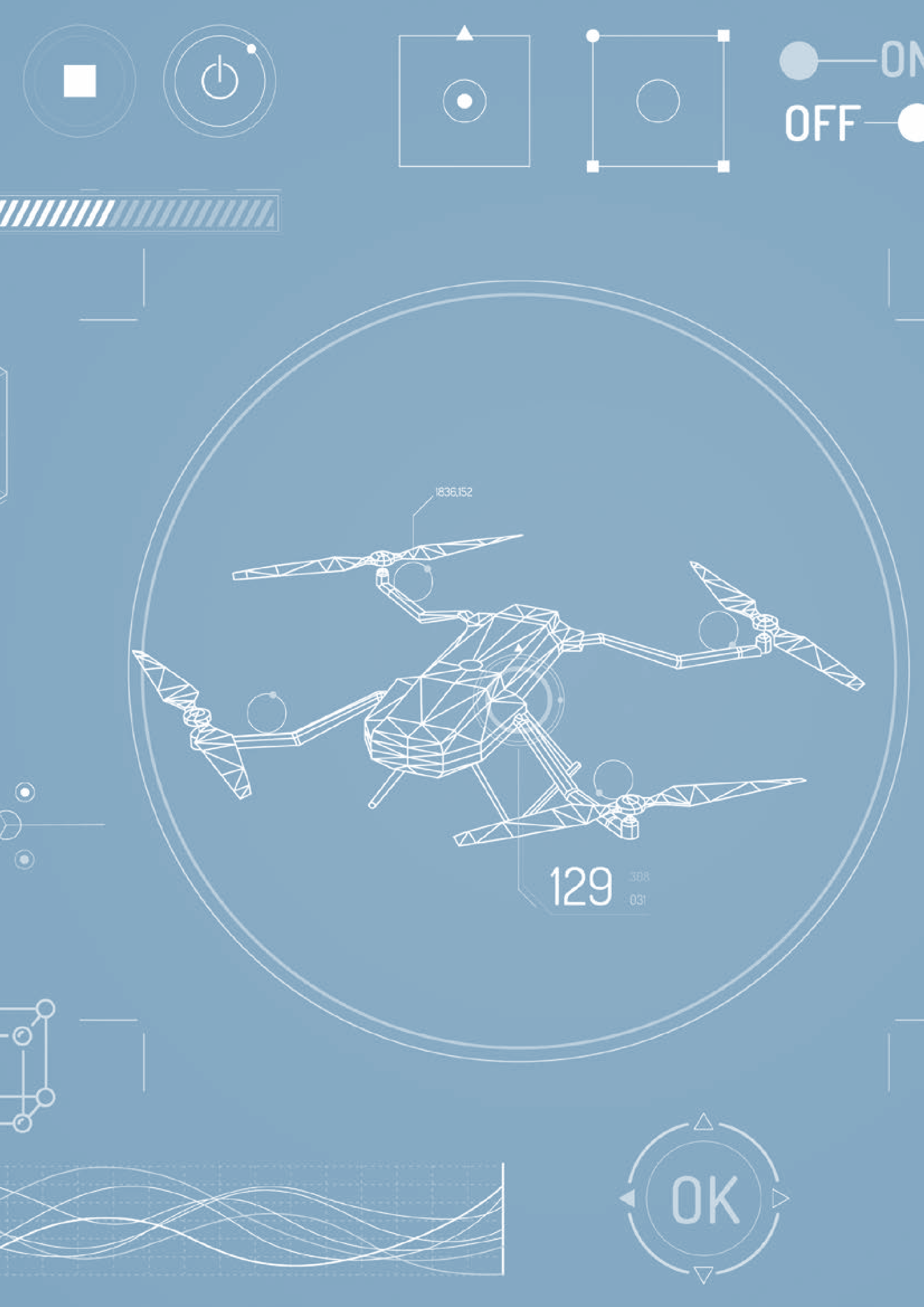
Preparing for Hostile Drones in Urban Environments

Report 2024

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK



ON
OFF
1836,152
129
308
031
OK

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK

www.london.gov.uk/ctpn

Contributors and Reviewers

Christopher Church
Senior Forensics Specialist (Counter Drone)
International Criminal Police Organisation (INTERPOL)

Valerio Liberatori
Policy Officer (Counter Drone)
European Commission – DG HOME Counter Terrorism Unit

Garik Markarian
Emeritus Professor
School of Computing and Communications
Lancaster University

Khalil Otmane
Programme Manager
Autonomous and Remotely Operated Systems Programme
United Nations Office of Counter Terrorism

Mike Paterson
Counter Drone Expert
National Police Chiefs Council
UK Counter Terrorism Policing Headquarters

Project Stadia
Safe and Secure Major Events
International Criminal Police Organisation (INTERPOL)

Andrew Staniforth
DroneWISE Training Coordinator
(EU Internal Security Fund Project)
Co-Author of *Countermeasures for Aerial Drones Handbook*

Alex Townsend-Drake
Head of Programme (Lead Author and Editor)
Counter Terrorism Preparedness Network

Kris Wright and Paul Monk
Chief Superintendent and Detective Superintendent
Protective Security Operations
Metropolitan Police Service

1 Introduction

> **The threats posed by drones transcend borders, and fuse the physical and digital. They remain a priority for protection and preparedness at national and city levels.**

The United Nations (UN) General Assembly has adopted a resolution on the eighth review of the Global Counter Terrorism Strategy. This makes references to vulnerable targets, including critical infrastructure and public places. It calls upon Member States to strengthen efforts to improve security and enhance resilience against terrorist attacks, particularly in civil protection.[1] The need to continuously enhance protective security and preparedness remains a priority at all levels.

This is pertinent within cities or complex urban environments – geographical footprints with a mass of people, industry and infrastructure that intersect across interdependent layers of structures, systems and services. They are often defined by their urban extent (the spread of built-up structures) and/or degree of urbanisation (the local population living within the city's boundaries).[2]

The concept of a safe and secure city is, therefore, one that is riddled with risks and vulnerabilities that demand a comprehensive, multi-agency approach to mitigate, minimise and manage these. Central to this is protective security: a set of measures and strategies designed to safeguard individuals, assets, information and organisations from various threats.

This protective security would include the protection of public figures (e.g. royalty, politicians, celebrities or other protected persons), critical infrastructure (e.g. government facilities, transport, power stations, hospitals and data centres), as well as events and crowded places or other vulnerable targets (e.g. schools, shopping centres, restaurants and hotels).

These are all context-dependent and subject to assessments that determine the level and duration of protective security required. For static sites, a layered and integrated approach involving access control, surveillance, trained security personnel, crowd-management tactics and barriers for hostile vehicle mitigation may be applied. For mobile convoys or widespread events, there may be an increase in overt or covert operatives and security personnel, the installation of temporary surveillance cameras, the strategic deployment and use of specialist resources, as well as additional security measures at key locations. The Counter Terrorism Preparedness Network (CTPN) report *"Protecting Major Events and Crowded Places"*[3] explores some of these considerations.

Yet the landscape is becoming increasingly complex because of rapid evolutions in technology that fuse the physical and digital. The threats posed by cyber-attacks, artificial intelligence (AI), deep-fake manipulation, biometric data and general advances in computing are compounded by society's dependence upon the internet and technology. Cyber-attacks, for example, can manifest with real-world implications, as highlighted by the CTPN report *"City Preparedness for Cyber-Enabled Terrorism"*.[4]

The report touched upon the link between cyber, AI and drones, which are widely recognised as pressing security concerns. The UN Security Council has also acknowledged the drone threat, noting a need to prevent the flow of weapons including drones and their components to and between the Islamic State of Iraq and Syria (ISIS) and Al-Qaida (AQ), their affiliates or associated groups, as well as other illegal armed groups and criminals.[5]

The threats posed by drones transcend borders, and fuse the physical and digital. They remain a priority for protection and preparedness at national and city levels, creating an increasing need for robust policies and procedures; the enhanced capability and capacity of organisations; the development of expert knowledge and operational training; and multi-agency arrangements. There is an onus upon public authorities to prepare, and that is the focus of this report.

The landscape is becoming increasingly complex because of rapid evolutions in technology that fuse the physical and digital.

2 Terminology

> **The term "drone" has become commonplace for explaining "an aircraft that can operate in an automated manner or be piloted remotely without human presence on or in the aircraft".**

The term "drone" has become commonplace for explaining "an aircraft that can operate in an automated manner or be piloted remotely without human presence on or in the aircraft".[6] These are also referred to as unmanned aircraft systems, uncrewed aerial systems, uncrewed aerial vehicles and remotely piloted aerial systems. Different terminologies are used in different contexts.

The current position of the International Civil Aviation Organization and the UN is that the preferred term is unmanned aircraft systems (UAS) or counter(C)-UAS.[7] This takes into account the complete system (vehicle, controller, operator, communication systems, etc.). However, on 18 October 2023, the European Commission adopted "drone" and "counter drone" as agreed terminology.[8] This report follows this decision to support understanding, accessibility and readability.

It is, however, important to recognise that the broader term "drone" can also apply to those that are water-surface, underwater or ground-based, or even operated in outer space, which are beyond the scope of this report. This report is only concerned with aerial drones.

On this basis, the focus is on preparing for hostile drones in urban environments. This report reflects on the evolution of drones and how this applies to domestic settings; reviews the current and potential threats posed; and draws upon existing guidance to distil considerations around the protective security and multi-agency preparedness needed to counter and respond to hostile drones. It concludes with key considerations and recommendations for cities and their authorities.

Although the current domestic threat of the use of drones by terrorists is viewed as relatively low, the potential for this to increase through small off-the-shelf drones or as technologies and terrorist tactics continue to evolve should be considered.

This report:

1. Reflects on the evolution of drones and how this applies to domestic settings.
2. Reviews the current and potential threats posed.
3. Draws upon existing guidance to distil considerations around the protective security and multi-agency preparedness needed to counter and respond to hostile drones.

3 The Rise of Drones

> “There could be more than 900,000 drones in UK skies by 2030... drones could contribute an extra 45 billion GBP in gross domestic product to the UK economy and provide 650,000 jobs.”

Drones have been around for decades but, until recently, they have been a weapon of war reserved for specialist military operators. Now recreational and commercial drones are common, as well as bespoke drones where component parts can be purchased individually and put together.[9] Today, a reliable drone can be purchased for less than 100 GBP, and learning to operate it can take minutes.[10]

Drones continue to proliferate at an alarming rate. A study by PricewaterhouseCoopers (PwC) estimated that there could be more than 900,000 drones in UK skies by 2030. It also states that drones could contribute an extra 45 billion GBP in gross domestic product to the UK economy, provide 650,000 jobs and reduce carbon emissions by 2.4 million tons in the same timeframe.[11]

Indeed, drones can be used for services from media to agriculture to search and rescue, as well as topographical mapping, inspections, monitoring and surveillance. Commercially, companies like Amazon are also exploring how drones could be utilised for deliveries, announcing that it will start using drones to deliver parcels.[12] In the UK, a “superhighway” is being considered to support drone deliveries by air.[13] This would revolutionise logistics. Singapore is also exploring the use of drone technology to develop air-based taxis.[14,15]

The US Department of Defense's Advanced Research Projects Agency (DARPA) is otherwise working on a project that would enable commercial drones to fly missions autonomously even if operator connectivity is lost or disrupted.[16]

Advances in drone technology (such as longer flight times, improved camera systems, obstacle-avoidance systems and carrying capabilities) continue to expand their potential uses. This offers many benefits and opportunities but also creates widely recognised threats and challenges.

Aside from concerns as to how drones can use airspace without endangering crewed aircraft, the European Commission highlighted the potential for misuse. It revealed that drones "can be used to breach privacy rules, for espionage by using camera technologies, to hijack telecommunication signals and, in combination with biological or chemical agents, explosives or other weapons, they can harm persons, disrupt services and damage infrastructure".[17]

The newly adopted European Commission communication on countering potential threats posed by drones highlights the potential use of drones for terrorist attacks.

It notes how the number of drones in the European Union is "set to grow significantly in the coming years, and they will improve greatly in terms of speed, agility, maximum range, payload capabilities, precision of sensors and use of artificial intelligence".[18]

For this reason, the European Commission has developed various related guidance or handbooks.[19,20,21] These concerns are endorsed by the UN[22] and highlighted by INTERPOL, which has released its *"Framework on Responding to a Drone Incident"*.[23] This is further evidenced through countless counter drone legislation and strategies.[24,25,26,27]

4 The Use of Drones in Warfare

> Militaries have embraced drones because of the advantages and efficiencies they offer in conflict… and the role they can play in surveillance and air strikes.

A BBC article highlighted drones as a new era in warfare, compounded by public-private relationships that drive the market.[28] Militaries have embraced drones because of the advantages and efficiencies they offer in conflict (e.g. remote command, relatively low cost, small size, no human pilot etc.) and the role they can play in surveillance and air strikes.[29]

This use of weaponised drones has been evident in the Russia–Ukraine (where both sides started off with commercial off-the-shelf drones and moved quickly to building their own) and Israel–Hamas conflicts. The use of drones in conflict zones is nothing new, as observed during operations in Libya, Syria, Iraq and Afghanistan, where the US military's Predator and Reaper drones dominated remote warfare. These drones were enabled with long-range data transmission, innovative computation technology, advanced video relay and high-tech guided missiles, which allowed the US to deploy force globally without putting any allied military lives at risk.[30]

Military-grade drones now have unprecedented speed and range, with increasingly impactful and accurate weapon capabilities. This type of technology enabled the US to neutralise AQ leader Ayman al-Zawahiri in 2022.[31]

The use of drones has inspired terrorist groups such as ISIS, Hezbollah and Hamas.

However, such drone capabilities are not confined to the West; a sophisticated attack against two of Saudi Arabia's largest crude oil plants was carried out by drone. This attack knocked out half the Kingdom's oil production and was believed to be linked with Iran.[32,33]

The NATO Review referred to the "second drone age" in which "all competitors, from peers to terrorists and non-state actors, are including drone technologies in their standard tactics and concept of operations".[34] This nods to the importance of preventing and countering weapon flows.

It is no surprise that the use of drones has inspired terrorist groups such as ISIS, Hezbollah and Hamas. The fact that ISIS has been using consumer and recreational drones to plan, prepare and execute battlefield attacks since 2017 puts the threat into perspective.[35,36]

A 2018 report by the Combating Terrorism Center at West Point charted the use of drones by ISIS, noting the organisation was "able to build and deploy a fleet of attack, bomb-drop capable drones and achieve moderate impacts because the group found gaps… to source commercial drones, and related components".[37] These low-cost drones have been used to take out multi-million-pound pieces of war equipment, meaning the risks and costs between state forces and non-state actors are severely unbalanced.

ISIS has conducted hundreds of armed aerial attacks and guided vehicle-borne improvised explosive devices towards their targets by using off-the-shelf drones.[38] It is reported that ISIS can release smaller munitions with considerable accuracy, and the terrorist group has promoted this capability online.[39] ISIS has also targeted aid workers with drones carrying 40mm rifle grenades and used drones as bait.

In one case, an ISIS drone was detonated while being examined, killing two Kurdish military personnel and injuring two French special forces operatives.[40] The drone had been modified into an improvised explosive device (IED) that detonated when disassembled. The UN has referred to the malicious use of drones more broadly, including the use of mini-drones by Al-Shabaab in Somalia.[41]

The Houthi movement, officially known as Ansar Allah, is a Shia Islamist political and military organisation that also has a track record of using drones. Within Saudi airspace, it has mounted successful attacks on a variety of targets. In January 2019, it used a drone to detonate 80kg of explosives at a Yemeni military parade, killing six soldiers and injuring many others. It subsequently used an armed drone as part of a strike on a military camp that killed 36 people.[42] In 2022, a kamikaze drone hit a church in Hama, Syria, leaving two dead and more than a dozen injured. Syrian jihadist group Hayat Tahrir al-Sham is believed to have been behind the attack.[43]

> **ISIS has conducted hundreds of armed aerial attacks and guided vehicle-borne improvised explosive devices towards its targets by using off-the-shelf drones.**

In December 2023, a British warship also shot down a drone in the Red Sea. Yemen's Houthi rebels "have targeted foreign ships in the area since the start of the Israel-Hamas war. They have declared support for Hamas and have said they were targeting ships travelling to Israel".[44,45]

This continued in January 2024, when US and British naval forces shot down 21 drones and missiles fired by the Houthis towards the southern Red Sea as the ships protected these international shipping lanes. British Defence Secretary Grant Shapps said this was the largest attack in the area by the militants to date, as the war between Israel and Hamas in Gaza spills over into other parts of the Middle East.[46]

There are multiple examples of drones being used as weapons in conflict whether by states, terrorist groups or other non-state actors, and there are others at play including serious organised crime. The fact that drone technology and products transcend borders and can be operated from a distance with a degree of anonymity compounds the issue, adds extra complexity and accelerates domestic security concerns.

Major General Sean Gainey, Director of the Pentagon's Joint Counter-Unmanned Aircraft Systems Office, said, "Globally, we're seeing the threat continue to grow, and you'll see a range of employment of that threat from large to small amounts, depending on where you are".[47] Indeed, drones have changed the character of warfare, offering a low-cost and a high-reward potential.[48]

General McKenzie, former Commander of US Central Command, flagged the urgency of the situation by highlighting how commercially available small drones, coupled with a lack of dependable, networked capabilities to counter them, is the most concerning tactical development since the rise of the IED.[49] Ultimately, this is an uncontrolled and fast-developing technology moving within various legal frameworks and practices with complex ethical questions.[50]

Given the popularity of cheap, commercial alternatives to military drones, countries need to adopt a holistic approach to countering them.[51] Therefore, this is a particular security concern domestically,[52] where the use of drones by terrorists represents a threat.[53]

That is the core of this report. That is what the threat could look like, how it could evolve and how this could be countered through protective security measures and multi-agency preparedness and response.

5 The Domestic Threat of Drones

> “Commercially available small drones, coupled with a lack of dependable, networked capabilities to counter them, is the most concerning tactical development since the rise of the IED.”

Drones have caused a mix of safety, security and privacy concerns. These include crime and unauthorised surveillance; use during protest activity; risks towards other crewed and uncrewed aircraft in the same airspace; and malicious use (such as by hostile states and terrorists). They can be used to carry hazardous loads; for smuggling and propaganda; to cause disruption and interference; to gather intelligence through surveillance; and to cause jamming and cyber-attacks.[54]

The use of drones for crime is growing. In France, two men were arrested for reportedly using a drone to enter the air vent of a Caisse d’Epargne bank and open the door to access the ATM’s cash box and steal around 134,000 euros.[55] Other examples include a drone with traces of radiation landing on the Japanese Prime Minister’s residence[56] and an assassination attempt against President Nicolás Maduro in Venezuela via two commercial drones carrying explosives.[57]

Drones have become popular for smuggling contraband into prisons and across heavily secured borders. There have been sightings of drones over sensitive facilities, such as a submarine base in Washington State and nuclear facilities in France and Sweden. Moreover, the ever-present risk of disruption to airports persists.

In 2018, a drone impeded airspace at Gatwick Airport and grounded flights for more than 36 hours, leaving hundreds of thousands of passengers stranded and costing airlines an estimated 60 million US dollars.[58,59] Greenpeace also used a drone to drop a smoke bomb onto a nuclear-material storage building.[60]

The threats posed by drones are diverse, and trends show a significant increase in drone ownership and sightings. There are ample ideas and videos online showing how drones can be used and modified. This amplifies the likelihood that they could be used for malicious purposes, including by terrorists to carry out an attack, whether directly or indirectly. With relatively simple modifications, consumer drones can be converted into rudimentary yet potentially lethal weapons.

As Paul Scharre, Director of Studies at the Center for New American Security, stated, “Commercial drone technology is so widely available that anyone could build a crude DIY attack drone for a few hundred dollars, and some terrorist groups have”.[61]

There have long been warnings about terrorists planning to release chemical agents over urban areas and stadia.[62] Several terror plots involving the use of drones have been foiled,[63,64] and authorities have disrupted a number of schemes to use drones for various kinds of attacks.[65] The sentencing of a jihadist by a Spanish court in October 2022 for planning to attack a stadium during a major football match using a drone is a case in point.[66,67,68]

The Christchurch attacks in New Zealand were also planned with help from a drone.[69,70] Additional examples include the sentencing of a Belgian citizen for attempting a bomb attack using drones against a prison[71] and the conviction of a PhD student in the UK for designing and building a drone for terror group ISIS that was capable of delivering a bomb.[72]

The UN “*Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes*” noted how “terrorism has become notably more diffuse and diverse in nature, aided in part by the adoption of new and emerging technologies”.

The UN identified:

1. More terrorist groups have developed drone capabilities.
2. Some terrorist groups are seeking to identify new avenues for acquisition and advancement of drone capabilities.
3. Some terrorists groups are sharing technology and training on the use of drones.
4. The use of drones by terrorist groups continues to proliferate globally.[73]

The European Commission endorses the findings of the UN report by noting how innovation, coupled with ease of access to drone technology, means the targeting of public spaces, individuals and critical infrastructure is likely to increase.[74,75]

Driving factors include:

- the unregulated and increasingly sophisticated civilian market for drone technology;
- the wide availability of unregulated, uncontrolled and unsecured explosives, which can be used as payloads on drones;
- access to explosive precursors; and
- the availability and transferability of technical expertise.[76]

This is expanded on the next page.

Open market availability

A variety of drones can be purchased in stores or online. The market will become saturated with options as technology companies compete. Ongoing collaborations or competition in this space will bring down the unit cost of technologies. As relative prices are driven down, barriers to entry will erode, and the acquisition of drones will increase. This diffusion of drones – and wider technologies – means they will spread to regions, cities and local areas.[77]

Generational shifts in expertise

As more and more people learn and understand how to operate and fly drones, the devices will become normalised in day-to-day life. They will go from being a novelty or specialist tool to one that can be used by many for multiple means.

Visibility of global events

The role of drones in conflict zones is widely reported. It is now a standard military capability for both allied and hostile states, which serves as inspiration for non-state actors including terrorists (see previous section) and returning foreign fighters.

Technological capability

Criminals are already using drones to drop payloads, contraband and propaganda (including radicalisation material) into prisons. States and terrorists are already using them as weapons. As technology continues to develop and become increasingly integrated, drones' capability to carry larger payloads or more complex weaponry will advance, as will the accuracy of their delivery. Sleeper drones that can deploy to a location then "sleep" or "hibernate" for long periods before attacking are also emerging.

Opportunity and intent

Drones can be operated remotely, providing a degree of anonymity for the user. They can also be flown (whether legally or illegally) into vulnerable areas, sensitive sites or otherwise hard-to-reach locations if security measures can be bypassed or stalled. With intent, the drone is a unique weapon, and it only needs a short time to deliver a malicious act.

The average air speed of a consumer drone is 40–70mph, meaning that, even at the lower end, it could cover one mile in 1.5 minutes. The continued growth in use and evolution in associated technology means that the threats are evolving. "Improved batteries and engines will permit longer flight times with increased payloads while faster mobile networks (5G) will allow for long-distance communication, and artificial intelligence applications can be used to enhance cooperation… so they can form swarms."[78]

Swarms of multiple drones and the prospect of autonomous flights and weaponry using AI present a step that could overwhelm counter measures.[79] A report, *"The Vulnerabilities of the Drone Age: Established Threats and Emerging Issues out to 2035"*, specified drone swarms, autonomy and AI as future threats. It also highlighted how the proliferation of land, air, sea and underwater drones will expand the domains and dimensions of drone threats.[80]

Indeed, AI risks becoming a tool that can automate specific tasks, such as programming commercially available drones to target individuals (through facial recognition), ethnic groups or specific locations/infrastructure.[81,82] It enables drones to process their surroundings, make real-time decisions while flying, and provide instant feedback to the pilot.[83] As such, drones already have some level of autonomy – they can fly, hover or navigate without human input. They can be automated and autonomous. For now, most drones are remotely piloted and/or automated rather than autonomous, but this is likely to change over time. These will be uncharted waters.[84]

The domestic threat of drones, therefore, presents a current and potential threat profile that poses considerable challenges for authorities. Although the current domestic threat of the use of weaponised drones by terrorists is viewed as relatively low, the potential for this to increase – either through small off-the-shelf drones, or over the next five to 10 to 15 years as technologies and terrorist tactics continue to evolve, is real.

> **Swarms of multiple drones and the prospect of autonomous flights and weaponry using AI present a step that could overwhelm counter measures.**

Moreover, the threat posed by drone technology involves not just weaponry but enhanced surveillance capabilities too. Cameras attached to drones can already conduct pre-emptive reconnaissance or be used to monitor and livestream attacks.

Countering this threat must involve preventing and mitigating against hostile drones and detecting and deterring them. However, developing a truly effective solution will require a nuanced and reactive approach. As the Director of the US Defense Threat Reduction Agency said, "This threat is evolving… this is going to be a continuing challenge due to the adaptive nature of the problem of being able to use small drones in so many different ways."[85]

This is endorsed by EUROPOL's "*EU Terrorism Situation and Trend Report*", which notes that drones enable terrorists to carry out attacks remotely, magnifying their impact. It also states that such weapons are expected to become more accessible, traded anonymously online or provided by criminal actors.[86]

Protecting Against Hostile Drones at Specific Sites

> “A useful way to understand the risk of attack is to consider targetability, vulnerability, threat and criticality.”

Countering and managing the threat of hostile drones is complex, requiring well-resourced and trained teams of experts and specialist equipment working across protection, preparedness and response. Although most uncooperative drone incidents will be the result of careless, untrained or uninformed public use, the handful of hostile drones will demand more sophisticated solutions.

The higher the threat, the higher the required mitigation, solution and stakeholder engagement levels. Addressing the threat requires the development of a counter drone strategy.

This is about:

1. understanding the risks posed as informed by threat and vulnerability assessments;
2. determining what can be done to reduce the risk (both non-technical and technical);
3. ensuring that counter drone technology is appropriate, suitable and convenient; and
4. setting associated policies, procedures and rules of engagement to underpin actions and dovetail operational plans.

A useful way to understand the risk of attack is to consider targetability (attractiveness, exposure and access), vulnerability (specific weaknesses that influence how susceptible a place or system is to attack), threat (likelihood and modes of attack) and criticality (how serious the consequences of an attack could be).[87]

This approach offers a method to help set priorities; after all, it is impossible to protect everything all the time. It also shifts thinking towards critical infrastructure, transport hubs, major events and venues. This approach could be used to assess the risk of an attack on a stadium (targetability) where crowds must congregate at entrance gates

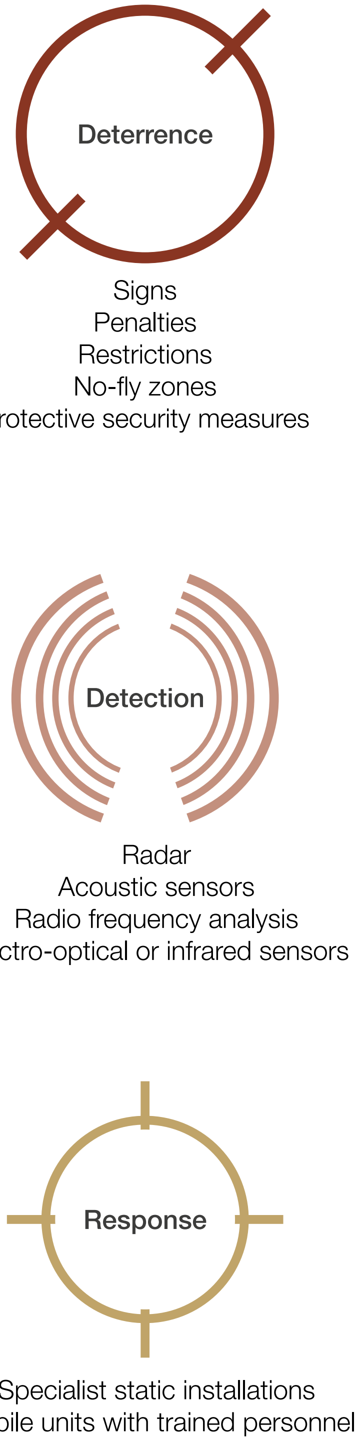
to show their tickets (vulnerability). A drone could drop an explosive device or spray a substance (threat), which could result in casualties, fatalities and secondary incidents or consequences, such as crowd stampedes and crushing (criticality).

To make a site secure, one option is to restrict the airspace. The national civil aviation authority could allocate that specified zone to a site owner, who would set rules for drone operations. Within the agreement, there would be authorisation for intervention in the event of uncooperative flights. The detail of any agreement would vary according to the country and local regulations. It is, therefore, important to include the regulating authorities in the design of such strategies.[88]

Investment in counter drone measures has also accelerated. “These may use radar, electro-optical/infrared, acoustic or radio frequency sensors to detect a drone’s physical, visual, thermal, audible or electromagnetic signatures. Once detected, the drone may be engaged via kinetic means (missiles, other drones, guns and nets) or non-kinetic means (measures that include electronic warfare, hacking or directed-energy pulses to jam, seize control of, or disable the drone).”[89] It is also possible to target the other elements supporting a drone or a drone operating system.

In some cases, for example if the drone is being used for criminal purposes or the hostile gathering of information, it may be necessary to secure and land it intact to allow for forensic investigation. This requires sophisticated cyber solutions that can take control over a drone’s operating system.[90,91]

Counter Drone Measures


Deterrence

Signs
Penalties
Restrictions
No-fly zones
Protective security measures

Detection

Radar
Acoustic sensors
Radio frequency analysis
Electro-optical or infrared sensors

Response

Specialist static installations
Mobile units with trained personnel

However, stopping a drone in mid-air is difficult at the best of times. Each operational environment will require different detection, tracking and identification capabilities. There are several commercial counter drone measures available on the market, but their claimed performance is often unsupported by evidence, and these systems can behave differently in different settings. “Some factors (such as weather conditions, terrain, rural or urban area, noise, where sensors are installed, or obstacles like high buildings) will affect the performance.” In other words, a system used in a desert setting would need to be different to one used in an urban area or a prison, for example.[92] Some detection systems can also give false positives or may be susceptible to attack.[93]

The inevitable evolution of drones will mean they may become more astute at navigating or overcoming counter measures. This leans towards counter drone systems with open architecture. This means it should be easier and therefore cheaper to integrate, add, change or replace hardware, software and components.

Identifying the right counter drone system is far more nuanced than the product’s specification. It requires on-site testing, installation and repeat testing to understand its true capability. Even then, it will have its limits and could be outsmarted by the attacking drone, especially when it is beyond visual line-of-sight, or the counter drone system is overwhelmed by a swarm. This means there may be significant variances between the performance and reliability of systems, which continue to lack maturity.[95] The UK National Protective Security Authority has been testing counter drone technologies against a technical standard since 2019. It offers guidance[96] as well as a Catalogue of Security Equipment to compare systems. However, it recommends that potential buyers develop an operational requirement before reviewing technologies; then look at what independent testing has been completed; and finally use this information to refine options to conduct their own in-situ operational testing.

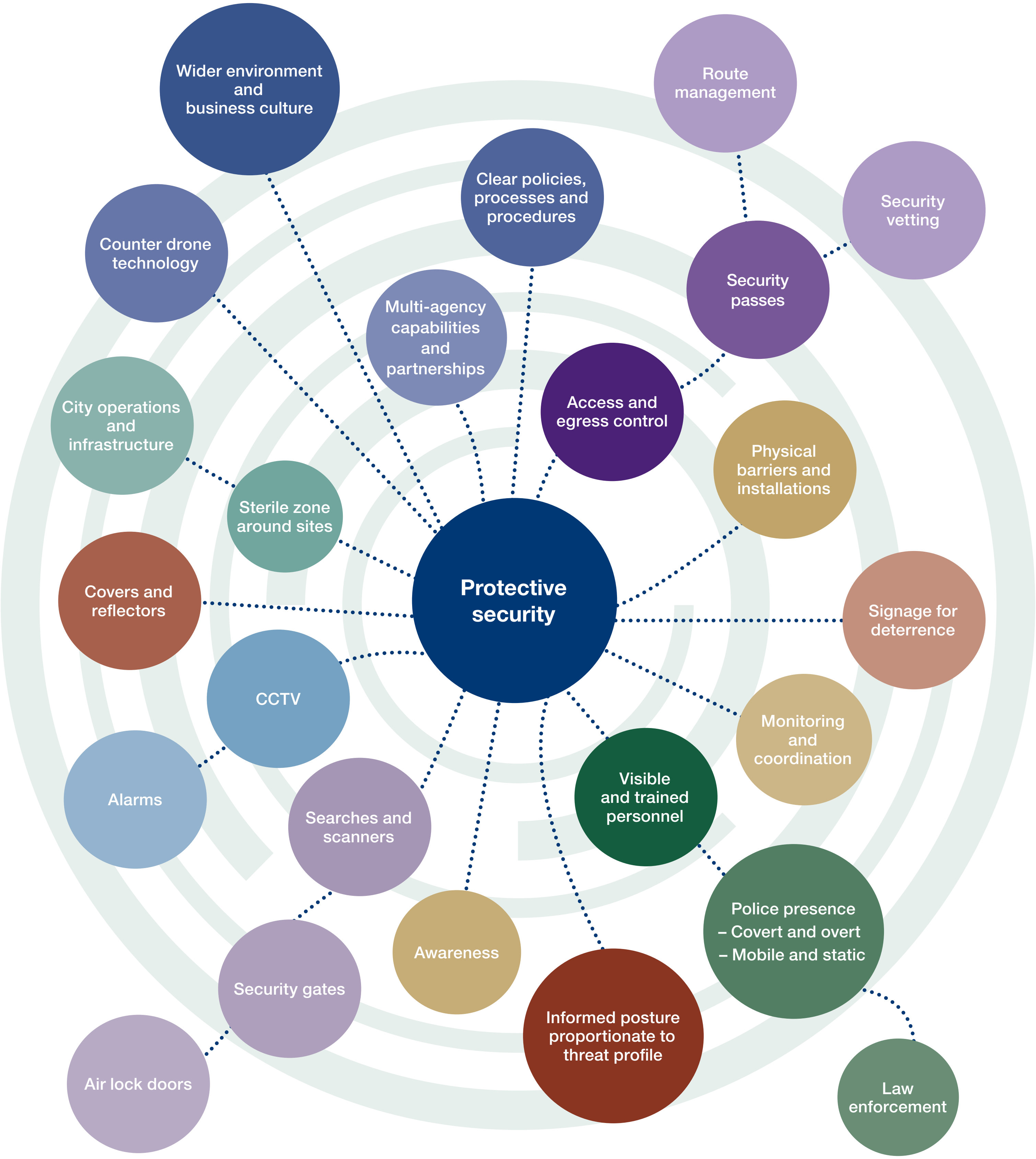
This type of comprehensive approach, potentially concluding with an exercise, is important. An INTERPOL exercise took place over three days at Oslo Gardermoen Airport to test and assess 17 counter measures, for example.[97] The European Commission funded Project COURAGEOUS also seeks to support this process by developing a standardised test methodology for drone detection, tracking and identification systems.[98]

Indeed, the European Commission has made major investments in drone and counter drone research projects in recent years. Projects include SKYFALL,[99] DroneWISE[100] and COURAGEOUS,[101] which bring together police and other government agencies across Europe, academia and the private sector. However, these types of initiatives need translating and implementing at a local level.

A UN-INTERPOL expert meeting emphasised the importance of having the right arrangements in place, with reference to the 2023 FA Cup Final where a drone pilot, who was reckless rather than malicious, was subsequently prosecuted for flying it in the event footprint.[102] There are countless examples of unauthorised drones entering airspace around stadia and causing disruptions. Following an incident in 2022, the US National Football League now has a policy to stop a game and clear the field if drones are spotted.[103] It is worth noting that the airspace around stadia may not be formally restricted, so there is a difference between a site not wanting drones to fly in/near its airspace and it being protected through legislation and laws. This is an important local consideration.

Attributes of counter drone systems with open architecture

1	ADAPTABILITY	The solution should have the ability to flex and apply to evolving requirements.
2	MODULARITY	The solution should consist of independently detachable components.
3	PORTABILITY	The solution should be moveable or transferable from one system to another.
4	SCALABILITY	The solution should be able to scale larger or smaller to meet needs.
5	INTEROPERABILITY	The solution should enable effective data sharing with other systems.[94]


Wider environment and business culture
Route management
Clear policies, processes and procedures
Security vetting
Counter drone technology
Security passes
Multi-agency capabilities and partnerships
Access and egress control
City operations and infrastructure
Physical barriers and installations
Sterile zone around sites
Protective security
Covers and reflectors
Signage for deterrence
CCTV
Monitoring and coordination
Visible and trained personnel
Alarms
Searches and scanners
Police presence
– Covert and overt
– Mobile and static
Awareness
Security gates
Informed posture proportionate to threat profile
Air lock doors
Law enforcement

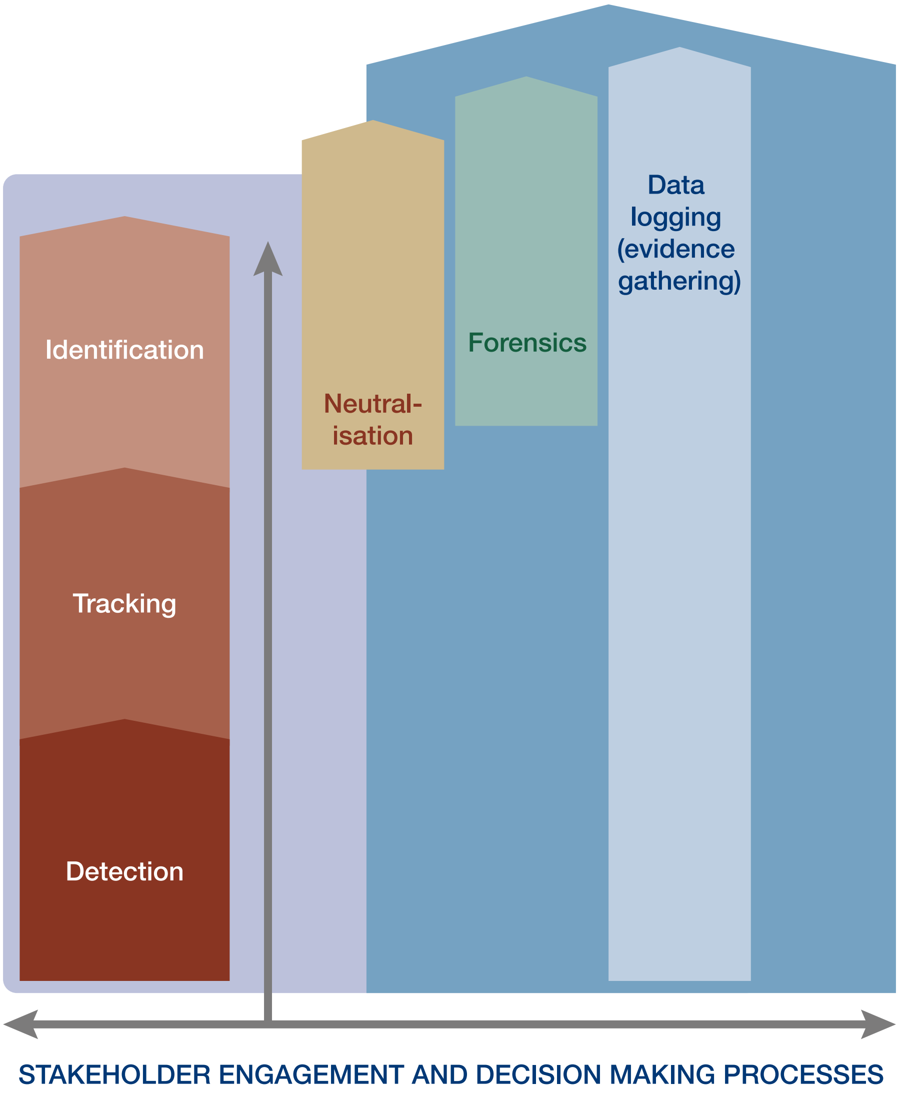
Stadia and sensitive sites, however, could employ simple measures like covers and reflectors to shield against drone activity. There are also several effector technologies available but these currently have significant limitations. Where the drones are using, for instance, 4/5G, satellite data links or pre-programmed navigation, signal disruptors are unlikely to be effective. Spoofing involves creating false signals to trick the drone into believing it is receiving legitimate commands but, given cost implications and local legal frameworks, such capabilities may be difficult to apply in practice.

The resourcing and staffing implications of using a specific technology also needs to be understood and considered as part of the whole system. Some systems require constant monitoring, while some can operate on a "distracted operator" basis, whereby attention only needs to be paid to the system when a specific incident occurs and an alert is raised. This will be an important factor when deciding which system to select for any given purpose. However, when the threat of drones in open urban environments (as opposed to specific static locations like stadia and airports) is considered, countering them becomes an even more significant challenge.

Geofencing is one option provided by certain counter drone manufacturers. This purports to be a virtual, invisible barrier that surrounds a specific area. It can be dynamically generated by the manufacturer (as in a radius around a point location) or match a predefined set of boundaries (such as school zones or neighbourhood boundaries). It can prevent drones from entering, flying within or taking off within restricted areas, or it can be used to alert the pilot to specific information relevant to that location.

However, the effectiveness of geofencing depends upon several factors, including the position location technology such as GPS (Global Positioning System), RFID (Radio Frequency Identification), Wi-Fi and, of course, the drone's software.[104] Further, unless supported by statutory legislation and laws, breaching a geofenced area may not constitute an offence or unlawful act.

Counter Drone Response


Identification
Tracking
Detection
Neutral-isation
Forensics
Data logging (evidence gathering)
STAKEHOLDER ENGAGEMENT AND DECISION MAKING PROCESSES

Some companies also install back-up systems that allow drones to continue operating in GPS-denied environments. These back-up systems can bypass geofencing by using video that recognises key buildings or use topography for navigation. Much also depends on the pilot keeping their geo-awareness database up-to-date. In short, geofencing is useful in some cases but there are many ways around it, so the levels of assurance it can provide are inadequate.

The NATO Review referred to "uncontrolled developments" in commercial technologies that will massively challenge counter drone measures and will open the possibility of operating drones from anywhere in the world. It also recognised that counter drone systems are becoming smarter. The big challenge, therefore, is the gaps, cracks and loopholes in between local laws and capabilities.

This implies that drone use requires better and clearer regulation and governance, which need to keep pace with technology. It shows the need for public-private partnerships to further incorporate and enforce software restrictions to support clear and clearly understood national regulations and legal frameworks. This will be critical in degrading any future hybrid threats that leverage and/or are based on commercial systems. Increased requirements and accountability in private sector companies need to be robust and suited to the modern age. However, this is challenging in an international market where products transcend borders and companies sell in different nations with different rules in place. In addition, there are of course the weighty issues of legality, ethics and expense, creating a minefield for policymakers and operators alike.

There is a clear need for a wrap-around counter drone strategy and security measures, systems and processes to discharge this.

This is expanded through five pillars:

Pillar One

Legislation, regulation and governance. This means clear laws around the purchase and use of drones, as well as registration, licensing and activity-based permits; mandated requirements for manufacturers; and an accountable body to retain oversight as part of the wider security agenda.

Pillar Two

A wrap-around counter drone strategy to set the direction for preventing and deterring hostile drones, complemented by a concept of operations for the detection, tracking, identification, response, neutralisation and investigation of non-cooperative or hostile drones.

Pillar Three

Investment, planning and multi-agency resource. This is investment in the necessary infrastructure, resources and expertise; the development of joint intelligence and coordination mechanisms to prepare for and respond to hostile drones; plus, training, exercising and testing.

Pillar Four

Risk assessment and protective security. This includes threat and vulnerability assessments, imposed restrictions relating to flight altitude and no-fly zones, as well as static and mobile options to protect against hostile drones. It is also about the tactical and operational capabilities to handle, intercept and mitigate drones in different contexts and environments.

Pillar Five

Incident logging and forensic recovery of drone data. This is data processing and analysis to expedite investigations and inform approaches towards countering hostile drone activity. This should be coupled with the interrogation of detection data to identify trends, risks and threats. This can help inform investigative and preventative responses.

> **Increased requirements and accountability in private sector companies need to be robust and suited to the modern age. However, this is challenging in an international market where products transcend borders and companies sell in different nations with different rules in place.**

The European Commission has released a handbook[108] focussed on the risk assessment and target hardening of sites against drones. It includes practical guidance on vulnerability, threat and consequence assessments; considerations relating to site architecture, perimeter and surrounding area security; as well as counter drone methods and management. Other publications, such as the UK National Protective Security Authority's *"Countering Threats from Uncrewed Aerial Systems: Making Your Site Ready"*,[109] or its Senior Executive Guide[110] are available online. The UN offers a good practice guide: *"Protecting Vulnerable Targets from Terrorist Attacks Involving Unmanned Aircraft Systems"*.[112] The International Organization for Standardization (ISO) also has a section dedicated to standards for drones.[113]

Specialists, such as the US Department for Homeland Security Modelling and Simulation Technology Center,[114] also boast subject matter expertise and the rapid prototyping of tools to model and simulate operations, threat forecasting and incident response in different environments. These types of specialists continue to innovate and drive solutions. Local equivalents should be consulted to maximise approaches towards countering drones. However, there remains a clear need to consider further how hostile drones can be identified and countered in open urban environments (rather than static sites), as well as how multi-agency partners can prepare for and respond to such threats.

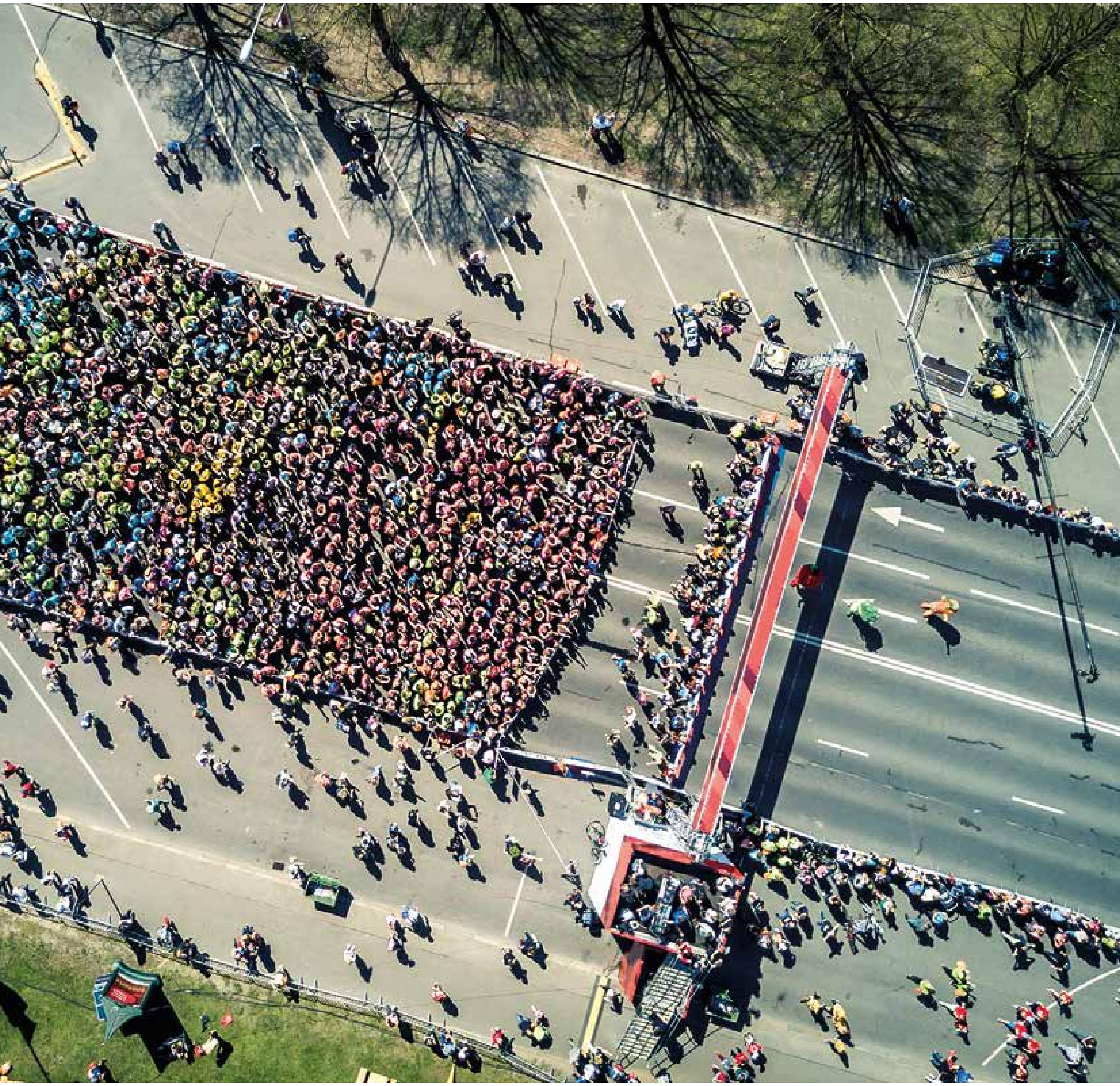
7 Preparing for Hostile Drones in Open Urban Environments

> “Although the traditional approaches associated with layered protective security still apply at ground level, a range of gaps and challenges emerge at just a few feet in the air.”

Rapid advances in drone technology, widespread market availability, and the threat of their malicious use show the necessity of reviewing multi-agency protect and prepare arrangements. That is, identifying and protecting against hostile drones and preparing to respond to drone attacks.

In civilian environments, counter drone technology is primarily used for securing the airspace around critical infrastructure, sensitive facilities, large events and venues, as well as for protecting VIPs.[115] Events on open public footprints, protests and high-footfall or densely populated locations such as city centre squares pose a different challenge. Even pre-event security sweeps conducted to sterilise and secure an area become immediately out-of-date.

Although the traditional approaches associated with layered protective security still apply at ground level, a range of gaps and challenges emerge at just a few feet in the air. Even where existing counter drone measures are deployed and/or installed, there are still gaps and very real threats, which can increase in busy, open urban areas. For the coronation of King Charles, drones were banned in central London and police had capabilities in place,[116] but this alone does not stop the threat. In fact, in this case, the victor in spotting a drone was the human eyeball – emphasising the need to focus on processes and staff resourcing before technology.



LEONARDO
BBC

Aside from simply launching and operating a small hostile drone in an area without restrictions or adequate security coverage to facilitate an attack, there are four other forms of drone attack that should be priorities in planning and preparedness.

These include:

1. drones that can operate in GPS-denied environments. These can navigate a route using landmarks, bypass security systems and create additional challenges in terms of detection and neutralisation;
2. a swarm of drones that could overwhelm security systems due to quantity. This has the potential to pose a significant threat and lowering costs makes multi-drone deployment more affordable.[117] Companies have already programmed hundreds and sometimes thousands of small drones for choreographed displays[118,119] – the current world record for the most drones flying simultaneously stands at 3,051;[120]
3. the carrying and use of malicious payloads such as chemical, biological and radiological agents or explosives; and
4. the ability of drones to deploy electronics to disable/disrupt facilities and/or conduct cyber-attacks. Researchers who hacked into a smart traffic-light system were able to feed it fake data from a drone flying overhead, for example.[121]

This highlights the relationship between urban planning and protective security; the connections between city design and safe operations; the associated implications for infrastructure; and the need for appropriate multi-agency preparedness and response arrangements. The concept of *securing the skies* now needs to be integrated into relevant city strategies from security to development.

This highlights the relationship between urban planning and protective security; the connections between city design and safe operations; the associated implications for infrastructure; and the need for appropriate multi-agency preparedness and response arrangements.

Flying High[122] is an initiative convening cities, technologists and researchers, regulators, government, public services and citizens to shape the future of urban drone use in the UK. This is about trying to meet people's needs and exploring the systemic requirements for integrating legitimate and lawful drone use into cities. This is where security and development need to be hand-in-glove, from the robust enforcement of no-fly zones to agreed flight pathways for drones (especially as numbers increase), although it is likely they will determine their own routes within outer areas.

Existing air traffic-management systems are simply not ready to accommodate drones and their flying patterns, and formal procedures aimed at controlling low-altitude drone traffic, defining restricted airspace and selectively granting or denying access to restricted areas are necessary.[123] This is in addition to the vulnerability mapping and risk classification of key areas; the installation of multi-tiered drone-detection systems; and building multi-agency response capabilities.

Just as technical interoperability is critical for counter drone technology, described as "linking systems and services of applications and infrastructures",[124] so is multi-agency preparedness and response. When considering this issue, the UK Joint Emergency Services Interoperability Principles (JESIP) can be applied. In this context, interoperability is defined as "the extent to which organisations can work together coherently as a matter of routine".[125] This is about the ability of organisations that operate under different legal frameworks to align powers, policies and procedures to achieve common goals. It is about shared understanding and expectations and complementary decision-making processes that enable them to discharge their responsibilities efficiently and effectively.

This does, however, require clear structures, ownership and responsibility. In the case of drones, understanding ownership of airspace is a cornerstone for preparedness.

In civilian environments, when criminality or unlawfulness is detected, the response to hostile drones should be led by the police services in close collaboration with partners. However, the difference between conflict and civilian settings is worth noting. In conflict environments, the military is likely to focus on neutralising an incoming drone before it carries out an attack. In civilian settings, where it is far less certain a drone is carrying a lethal payload, there are added complexities around the determination of pilot intent – and therefore the use of force and need to identify and investigate the pilot. This requires clear alert states, rules of engagement and powers of stop and search etc.

The speed, accuracy and conviction to intercept and/or immobilise hostile drones in urban environments is key to preventing an attack. This demands an increase in static and mobile counter drone measures, as well as the strategic placement of high-specification, high-speed response drones that can be deployed for "drone-to-drone" combat. These are increasingly common.[126] However, it will become even more important but even harder for counter drone operators to

Intraoperability... is about the ability of organisations that operate under different legal frameworks to align powers, policies and procedures to achieve common goals. It is about shared understanding and expectations and complementary decision-making processes that enable them to discharge their responsibilities efficiently and effectively.

differentiate between legitimate and rogue drones as the airspace becomes increasingly crowded. One tactic has been to mandate registered drone operators to install specific and approved LED tags.[127]

Another approach could be to compartmentalise cities into response zones with dedicated hubs to help manage the scale of the problem. Partnerships with the military could offer additional experience, expertise and resources under civilian assistance.[128] Likewise, the frequency of drone activity in cities means that civilian police can offer expertise in return. The *"Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems"* endorses the need for exchanges between civil-military partners.[129]

This suggests an imperative to establish a fully functional and dedicated centralised drone control and coordination centre with regional 24/7 monitoring, detection and response capability, staffed by highly skilled operatives. The need for extra vigilance in relation to the insider threat in these environments is obvious. Indeed, the speed at which these operators would need to process information (such as incident information, drone and flight characteristics and pilot descriptors) and deploy resources calls for a flat hierarchy with operational decision-making responsibility. "From the time of detection, and ideally with the capability to determine with certainty the drone's intentions, an operator has only a few seconds to react."[130] In these settings, complacency is not an option. Complacency could result in overlooking vulnerabilities, early warning signs, public reporting or credible threats, thus increasing vulnerability to an actual attack.[131]

This type of operation is intensified in busy urban environments that are inherently dynamic and can have “grey space”, where there is a lack of clarity on who is responsible and accountable for the ownership and protection of an area. This requires partners including local authorities to factor the drone threat into urban/spatial planning and local development/regeneration projects. It means that local authorities and businesses should support awareness-raising campaigns; consider the delivery of related staff training; and conduct their own assessments to identify attack vulnerabilities.

To ascertain these vulnerabilities, local authorities should seek to:

1. assess the threat posed by drones to different locations (disruption, surveillance, payload);
2. identify likely target points (i.e. the areas/locations that are critical and/or vulnerable);
3. understand potential threat actors and their level of capability and experience;
4. determine which drones are likely to be used for each scenario and how they would probably be flown. This information will help indicate launch points and possible collateral damage; and
5. analyse findings to provide a scenario-based risk rating to inform further actions.

Locations or sites identified may include open events with dense or widespread footfall; crowded places with limited counter drone security coverage; high-profile sites, critical infrastructure and locations of national significance; buildings of diplomatic importance or those occupied by “known” individual(s); and protected person(s) or person(s) of interest in a current investigation.

Many other targets could be identified with varying threat and risk levels. City centre squares, parks and shopping streets should also be flagged, for example.

By extension, this approach should drive multi-agency planning for cases where a drone attack can't be prevented and where the challenge then becomes managing the incident and its consequences while locating, identifying, apprehending and investigating the pilot(s). The motives and affiliations of the pilot(s) may not be known for some time, which may create a degree of uncertainty around whether the attack is terrorist-related and whether any further attacks are likely. In any case, the direct impacts and consequences will need to be addressed.

Herein lies the importance of consequence-based planning and the ongoing development of specialist resources that are transferrable to different incidents – casualty and mass-fatality planning, or chemical, biological, radiological, nuclear, explosive (CBRNE) plans that build in considerations around aerial threats specifically. This may include the spraying of agents or the dropping and/or detonation of small munitions. In one example, an agricultural drone was reported to have sprayed suspected chemicals and excreta over people at an event.[132]

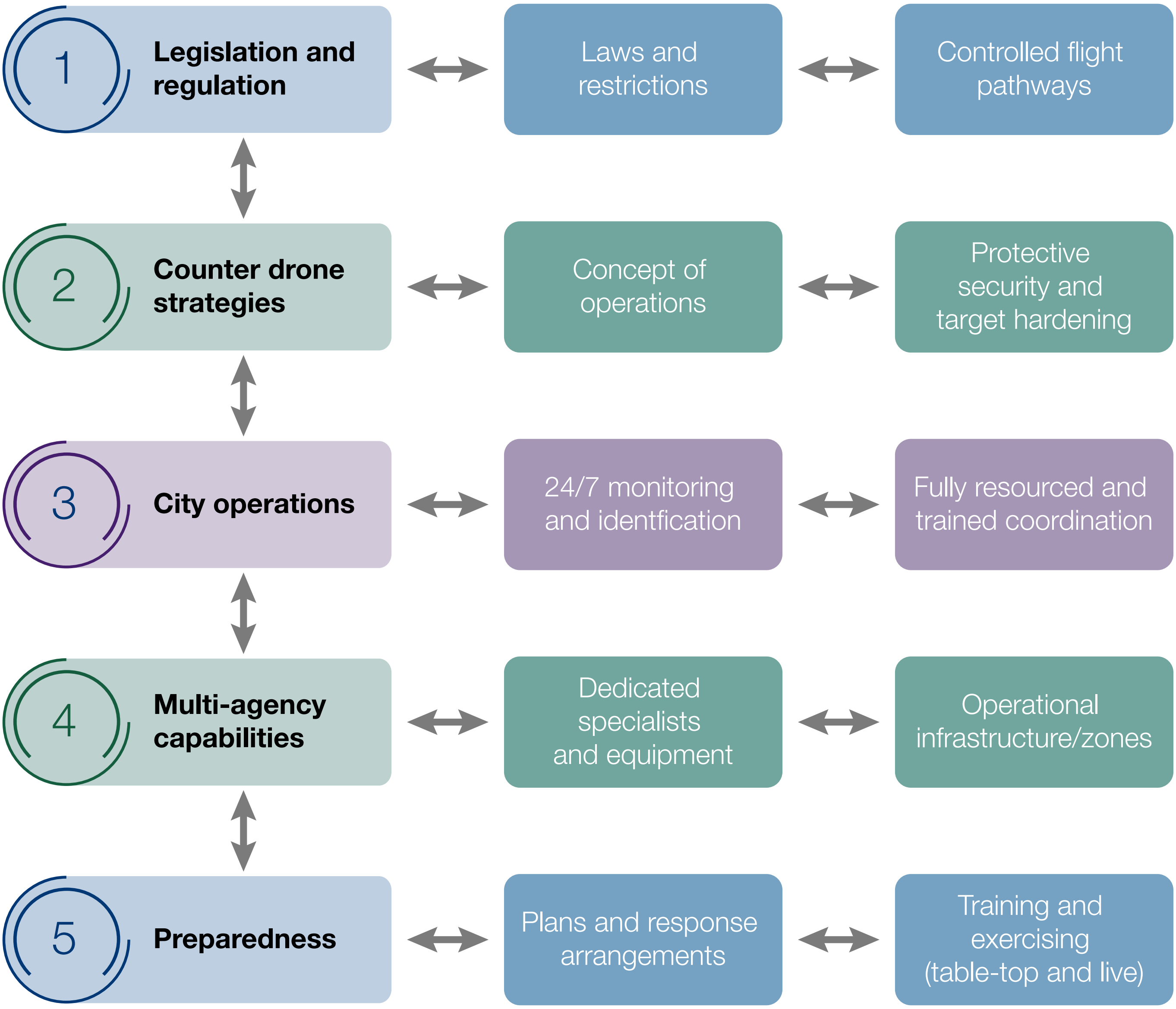
Plans also need to recognise hostile drones as potential IEDs that could be triggered upon landing, and what this could mean for the evacuation of any given area and for explosive ordnance disposal. Furthermore, the potential for drones to be fitted with light firearms shouldn't be ignored and may warrant awareness campaigns akin to "Run, Hide, Tell".[133]

These types of scenarios need to be explored by multi-agency partners through a clear training and exercising programme that seeks to inform and develop arrangements and capabilities. The consideration of potential attack scenarios should factor in realistic drone types (e.g. maximum payload, range, manoeuvrability and velocity), and focus on the possible tactics and weaponry as part of this. It is important to emphasise that smaller drones, such as those that weigh less than 20kg,[134,135] may be considered a higher threat because of their availability, rather than heavier drones that tend to be more specialised, complex and expensive with higher barriers to access (although these shouldn't be discounted). In addition, focussing on at-risk areas based on vulnerabilities versus target attractiveness and susceptibility would strengthen the exercise.

The speed, accuracy and conviction to intercept and/or immobilise hostile drones in urban environments is key to preventing an attack.

Preparations for the 2022 FIFA World Cup also included red and blue team exercises. This type of live exercise can be very beneficial. The red team are able to penetrate defences by targeting or attacking a site or area, thus identifying gaps, while the blue team are able to gain operational experience in responding to unknown drone threats with their current capabilities, thereby identifying any shortcomings or limitations. The aim of these exercises is to secure the asset or location against these threats or attacks using the existing operational procedures and counter drone technology. These can be used to test response plans and capabilities as well as communication and decision-making processes in real-time with a view to developing arrangements.[136]

From a public authority perspective, the European Commission underscored the need to "have clear and harmonised frameworks and procedures in place and provide clear authority for responsible public and private stakeholders to intervene against non-cooperative drones and facilitate collaboration between stakeholders that are not always accustomed to working together (law enforcement, civil aviation authorities, operators, manufacturers, mobile-network operators)".[137]


1
Legislation and regulation
Laws and restrictions
Controlled flight pathways
2
Counter drone strategies
Concept of operations
Protective security and target hardening
3
City operations
24/7 monitoring and identfication
Fully resourced and trained coordination
4
Multi-agency capabilities
Dedicated specialists and equipment
Operational infrastructure/zones
5
Preparedness
Plans and response arrangements
Training and exercising (table-top and live)

The above infographic summarises the need for robust legislation and regulations, controlled flight pathways and trained specialists. It also summarises the need to embed operational plans and processes as part of a dedicated and fully resourced infrastructure; the identification, testing and installation of counter drone measures (both static and mobile); and the need for multi-agency exercises including red and blue teaming. This is non-exhaustive but is offered in support of city-level planning and preparedness, and can be adapted, enhanced or applied locally according to context.

Ultimately, the most effective defences against drones are "layered, integrated, interoperable systems capable of providing 360-degree coverage, employing a variety of hard- and soft-kill solutions".[138] However, there needs to be a spotlight on enhancing the underpinning legislation and recognising the technical and operational limitations of current counter drone options. These limitations mean that the target hardening of sites and the multi-agency response arrangements are critical.

Beyond this, awareness of drone activity needs to be increased and built into business-as-usual city operations. This is not dissimilar from how cities monitor traffic volumes or patterns and problems via CCTV and other methods. If city authorities recognise the need to apply a similar approach, this could help reduce dependence on trained experts and enhance both preparedness and resilience.

FIRE LANE

8 Summary and Recommendations

> “The core challenge here is achieving the political buy-in, prioritisation and investment needed to prevent, protect against and prepare for the threat of hostile drones given other competing demands, threat perceptions and financial constraints.”

Drones straddle conflict zones, crime and terrorism, as well as services and hobbies. They span issues from international law to border security and the flow of weapons; regulations, ethics and public-private sector responsibilities; counter drone measures; and multi-agency preparedness.

This report considered the military origin of drones and their role in warfare, and the domestic threat (and potential threat) of drones with a focus on terrorism. It then reflected on the options and challenges for protecting against drones at static sites and concluded with a section on preparing for hostile drones in open urban environments.

Although the threat of hostile drones in open urban environments may be considered relatively low, it needs to be taken seriously. It is very real, and the landscape will be significantly different in the next five to 10 to 15 years, requiring cities and their constituent authorities to be ahead of the curve. The core challenge here is achieving the political buy-in, prioritisation and investment needed to prevent, protect against and prepare for the threat of hostile drones given other competing demands, threat perceptions and financial constraints. This is a delicate balance.

However, as the *Countermeasures for Aerial Drones* handbook notes, the industry continues to outpace the development of rules and regulatory systems to govern drones’ use, and by extension, the powers for police and other civil authorities to enforce laws effectively.

The handbook states that the scale and scope of technological advances, coupled with increasing levels of analytical computer power and AI, ensure that the threat from drones will persist, remaining a major public safety and national security concern for the foreseeable future.[139]

This underscores the need to “anticipate trends, to imagine the desired end state and work towards it” using a mix of different approaches: preparedness, innovation and cooperation.[140] These lean towards a coordinated and adaptive approach that can navigate political sensitivities and blend technical solutions with multi-agency preparedness and public education in ways that enable society to reap the rewards drones offer whilst maintaining safety and security.[141]

> **Awareness of drone activity needs to be increased and built into business-as-usual city operations. This is not dissimilar from how cities monitor traffic volumes or patterns and problems via CCTV and other methods. If city authorities recognise the need to apply a similar approach, this could help reduce dependence on trained experts and enhance both preparedness and resilience.**

Recommendations

1. Clarify who owns the airspace above the city (e.g. civil aviation authority or local authority).

2. Continue to undertake threat, vulnerability, asset and security risk assessments to inform a prioritised and proportionate approach towards protect and prepare in urban environments.

3. Ensure a city-level counter drone strategy that is underpinned by legislation, powers and policies and complemented by an agreed concept of operations, standard operating procedures and response plans that are clearly owned and spearheaded by the lead agencies.

4. Develop a multi-agency hostile drone or aerial-threat consequence management framework that outlines the potential scenarios and impacts, as well as the capabilities, structures, processes and procedures that are in place and may need to be activated.

5. Enhance related intelligence and information sharing by engaging with relevant stakeholders.

6. Embed awareness training for emergency services, local authorities and security personnel.

7. Consider approaches for public awareness and education (e.g. schools and groups). This could be a city toolkit for community engagement and deterrence communication campaigns etc.

8. Seek advice from the relevant protective security authorities and experts regarding target hardening and counter drone technology, including static installations and mobile deployments at key sites and locations. This should be an ongoing priority.

9. Agree minimum standards and a testing criterion for the procurement of counter drone systems. This must include consideration of appropriate resource and staffing commitments.

10. Test counter drone systems in the environments where it is intended they will operate. The digital landscape may change frequently and systems may need to be refined or recalibrated to ensure that optimal detection, tracking, identification and mitigation coverage is maintained.

11 Establish a unified drone-threat reporting system and data-exchange protocol between agencies such as law enforcement, civil aviation and other partners. This should include critical infrastructure operators, airports and stadia to ensure comprehensive monitoring.

12 Invest in a fully functional and dedicated joint command, control and coordination centre or unit that operates on a 24/7 basis. This should be a multi-agency resource.

13 Engage specialists to build analytical products and practices to review drone forensics and data. This is essential for capturing and understanding baseline drone activities, patterns, threats and vulnerabilities, to develop tactical options to counter drone threats.

14 Deliver a training and exercising programme that covers a mix of hostile drone scenarios at strategic, tactical and operational levels. Complement this with red and blue team exercising, whereby the red team behaves as a threat actor. This should mimic real-world threats to test the defences and operations of an asset or location and/or multi-agency response capabilities.

15 Promote targeted exercises with business districts to raise awareness and preparedness.

16 Ensure that agencies involved in the response to hostile drones are regularly trained and that different types of drones are used to test response, mitigation and decision-making processes.

17 Convene a multi-agency governance group (chaired by the agreed lead agency) that includes public sector partners, protective security authorities, critical national infrastructure, aviation and military to oversee, and account for, city-level arrangements in countering hostile drones.

18 Participate in related research and innovation projects to capture and share best practices; horizon scan for developments in drones and counter drones; identify new and emerging threat vectors; and work with cross-sector stakeholders as appropriate to address these.

Note: This is an international report designed for an international audience. It is accepted that different recommendations will apply to different cities and organisations, subject to context and existing arrangements. These recommendations are non-exhaustive and further insight is required.

9 Reference List

1. United Nations Office of Counter Terrorism (2023). United Nations Global Counter-Terrorism Strategy (accessed online).
2. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism, Counter Terrorism Preparedness Network, p.40 (accessed online).
3. CTPN (2019). Protecting Major Events and Crowded Places, Counter Terrorism Preparedness Network.
4. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism.
5. United Nations Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks Involving Unmanned Aircraft Systems (UAS): Good Practices Guide, United Nations, p.2 (accessed online).
6. Karlos, V., Larcher, M. (2023). Protection Against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites, JRC technical report, European Commission, p.5.
7. United Nations (2023). Letter dated 19 December 2023 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council.
8. European Commission (2023). Communication from the Commission to the Council and the European Parliament on Countering Potential Threats Posed by Drones, Brussels (released 18 October 2023).
9. INTERPOL (2020). Framework for Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners, INTERPOL, p.14 (accessed online).
10. HM Government (2019). UK Counter-Unmanned Aircraft Strategy, p.3 (accessed online).
11. PwC (2022). Skies Without Limits v2.0, p.2 (accessed online).
12. Simpson, E. (2023). “Amazon pledges parcels in an hour using drone deliveries”, BBC News (accessed online).
13. Clifton, P. (2023). “UK drone superhighway due to complete by 2024”, BBC News (accessed online).
14. Benner, T. (2019). “Volocopter takes to Singapore sky, but can air taxis take off?”, Al Jazeera (accessed online).
15. Loi, E. (2023). “Lack of local funding partners forces Volocopter to put air taxi launch in Singapore on hold”, *The Straits Times* (accessed online).
16. DARPA (2023). “DARPA Seeks Tech Solutions to Create Autonomous Capabilities for Commercial Drones” (accessed online).
17. Hansen P., and Pinto Faria, R. (2023). Protection Against Unmanned Aircraft Systems: Handbook on UAS Protection of Critical Infrastructure and Public Space: A five phase approach for C-UAS stakeholders, European Commission, Joint Research Centre, p.5 (accessed online).
18. European Commission (2023). Communication from the Commission to the Council, p.1.
19. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems, p.6.
20. European Commission (2023). Communication from the Commission to the Council, p.8.
21. European Commission (2022). A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe, COM(2022) 652 final, 29 November 2022.
22. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks.
23. INTERPOL (2020). Framework for Responding to a Drone Incident.
24. HM Government (2019). UK Counter-Unmanned Aircraft Strategy (accessed online).
25. Airports Council International (no date). Counter Drone Knowledge Centre (accessed online).
26. Department for Transport (2018). Taking Flight: The Future of Drones in the UK, UK Government (accessed online).
27. EASA (2021). ¬Drone Incident Management at Aerodromes, European Union Aviation Safety Agency (accessed online).
28. Marcus, J. (2022). “Combat Drones: We are in a new era of warfare – here’s why”, BBC News (accessed online).
29. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems, p.5.
30. Rogers, J. (2017). Countering Weaponised Drones, Counter Terror Business (accessed online).
31. Murphy, M. (2022). “Ayman al-Zawahiri: How US spies found al-Qaeda’s top man in Kabul”, BBC News (accessed online).
32. Bell, J. (2022). Countering Swarms: Strategic Considerations and Opportunities in Drone Warfare, JFQ 107, 4th Quarter, p.5 (accessed online).
33. BBC News (2019). “UN ‘cannot confirm Iran behind Saudi oil attacks’”, BBC News (accessed online).
34. Palestini, C. (2020). Countering Drones: looking for the silver bullet, NATO Review (accessed online).
35. Ibid.
36. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism, p.34.
37. Rassler, D. (2018). The Islamic State and Drones: Supply, Scale, and Future Threats. Combatting Terrorism Centre at West Point, United States Military Academy, p.23 (accessed online).
38. Michel, A. (2019). *Counter-Drone Systems, 2nd Edition*, Center for the Study of the Drone at Bard College, p.8 (accessed online).
39. Rogers, J. (2017). Countering Weaponised Drones, Counter Terror Business (accessed online).
40. Ibid.

Reference List
continued

41. UN Office of Counter Terrorism (2023). Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes, UNOCT AROS Programme and Conflict Armament Research (accessed online).P.2.
42. Michel (2019). *Counter-Drone Systems, 2nd Edition*.
43. Dass, R. (2022). Militants and Drones: A Trend That is Here to Stay, Royal United Services Institute (accessed online).
44. Atkinson, E. (2023). "HMS Diamond: British warship shoots down suspected attack drone in Red Sea", BBC News (accessed online).
45. Reed, S. (2024). "Red Sea Attacks Menace Energy Tankers but Don't Stop Them", *The New York Times* (accessed online).
46. Ward, J., and Beech, E. (2024). "US, UK forces repel 'largest attack' by Houthi's in Red Sea", Reuters, 10 January 2024 (accessed online).
47. Judson, J. (2023). "Pentagon's counter-drone boss tackles rising threat", Defense News, (accessed online).
48. Bell (2022). Countering Swarms, p.5.
49. Feely, E. (2023). A "System of Systems" Approach to Countering Drones: Examining Recent Operations from the Middle East to Ukraine. The Washington Institute for Near East Policy, Policy Notes, August 2023, No. 139, p.11.
50. Palestini (2020). Countering Drones.
51. KKunertova, D. (2022). The Ukraine Drone Effect on European Militaries, *Policy Perspectives*, Volume 10/15 (December 2022). Center for Security Studies (CSS), ETH Zürich, p.2.
52. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems, p.6.
53. European Commission (2023). Communication from the Commission to the Council, p.2.
54. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.17.
55. ATM MarketPlace (2022). "Drone steals nearly $150K from an ATM" (accessed online).
56. AP, (2015). "Drone 'containing radiation' lands on roof of Japanese PM's office", *The Guardian*, 22 April 2015, (accessed online).
57. Michel (2019). *Counter-Drone Systems, 2nd Edition*, p.8.
58. Ibid, p.9.
59. BBC (2022). "Sweden drones: Sightings reported over nuclear plants and palace", BBC (accessed online).
60. Lye, H. (no date). A New Threat Dimension: Protecting Critical Infrastructure from Drone Attacks, *Global Defence Technology* (accessed online).
61. Marcus, J. (2022). "Combat Drones: We are in a new era of warfare – here's why", BBC News (accessed online).
62. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks.
63. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems, p.5.
64. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets, pp.3–5.
65. Michel (2019). *Counter-Drone Systems, 2nd Edition*, p.8.
66. Catalan News (no date). "3-year sentence for plotting drone terror attack in Camp Nou during Barça v Real Madrid game" (accessed online).
67. European Commission (2023). Communication from the Commission, p.2.
68. Cruikshank, P. (2023). A View from the CT Foxhole: Catalan Police – Mossos d'Esquadra with Lluis Paradell Fernandez, Head of the Central Analysis Unit, Intelligence and Counterterrorism Service; Xavier Cortés Camacho, Head of the Counterterrorism Central Area, *CTC Sentinel*, April 2023 16(4).
69. Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019. (no date). "Planning the Terrorist Attack" (accessed online).
70. Macklin, G. (2019). "The Christchurch Attacks: Livestream Terror in the Viral Video Age", *CTC Sentinel*. July 2019, 12(6), Combatting Terrorism Centre at West Point (accessed online).
71. EUROPOL (2022). European Union Terrorism and Trend Situation Report 2022, p.13 (accessed online).
72. Gall, C. (2023). "Coventry student guilty of making IS chemical weapon drone", BBC News (accessed online).
73. UN Office of Counter Terrorism (2023). Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes, UNOCT AROS Programme and Conflict Armament Research (accessed online).
74. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.5.
75. EUROPOL (2023). European Union Terrorism Situation and Trend Report 2023, p.74 (accessed online).
76. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets, p2.
77. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism, p.34.
78. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.18.
79. UK Ministry of Defence (2018). Global Strategic Trends: The Future Starts Today, sixth edition, p.35 (accessed online).
80. Rogers, J. and Kunertova, D. (2022). The Vulnerabilities of the Drone Age Established Threats and Emerging Issues out to 2035, Centre for War Studies and Centre for Security Studies ETH Zurich, supported by the NATO Science for Peace and Security Programme, p.2 (accessed online).

Reference List
continued

81. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism, p.34.

82. United Nations Office of Counter Terrorism (2021). Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes, p.34 (accessed online).

83. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems, p.5.

84. Bell (2022). Countering Swarms, p.6.

85. Michel (2019). *Counter-Drone Systems, 2nd Edition*, p.10.

86. EUROPOL (2023). European Union Terrorism Situation, p.74 (accessed online).

87. CTPN (2019). Protecting Major Events, p.12.

88. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.39.

89. Feely, E. (2023). A “System of Systems” Approach to Countering Drones: Examining Recent Operations from the Middle East to Ukraine, The Washington Institute for Near East Policy, Policy Notes No. 139 (August 2023), p.2.

90. European Commission (2023). Communication from the Commission to the Council, pp.3–4.

91. Best, K. et al (2020). How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools, RAND Corporation (accessed online).

92. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.47.

93. Ibid, p.50.

94. Ibid, p.56.

95. Michel (2019). *Counter-Drone Systems, 2nd Edition*, p.13.

96. National Protective Security Authority (2023). Countering Threats From Uncrewed Aerial Systems: Developing Operational Requirements for C-UAS Detect, Track and Identify Technology, UK Government.

97. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks, p.41.

98. Project COURAGEOUS (no date). Towards a Better understanding of Counter-Drone Systems (accessed online).

99. Mayors of Europe (2020). “SKYFALL: Special training initiative focused on protecting against drone attacks took place in Antwerp” (accessed online 19 December 2023).

100. DroneWISE (2022). DroneWISE – Deliver the impact (accessed online).

101. COURAGEOUS (2022). COURAGEOUS – Building towards a better understanding of the capabilities of counter-drone systems, (accessed online 19 December 2023).

102. UN and INTERPOL (2023). Global Sports Programme and INTERPOL – Project Stadia Online Expert Discussion: Investigating the Nexus Between New and Emerging Technologies and Major Sporting Event Protection, webinar.

103. Grasha, K. (no date). “Man sentenced in 2022 drone incident during Bengals-Raiders game that changed NFL policy”, *Cincinnati Enquirer* (accessed online).

104. Davis, K. (2022). Geofencing on Drones, DroneBlog (accessed online).

105. Palestini (2020). Countering Drones

106. Rassler, D. (2018). “The Islamic State and Drones: Supply, Scale, and Future Threats”, Combatting Terrorism Centre at West Point, United States Military Academy, p.5 (accessed online).

107. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.7.

108. Karlos and Larcher (2023). Protection Against Unmanned Aircraft Systems.

109. National Protective Security Authority (2020). Countering Threats from Uncrewed Aerial Systems: Making Your Site Ready. UK Government (accessed online).

110. National Protective Security Authority (2023). Countering Threats from Uncrewed Aerial Systems: A Senior Executive Guide to Making Your Site Ready. UK Government (accessed online).

111. Patel, B. and Rizer, D. (2019). Counter-Unmanned Aircraft Systems Technology Guide, US Department of Homeland Security Science and Technology and National Urban Security Technology Laboratory (accessed online).

112. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks.

113. International Organization for Standardization (no date). Unmanned aircraft systems (accessed online).

114. US Department of Homeland Security (no date). Modelling and Simulation Technology Center (accessed online).

115. Michel (2019). Counter-Drone Systems, 2nd Edition, p.5.

116. Sabbagh, D. (2023). “Drone flights banned in central London for King Charles coronation”, *The Guardian* (accessed online).

117. Kunertova (2022). The Ukraine Drone Effect on European Militaries, p.4.

118. Bell (2022). Countering Swarms, p.5.

119. ITV News (2021). “Greenpeace uses 300 drones to send message to G7 leaders at summit in Cornwall” (accessed online).

120. Zhan, E. (2020). “3,051 DRONE create spectacular record-breaking light show in China”, Guinness World Records (accessed online).

121. CTPN (2022). City Preparedness for Cyber-Enabled Terrorism, p.45.

122. Flying High (2017). Shaping the future of drones in UK cities, Nesta (accessed online).

123. UN Office of Counter Terrorism (2022). Protecting Vulnerable Targets from Terrorist Attacks, p.22.

Reference List
continued

124. Hansen and Pinto Faria (2023). Protection Against Unmanned Aircraft Systems, p.56.

125. JESIP (no date). Joint Emergency Services Interoperability Principles (accessed online).

126. HM Government (2019). Action to detect, deter and disrupt the misuse of drones (accessed online).

127. INTERPOL (2022). Security Observer Programme to the FIFA World Cup.

128. Royal Air Force (no date). The Defence Warning and Reporting Flight (accessed online).

129. GCTF (no date). Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, Global Counterterrorism Forum (accessed online).

130. Palestini (2020). Countering Drones.

131. GCTF (no date). Berlin Memorandum (accessed online).

132. DroneSec (2023). “Farming drone was used to spray a suspected farming chemicals and excreta onto civilian and political attendees during an event”, LinkedIn post (accessed online).

133. UK Counter Terrorism Policing (no date). What you can do: The cooperation between the public and the police is a powerful defence (accessed online).

134. HM Government (2019). UK Counter-Unmanned Aircraft Strategy, p.8 (accessed online).

135. Wilson, B. et al (2020). Small Unmanned Aerial System Adversary Capabilities, RAND Corporation (accessed online).

136. INTERPOL (2023). Stadia protection and mitigation from drone incursion and threats: Case study FIFA World Cup Qatar 2022, Project Stadia, Safe & Secure Major Events.

137. European Commission (2023). Communication from the Commission to the Council, p.2.

138. Feely (2023). A “System of Systems” Approach.

139. Markarian, G. and Staniforth, A. (2022). Countermeasures for Aerial Drones, Chapter 8: A strategic approach to counter rogue drone threats, 8.9 Balancing Act, p. 211, Artech House: London, available online.

140. Palestini (2020). Countering Drones.

141. HM Government (2019). UK Counter-Unmanned Aircraft Strategy, p.4 (accessed online).

3. 141592653589
INT MAIN (INT ARGC, CHAR **ARGV) {
VECTOR<CHAR> ACC
CHAR CH;
IFSTREAM INFILE (ARGV[1])
SAT
01/6
2. 71828818228
INT MAIN (INT ARGC, CHAR **ARGV) {
INT MAIN (INT ARGC, CHAR **ARGV) {

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK

www.london.gov.uk/ctpn