespread availability and technical capability of drones ensures their permanence as a rogue reconnaissance security threat that requires a detected and determined response. Organized crimes, which undermine local and national economies, destroy the environment, and jeopardize the health and well-being of the public, will be increasingly facilitated by the use of drones, and, until the paradigm of high profits and low risks is challenged, organize crime will continue to reap the rewards of their illegal activities [44]. As organized crime groups embrace new and emerging technologies to develop their enterprise, the use of drones with their increasing payload capacities will further facilitate the commission of crimes, becoming a regular feature across the landscape of criminal investigations.

The new era of global international terrorism and the sudden rise of nationalist terrorist atrocities reveal with alarming regularity that terrorist plotters achieve their intended objectives, defeating all of the states' security measures put in place at the time. Unfortunately, this pattern is not set to change; governments across the world will prevent further terrorist atrocities, but there is a very strong likelihood that they will not stop them all. In the light of that conclusion, all in authority must dedicate themselves to increasing their knowledge and understanding of counterterrorism and the new threat vector of the deadly and determined terrorist use of drones. The adaption of drones to commit all manner of cyber-related crimes and security breaches is the latest cyber threat to emerge, brought about by the combination of advancements in UAV technology and the unlimited creativity of actors with hostile intent. Taken together, the malevolent use of drones to disrupt, damage, and destroy provides a complex and challenging threat landscape. The security challenges posed by the nefarious use of UAV technology are not insurmountable, but will require a determined response. To mitigate rogue drone risks, all in authority would be wise to learn that responding to the threat of drones is ineffective without fully understanding the threat landscape through increasing knowledge

of drone and counter-drone technologies, alongside assessing motivations from hostile actors and specific risks and vulnerabilities of their intended target. To defeat all manner of rogue drone threat vectors, the procurement and deployment of appropriate equipment are required, combined with the integration of that equipment into a comprehensive and coherent counter-drone strategy that is synchronized with existing security operations, and embedded within the very culture of resilience planning.

References

[1] HM Government, *UK Counter-Unmanned Aircraft Strategy*, October 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf.

[2] Prince, L., "Kentucky Man Arrested After Shooting Down Neighbor's Drone," *NBC News*, August 1, 2015, https://www.nbcnews.com/news/us-news/not-my-backyard-man-arrested-after-shooting-drone-down-n402271.

[3] Vincent, J., "Judge Rules Kentucky Man Had the Right to Shoot Down His Neighbor's Drone," *The Verge*, October 28, 2015, https://www.theverge.com/2015/10/28/9625468/drone-slayer-kentucky-cleared-charges.

[4] U.K. Government, "Public Dialogue on Drone Use in the UK: Moving Britain Ahead," Department for Transport, December 21, 2016, https://www.gov.uk/government/publications/drone-use-in-the-uk-public-dialogue.

[5] BBC News, "Coronavirus: Northamptonshire Police Could Use Drones," March 23, 2020, https://www.bbc.co.uk/news/uk-england-northamptonshire-52004297.

[6] Holroyd, M., "Coronavirus: Italy Approves Use of Drones to Monitor Social Distancing," *Euronews*, March 23, 2020, https://www.euronews.com/2020/03/23/coronavirus-italy-approves-use-of-drones-to-monitor-social-distancing.

[7] McGee, P., and K. Stacey, "California Police to Use Drones to Patrol Coronavirus Lockdown," *Financial Times*, March 20, 2020, https://www.ft.com/content/c7d0dee1-6125-475c-9cc7-78f4671d7cea.

[8] Hope, A., "Privacy Concerns over Surveillance Drones Used in Monitoring Social Distancing," *CPO Magazine*, April 20, 2020, https://www.cpomagazine.com/data-privacy/privacy-concerns-over-surveillance-drones-used-in-monitoring-social-distancing/.

[9] American Civil Liberties Union of Connecticut, "About Us: American Civil Liberties Union of Connecticut," 2020, https://www.acluct.org/en/about/about-us.

[10] Samuel, K., "Rethinking Counter-Drone Management: The Need for a Resilience Solution," *Defence iQ,* February 1, 2020, https://www.defenceiq.com/cyber-defence-and-security/articles/rethinking-counter-drone-management-the-need-for-a-resilience-solution.
[11] BSI, "Organizational Resilience: Harnessing experience, embracing opportunity. Executive Summary," November 25, 2015, https://www.bsigroup.com/globalassets/Global/revisions/Org-Resilience-Exec-summary2--FINAL-25Nov15.pdf.
[12] Malik, Y., "Counter-Drone System Procurement Training," *Defence iQ*, March 2020, https://www.defenceiq.com/events-countering-drones/.
[13] Omand, D., *Securing the State*, London, U.K.: C Hurst & Co., 2010.
[14] Markarian, G., and A. Staniforth, "Counter-Drone Detection, Evaluation, Identification and Neutralisation Training," Rinicom Ltd. and Saher-UK Ltd., 2020. Available at: https://rinicom.com/wp-content/uploads/2019/09/DeNI-Training-Brochure-MERGED-Updated-16.09.2019-ONLINE-.pdf (Accessed July 16, 2020)
[15] Levush, R., "Regulation of Drones: Comparative Analysis," The Law Library of Congress, 2016, https://www.loc.gov/law/help/regulation-of-drones/comparative.php.
[16] Abbott, C., et al., "Hostile Drones: The Hostile Use of Drones by Non-State Actors Against British Targets," Remote Control Project, Network for Social Change, Oxford Research Group, January 2016, https://www.openbriefing.org/docs/Hostile-use-of-drones-report_open-briefing.pdf.
[17] Department for Transport, "Taking Flight: The Future of Drones in the UK Government Response. Moving Britain Ahead," January 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771673/future-of-drones-in-uk-consultation-response-web.pdf.
[18] Jones, T., *International Commercial Drone Regulation and Drone Delivery Services*, RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR1718z3.html.
[19] UAV Coach, "Master List of Drone Laws (Organized by State & Country)," 2020, https://uavcoach.com/drone-laws/.
[20] ICAO DRONE ENABLE Symposium 2020, 2020, https://www.icao.int/Meetings/DRONEENABLE4/Pages/default.aspx.
[21] Franken, P., "EU Drone Regulations for Dummies: An Explanation and Implications for Drone Service Providers," *Terra Drone*, April 26, 2019, https://terra-drone.eu/en/articles-en/eu-drone-regulations-explained-for-dummies/.
[22] European Commission, "European Commission Adopts Rules on Operating Drones," May 24, 2019, https://ec.europa.eu/transport/modes/air/news/2019-05-24-rules-operating-drones_en.
[23] European Union Aviation Safety Agency, "EASA Publishes First Rules for Safe Drone Operations in Europe's Cities," April 6, 2020, https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-publishes-first-rules-safe-drone-operations-europe's-cities.
[24] Doffman, Z., "Warning over Terrorist Attacks Using Drones Given by EU Security Chief," *Forbes*, August 4, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones/#4bcb380d7ae4.

[25] Department for Transport, "New Powers for the Police to Enforce Drone Laws," January 27, 2020, https://www.gov.uk/government/news/new-powers-for-the-police-to-enforce-drone-laws.
[26] European Commission, "DroneWISE: ISFP-2019-AG-PROTECT – SEP-210640116," Directorate-Migration and Home Affairs, International Security Fund – Police, Brussels, 2019.
[27] Scott, G., and T. Smith, "Disruptive Technology: What Is Disruptive Technology?" *Investopedia*, March 21, 2020, https://www.investopedia.com/terms/d/disruptive-technology.asp.
[28] Haidt, J., and D. Wilson, "The Grand Theory of Business from Charles Darwin," *Forbes*, October 11, 2013, https://www.forbes.com/sites/darwinatwork/2013/10/11/the-grand-theory-of-business-from-charles-darwin/#1a6237846528.
[29] Schonfeld, J. J., "Innovation and Leadership – Guide for an Innovative Eco-System," *Politie*, Dutch National Police, 2015.
[30] Pietsch, B., "Global Drone Market Estimated to Reach $14 Billion over Next Decade: Study," *Reuters*, July 17, 2019, https://uk.reuters.com/article/us-usa-security-drones/global-drone-market-estimated-to-reach-14-billion-over-next-decade-study-idUKKCN1UC2MU.
[31] Europol, *European Union Terrorism Situation and Trend Report 2019*, June 27, 2019, https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat.
[32] European Commission, "Internal Security Fund – Police: Union Actions," Directorate-Migration and Home Affairs, 2020, https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions_en.
[33] University of Applied Sciences for Public Administration in Bavaria, "Study in Hof –Presentation of the University of Applied Sciences," 2020 https://www.aiv.hfoed.de/en/international/study-in-hof.html.
[34] European Institute, "Profile of the European Institute," 2020, http://www.europeaninstitute.bg/en/page.php?c=14.
[35] Center for Security Studies (KEMEA), "Welcome to KEMEA," 2020, http://www.kemea.gr/en/kemea/about-kemea.
[36] RiniGARD Smart Technology, "About Us," 2020, https://rinigard.com/.
[37] Saher Europe, "Welcome to Saher Europe: Research, Training, Consultancy," 2020, http://www.saher-eu.com.
[38] Velika Gorica, University of Applied Sciences, "Welcome to the University of Applied Sciences, Velika Gorica," 2020, https://www.vvg.hr. In Croatia.
[39] National Aerospace Technology Programme (NATEP), "NATEP Project DENI at SCTX2016," 2016, http://www.natep.org.uk/SCTX2016.
[40] Rinicom and Saher, "DeNI (Detection, Evaluation, Neutralisation and Investigation) Training Course: Countering Rogue Drones Training," 2019, https://rinicom.com/wp-content/uploads/2019/09/DeNI-Training-Brochure-MERGED-Updated-16.09.2019-ONLINE-.pdf.
[41] Rinicom, "DeNI Rogue Drone Training Course," 2019, https://rinicom.com/drone-detection/deni-rogue-drone-training/.
[42] Malik, Y., "Counter-Drone System Procurement Training," *Defence iQ*, March 2020, https://www.defenceiq.com/events-countering-drones/.

[43] Johnson, J., "Heathrow Protest Thwarted as Police Use Radiowaves to Jam Extinction Rebellion Group Drones," *The Telegraph*, September 13, 2019, https://www.telegraph.co.uk/news/2019/09/13/two-arrested-within-grounds-heathrow-extinction-rebellion-group/.
[44] Global Financial Integrity, "Executive Summary: The Retail Value of Transnational Crime," March 2017, https://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final-_exec-summary.pdf.

About the Authors

Garik Markarian is the Emeritus Professor of Lancaster University, Lancaster, United Kingdom, and the chief executive officer and founder of Rinicom Ltd., a Lancaster, U.K.-based small and medium enterprise (SME) specializing in intelligent solutions for security, military, and first-responder applications. Over his long professional career, he successfully combined academic research with the practical and commercial implementations of the results of his research. He actively contributed to DVB-DSNG, DVB-S(2), DVB-RCS, IEEE802.16a/d/e/m, and EUROCAE standards where he chaired a number of committees and provided technical contributions that are incorporated into these standards. Professor Markarian is a Fellow of National Academy of Sciences in Armenia, and he has also acted as the chairman of the IET Professional Panel on Communications and as a member of the U.K. Government Advisory Committee on Measurements in Emerging Technologies. He has coauthored over 400 publications, including 4 textbooks and 42 national and international patents.

Andrew Staniforth is the director of innovation at Saher-Europe, a security research and training consultancy operating at a global level. As an international security and innovation expert and a former Special Branch intelligence officer and counterterrorism police detective, he has supported missions of the United Nations Terrorism Prevention Branch. As a qualified teacher, he has designed international multi-agency security exercise programs and has delivered training to senior police commanders from across the world. As a senior research fellow and visiting lecturer, he has held academic positions at leading research institutes and is the author, coauthor, editor, and coeditor of a number of security-related books. Andrew leads the Saher-Europe coordination of the Detection, Evaluation, Neutralisation and Identification (DENI) counter-UAV training program. He is an expert

evaluator for the European Commission security research and innovation programs for cyber security and disaster resilience and is a regular contributor of articles to defense, security, and policing magazines.

Index