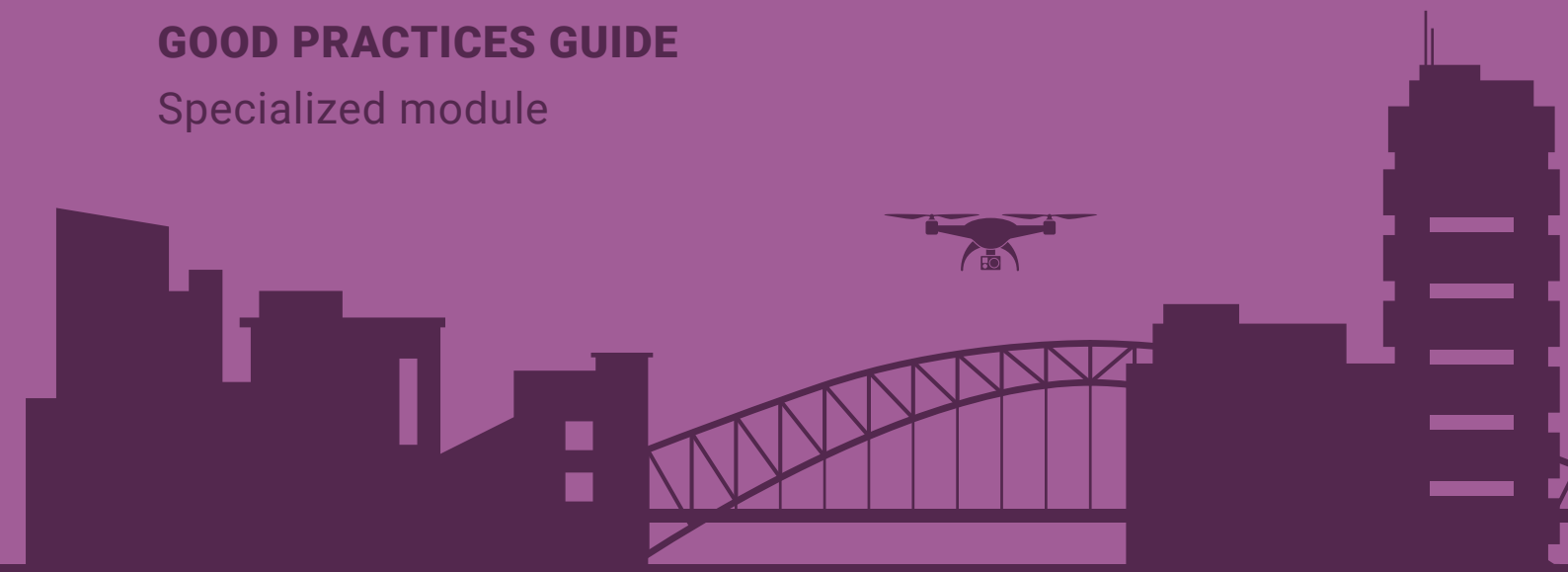
UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

5

Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)

GOOD PRACTICES GUIDE

Specialized module



Global Programme on Countering Terrorist Threats against Vulnerable Targets

Implemented in partnership with:

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

UNAOC
United Nations Alliance of Civilizations

unicri
United Nations Interregional Crime and Justice Research Institute

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)

GOOD PRACTICES GUIDE

Specialized module

Global Programme on Countering Terrorist Threats against Vulnerable Targets

Implemented in partnership with:

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

UNAOC
United Nations Alliance of Civilizations

unicri
United Nations Interregional Crime and Justice Research Institute

Contents

Preface

The Office of Counter-Terrorism (UNOCT)'s Global Programme on Countering Terrorist Threats against Vulnerable Targets[1] developed this document as a guide on the protection of vulnerable targets against terrorist attacks involving unmanned aircraft systems (UAS). This sector-specific module complements *The Protection of Critical Infrastructure against Terrorist Attacks: Compendium of Good Practices*.[2]

Following an overview of key threats and vulnerabilities exposing vulnerable sites to terrorist attacks involving unmanned aircraft systems (UAS), this module explores the specific role that individual stakeholders can and should play in a complex – and often volatile – security environment by acting within the conceptual framework of a risk and crisis management approach. It contains a selection of case studies illustrating how key security-related principles – including internationally endorsed recommendations – have been operationalized by Governments, private-sector entities, operators of vulnerable sites and civil society organizations. The module also summarizes the content of several tools (manuals, handbook, compendiums) which provide guidance on establishing sound policies and operational settings to reduce the exposure of vulnerable targets to terrorist attacks involving UAS and increase their resilience.

The analytical framework, case studies, tools and all the resources featured in this module are the result of intensive desk research, a formal request for inputs from all 193 United Nations Member States, discussions with individual experts, international organizations and project partners, as well as input from the Working Group on Emerging Threats and Critical Infrastructure Protection of the Global Counter-Terrorism Coordination Compact.[3] Important

1 The programme partners are the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Alliance of Civilizations (UNAOC) and the United Nations Interregional Criminal Justice Research Institute (UNICRI). The Programme is being implemented in close consultation with other relevant organizations, including INTERPOL. See www.un.org/counterterrorism/vulnerable-targets.

2 The Compendium was developed in 2018 by the Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security of the Counter-Terrorism Implementation Task Force (CTITF). In 2019, CTITF was folded into the Global Counter-Terrorism Coordination Compact. Under this new structure, the above-mentioned Working Group and the Working Group on Preventing and Responding to Weapons of Mass Destruction Terrorist Attacks were combined to create the Working Group on Emerging Threats and Critical Infrastructure Protection.

3 See www.un.org/counterterrorism/global-ct-compact.

insight was obtained from two Expert Group Meetings (EGM) that were organized by UNOCT, which brought together experts from Member States, international and regional organizations, civil society, the private sector and academia. The first EGM was held on 29 June 2021, during the Virtual Counter-terrorism Week, and the second was held on 6 October 2021. The process also benefited from the input of UNOCT's Gender Advisor and a dedicated human rights consultant in UNOCT's Special Projects and Innovation Branch.

This module extensively cross-references *Preventing Terrorists from Acquiring Weapons: Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons* (hereinafter "Resolution 2370 Technical Guidelines"). The Guidelines contain two submodules, of which submodule II on preventing terrorists from acquiring unmanned aircraft systems and components.[4]

4 See www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf. In December 2021, Resolution 2370 Technical Guidelines were in the final stages of development as part of a joint project implemented by the Counter-Terrorism Committee Executive Directorate (CTED) on behalf of the Working Group on Border Management and Law Enforcement of the Global Counter-Terrorism Coordination Compact. The project is funded by the United Nations Counter-Terrorism Centre (UNCCT) of the Office of Counter-Terrorism (UNOCT), and co-implemented by UNCCT and the United Nations Institute for Disarmament Research (UNIDIR), in close cooperation with member entities of the aforementioned Working Group.

Index of boxes

Index of case studies

Index of tools

[1]

The terrorist threat posed by UAS to vulnerable targets

Unmanned aerial vehicles (UAVs), or drones, are aircraft that do not require the presence of a human pilot on board. Drones are the flying component of unmanned aircraft systems (UAS), which also comprise a ground control system (GCS) and payloads.[5]

UAS are operated using different flight navigation methods,[6] which provide them with different degrees of autonomy from human intervention. There is a wide variety of sizes, weights, shapes, technological equipment and prices. UAS can be designed and used in the military or civilian domain; those used for civilian purposes include recreational drones, designed for amateurs and hobbyists, and those employed for professional uses. The latter have a wide and

5 See Resolution 2370 Technical Guidelines, submodule II, Components of UAS (1.1.1).

6 UAS basic navigation methods consist of: (1) Manual navigation, relying on radio communication between the UAV and GCS; (2) GPS navigation, not relying on radio signals and enabling UAVs to be pre-programmed to fly autonomously to specified locations or follow specified flight segments; (3) Autonomous navigation, based on the UAV's own on-board sensors, allowing the device to follow moving objects and people or aim at unmoving objects.

ever-growing range of applications, from crop monitoring and treatment to industrial inspection, rescue and disaster relief operations, among others.

UAS continue to benefit from rapid technological progress[7] as well as advances in artificial (AI) intelligence research and applications.[8] Many commercial off-the-shelf UAS can be easily modified or upgraded to suit users' individual needs. Other UAS (called "bespoke UAS") are assembled by using components that are bought individually and put together to fit the specific purposes of their users.

While UAS clearly contribute to societies' growth and development in many respects, they also open a world of new opportunities for terrorist purposes. These devices offer users increasing levels of accuracy and reliability, as well as easy integration of custom-made features. While overwhelmingly used for legitimate goals, they are also exploited for criminal and terrorist purposes.

The Security Council has already acknowledged and requested that action be taken to mitigate the threat of UAS falling into the hands of terrorists. Resolution 2370 (2017),[9] in particular, "strongly condemn[s] the continued flow of weapons, including small arms and light weapons, military equipment, unmanned aircraft systems (UASs) and their components, and improvised explosive device (IED) components to and between ISIL (also known as Da'esh), Al-Qaida, their affiliates, and associated groups, illegal armed groups and criminals, and encourag[es]) Member States to prevent and disrupt procurement networks for such weapons, systems and components".

In the current global security environment, the risk of terrorist groups acquiring, developing the expertise for, and effectively using UAS appears to be facilitated by a number of concomitant factors, such as:[10] (1) the unregulated and increasingly sophisticated civilian market for UAS technology; (2) the wide availability of unregulated, uncontrolled and unsecured explosives, which can be used as payloads on UAS; (3) access to explosive precursors (ammonium nitrate, peroxide, etc.); and (4) the availability of technical expertise from terrorists/associated individuals and groups, as well as transfers of this expertise and knowledge.

The above does not necessarily suggest that UAS will become the principal means of attack for terrorist purposes in the foreseeable future. However, there are increasing indications that non-State actors are attempting to leverage UAS in the pursuit of terrorism-related objectives well beyond areas affected by military operations. This would point to a significantly increased risk of future attacks targeting critical infrastructure and other vulnerable targets.

7 Strong market demand has spurred the development of increasingly sophisticated sensors, automated capabilities, longer battery life, etc. Given the sustained pace of innovation in this sector, UAS models are constantly surpassed by new, higher-performing products.

8 UAS powered by artificial intelligence would effectively constitute autonomous weapons systems capable of searching, selecting and engaging targets on their own. They may have already been deployed in Libya when "logistic convoys and retreating HAF [Haftar Affiliated Forces] were … hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems … and other loitering munitions. The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget and find' capability" (S/2021/229, para. 63).

9 An identical provision is contained in subsequent instruments of the Security Council, such as resolution 2482 (2019).

10 UNOCT-organized side event on 29 June 2021 (Virtual Counter-Terrorism Week).

Box 1.

The terrorist threat posed by UAS and chemical, biological, radiological or nuclear (CBRN) agents

In order to cause a CBRN incident, hostile actors may use UAVs to spread CBRN agents through the UAS's payload capacity,[11] and as weapons to attack a CBRN facility.

Historically, the first recorded incident involving non-State actors using CBRN agents for terrorist purposes dates back to 1994, when the millenarian sect Aum Shinrikyo unsuccessfully attempted to use two remote-controlled helicopters to spray sarin gas. In 2015, a man managed to fly a drone carrying radioactive sand onto the roof of the Japanese Prime Minister's office. Crucially, the drone was discovered only by chance a few days afterwards. The following year, the then British Prime Minister warned that ISIL/Da'esh affiliates were planning to carry out "dirty bomb" attacks by releasing UAS-borne nuclear agents over densely populated urban areas.

In 2019, France's Anti-Terrorism Coordination Unit (UCLAT) released a confidential report alerting about "a possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents". The warning was reiterated by the European Commissioner for the Security Union.[12]

(continued)

11 For example, UAS designed for agricultural purposes (e.g., to release pesticides on crops) may be repurposed to spray CBRN agents.

12 The threat of UAS being used to target spectators and athletes, especially in crowded sport competitions, is mentioned in the *Guide on the Security of Major Sporting Events* (UNOCT, UNICRI, UNAOC, ICSS, 2021), p. 36 (www.unaoc.org/wp-content/uploads/GUIDE-on-MSE-Security-with-Annex-Final.pdf).

The threat is considered to be serious in view of the disproportionate consequences that one single successful attempt may have. Furthermore, although a UAS-enabled CBRN attack may not necessarily cause extensive harm to people, it would have a strong psychological impact on the public. Even non-lethal agents may cause extensive panic, for example if several UAS flying above a stadium released toxic substances.[13] In addition, a CBRN attack may cause potentially very costly clean-up operations for large areas, as well as make it significantly more difficult for first responders and rescue services to remove debris, conduct searches and rebuild infrastructure due to contamination levels.[14]

The current international legal framework contemplates the possibility of non-State actors using UAS for delivering CBRN weapons and requests that Member States adopt the appropriate control measures. Security Council resolution 1540 (2004) notably decides that States shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery.

As UAS are "means of delivery", resolution 1540 can be seen as a fully-fledged tool requiring countries to stem the proliferation of UAS-based terrorist acts involving CBRN weapons.

In recent years, law enforcement authorities have either detected or disrupted various terrorism-related plans envisaging the use of UAS in non-conflict zones.[15] These include:

- At the 2016 Olympic Games in Rio De Janeiro, Al-Qaida operatives gave instructions to target athletes as well as spectators. The next day, the Brazilian police reportedly arrested a group of ten suspects in connection with the games (Moore, 2016);
- In 2019, a group of militants in the suburb of Jakarta were found in possession of an UAS and batteries. The following year, Indonesia's counter-terrorism police conducted a series of arrests which revealed terrorists' intentions to use drones (Association of the United States Army, 2021);
- In September 2020, a Danish appellate court confirmed guilty verdicts issued by a first-instance court against three individuals convicted of promoting and supporting Da'esh.[16] Notably, "the men had bought hobby aircraft, unmanned aerial vehicle (UAV or 'drone') parts … which were to be used in the [Da'esh] UAV programme and activities related to the fighting in Syria and Iraq" (Europol, 2021, p.37).

13 Remarks by Mr. Günter Povoden, Senior Consultant, UNODC, at the UNOCT-organized Expert Group Meeting on the Protection of Vulnerable Targets and Unmanned Aircraft Systems (UAS), 6-7 October 2021.

14 For a general assessment of the challenges that non-State actors may face in spreaing CBRN agents by means of UAS, see "Drones and CBRN terrorism threats and responses", presentation by Philipp C. Bleek at the 2020 Countering Drones conference, organized by Defense iQ, 4 June 2020 (www.middlebury.edu/institute/news/drones-and-cbrn-terrorism-threats-and-responses).

15 Don Rassler compiled a comprehensive list of suspected terror plots involving UAS, up to late 2016. Rassler notably distinguishes between "terror entities that have shown a more limited interest" in UAS and those whose drone "use is sustained and developed enough to be considered a 'program'" (Rassler. 2016).

16 The latest court decision has been appealed before Denmark's Supreme Court.

With the return of foreign terrorist fighters (FTF) from the Syrian Arab Republic and Iraq, concerns have been raised that Da'esh affiliates may be planning the transfer of UAS-related technologies and tactics learned on the battlefield to their home countries (GCTF, 2019).[17]

UAS offer terrorist groups a set of distinct advantages as part of their attack strategies, most crucially a greater potential to circumvent traditional physical protection measures based on multiple levels of security (e.g., in the form of hardened venue perimeters designed to stem vehicle-borne attacks, armed guards or visitor-screening barriers).

UAS operators can also carry out their activities from hidden or protected spots, thus reducing the risk of being reached by countermeasures. Technologies enabling UAS piloting beyond the visual line of sight are now routinely employed in various commercial and government applications. When these technologies are employed for illegal, including terrorist, purposes, they make it significantly more difficult for law enforcement authorities to detect and apprehend operators. Additionally, camera-equipped UAS allow prospective terrorists to maximize the media impact of their actions, for example by sharing live footage of their airborne attacks on social media platforms.[18]

Box 2.
UAS as targets and vectors of cyberattacks

UAS can be either targets or vectors of cyberattacks, depending on whether they are hacked or used to hack other devices.

- **UAS as targets:** terrorists may seek to gain control over a UAS in order to capture or destroy it, modify its route or interfere with its data.[19] For example, by communicating fake information to a UAS's GPS system, the targeted device may be tricked into thinking that it is following the planned itinerary. Failing to regularly search for and patch flaws in software gives terrorists a significant opportunity to utilize these security holes to gain access to legally registered and operated UAS – potentially including those engaged in government and law enforcement missions. Terrorists could then potentially take control of an official UAS and use it against the vulnerable or crowded site it was originally designed to protect.

(continued)

17 Noting that "ISIL/Da'esh has repeatedly utilized UAS for attacks, surveillance, and battlefield propaganda in Iraq and Syria", it is argued in the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems that "such knowledge and experience might be brought back from there by returning foreign terrorist fighters (FTFs), or may serve as a blueprint for homegrown terrorists, including lone actors."

18 Security experts are also considering potential scenarios where terrorist groups integrate facial recognition software into UAS to enable targeted assassinations, or software developed to estimate crowd size is repurposed so that UAS can inflict more casualties (Don Rassler, UNOCT Expert Group Meeting, 6–7 October 2021).

19 In 2009, using software available on the Internet for $26, insurgents in Iraq successfully penetrated United States-owned UAS and intercepted live video feeds that the UAS were relaying back to a United States controller, thus revealing potential targets. The hacking was discovered only after the United States accessed militants' laptops, which contained hours of videotaped recordings.

- **UAS as vectors:** terrorists may use UAS to carry out cyberattacks on non-UAS targets. Under this scenario, UAS are employed as "cyber weapons" to deliver malware against other systems such as critical information infrastructure. With the expansion of 5G technology as the new standard for broadband cellular networks, UAS's "communication payloads" may potentially become easier-to-use tools to disrupt private wireless communications.

Source: Ley Best and others, 2020.

Terrorist groups may use UAS to achieve a variety of goals.[20] In relation to vulnerable targets, they may engage in:

- *Intelligence, surveillance and reconnaissance:* UAS may be deployed to collect information about sites' weak points – which may not be apparent from the ground – with the intention to subsequently exploit the detected vulnerabilities by launching a conventional or drone-based attack.
- *Attacks:* UAS may be directed to crash against a target with the intention of causing casualties and/or property damage. Terrorists may also take advantage of the payload capacity of UAS and use them to discharge explosive devices[21] or release chemical, biological, radiological or nuclear agents (see box 1). UAS may also discharge "communication payloads", for example by emitting radio frequency jammers to interfere with signals used by

20 See Resolution 2370 Technical Guidelines, submodule II, Types of terrorist use of UAS (1.1.3).

21 In August 2018, Venezuelan President Nicolás Maduro was the target of a failed assassination attempt using two GPS-guided, explosive-laden UAS. In another development, Da'esh has repeatedly employed UAS in conflict zones to discharge small grenade-size bombs. Although the use of such devices did not change the fate of the conflict, it laid bare the potentially deadly impact of misusing unsophisticated UAS created for hobbyist or recreational purposes.

security personnel during the unfolding of a major event. The impact of weaponized UAS may be multiplied by using them in "swarms". While UAS are still typically operated with one operator per drone, simultaneously launching a large number of devices to form a massive, coordinated fleet is not such an implausible scenario.[22]

- *Propaganda:* by using UAS to film their attacks on crowded or vulnerable sites, terrorists may seek to maximize the media impact of their actions by releasing shocking images. The use of UAS for propaganda purposes has been a hallmark of Da'esh's UAS strategy.[23]
- *Service/event disruption:* Even when UAS are not weaponized, when flying over controlled or restricted airspace they may severely interfere with the functioning of government services, critical infrastructure, major events, etc. In recent years, several UAS have been detected near or inside airports' perimeters worldwide, causing disruption to civil aviation and sizeable economic impacts and losses.[24] In none of those cases has any connection been established with a terrorist purpose, and it is safe to assume that most of the reported unauthorized UAS events were the result of operators' negligence, recklessness or their intention to defy rules and obtain media visibility.
- *Exposing or increasing targets' vulnerabilities:* It cannot be excluded that UAS may be used for the specific purpose of diverting the attention of law enforcement and security personnel and resources away from the real target. Left unprotected, the latter may be subsequently attacked via conventional means or weaponized UAS, exploiting its increased vulnerability.

22 A "swarm" scenario occurred in 2018, when two of the Russian Federation's airbases in the Syrian Arab Republic were attacked by a fleet of 13 coordinated, GPS-controlled and explosive-laden UAS. Critically, neither the perpetrators of the attack nor the launching site has been identified.

23 In addition to weaponizing UAS, Da'esh has employed them as strategic tools to produce drone imagery that can feed its sophisticated propaganda machine.

24 The events that brought the issue to the attention of the general public occurred at London Gatwick Airport between 19 and 21 December 2018, when 115 drone sightings led to the closure of its single runway. Overall, the disruption led to the cancellation of over 1,000 flights and affected some 140,000 passengers. Since then, many airports across the world have experienced different degrees of drone-related interference.

Tool 1.
Islamic State and Drones: Supply, Scale, and Future Threats – Combating Terrorism Center at West Point, 2018
(https://ctc.usma.edu/islamic-state-drones-supply-scale-future-threats)

This report seeks to understand how Da'esh managed to develop its drone programme within a relatively short period and effectively use modified commercial UAS as weapons. It highlights some of the broader threat and policy implications associated with the pioneering use of UAS by Da'esh, including how its "model" could serve as an inspiration for other actors seeking to develop their own hybrid warfare capabilities and strategies.

The report highlights how countries might target UAS used for terrorist purposes and prevent their availability, focusing upon the following areas:

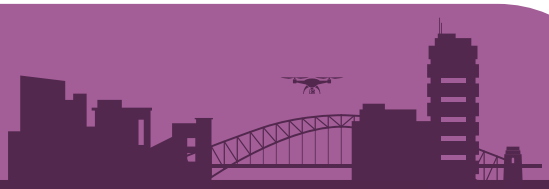
- Conducting better due diligence of transactions being shipped to the doorstep of a complicated warzone;
- If this is not possible, gaining access to a government or neutral third-party that could provide this type of assistance;
- Working with the industry to bolster or enhance how commercial UAS and their associated packing can be tracked or retraced after devices or components have been recovered in conflict areas;
- Dedicating more attention and resources to efforts that aim to prevent the delivery of select dual-use items to major conflict zone areas;
- Investigating and mapping out supply chain networks;
- Retracing specific equipment – like drones – found in the field so existing procurement channels can be closed more rapidly.

Tool 2.
How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools – Rand Corporation, 2020
(www.rand.org/pubs/research_reports/RR2972.html)

This tool proposes a conceptual framework towards the categorization of UAS-related cyber threats, covering the use of UAS as both targets and vectors of cyberattacks. In order to illustrate the range of current threats, the report classifies UAS-enabled cyber-attacks using the STRIDE taxonomy, which stands for:

- **Spoofing:** Violation of authentication protocols, enabling attackers to pretend to be something or someone that they are not. Where UAS are the target, spoofing could include claiming to be the authorized recipient machine for drone data.
- **Tampering:** Violation of a system's integrity by making some kind of modification to it. E.g., a UAS is used to deliver malware to a target computer using proximity to access an unsecured wireless network.
- **Repudiation:** Attackers refuse to take responsibility for an action. E.g., when UAS are cyber weapons, the operator could use repudiation to distance their identity from the consequence by interfering at the communication node loosely affiliated with the point of damage or disruption.
- **Information disclosure:** Violations of the principle of confidentiality. E.g., infiltrating a UAS sensor data system to access video, audio or other data.
- **Denial of service:** Involving, for example, infecting drone control software to make the devices unresponsive to user inputs.
- **Elevation of privilege:** Violation of the principle of authorization to perform an action. E.g., hijacking a UAS by posing as the legitimate controller.

[2]



Vulnerable targets' exposure to UAS-related terrorist attacks

Countries often face distinctive sets of challenges in protecting people and property from the risk of UAS-related terrorist attacks on open-air sites where large crowds gather for sporting or cultural events, tourist attractions and religious ceremonies, among others:

- *Poor recognition of the nature and extent of the threat:* threats posed by UAS have not yet been fully considered in the security plans of several open-air vulnerable targets. Exclusive reliance on security plans aimed at stemming the threat of land-, water- or cyber-based attacks may leave the site exposed to incursions carried out from the sky via UAS. Removing one set of vulnerabilities will inevitably incentivize hostile actors to exploit the next, unaddressed group of weaknesses.

  During the unfolding of a crisis, a substantial difficulty for law enforcement and security personnel is identifying the motivation behind a specific UAS event. While the ability to distinguish between actions triggered by negligence and malicious intent may be critical to adapting the response, scarce available information, contradictory reports and the need to act quickly often make this particularly challenging.

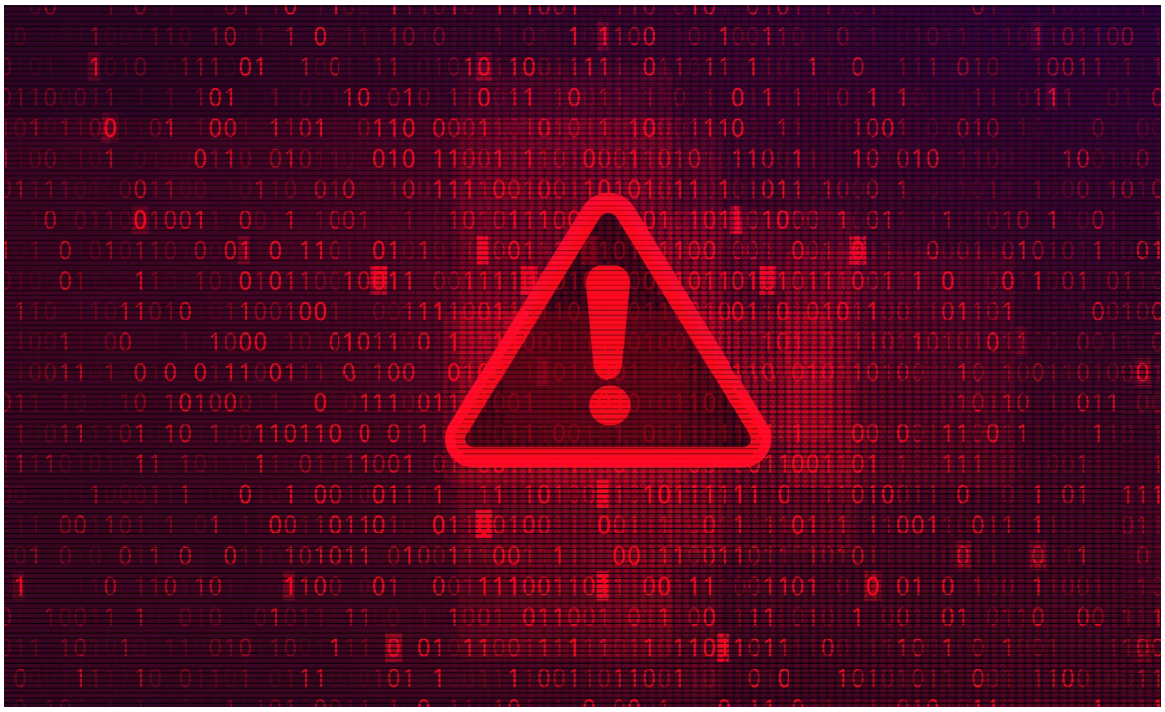
- *Inadequate regulatory frameworks:* Wherever they are in place, national regulatory frameworks – including to protect vulnerable sites against UAS attacks – are still largely in their infancy. Moreover, the market is evolving significantly faster than the applicable regulations. In their efforts to strike the right balance between the need to recognize and promote legitimate applications of UAS and the need to prevent their abusive exploitation, including for hostile purposes, many countries still have to address a series of pivotal issues. These range from the attribution of effective and proportionate powers to law enforcement and other government authorities against hostile drone activity, to the creation of the proper incentives for operators of vulnerable sites to strengthen their facilities against potential UAS attacks, for example through the shaping of public-private partnerships (PPP). Some countries equipped with a regulatory framework may need to address undefined or overlapping authorities in often complex multi-agency environments while those with little to no UAS regulatory understanding require familiarization and integration.

- *Unavailability of or challenges related to the use of counter-UAS (C-UAS) technologies:* C-UAS technologies are far from

being ready-to-use tools. They cannot be deployed without first conducting accurate assessments of systems' compliance with domestic laws and the specific characteristics of the site(s) where they are supposed to be used. Also, as UAS-related technologies are advancing progress at a very rapid pace, C-UAS technologies may quickly become obsolete. Additionally, system complexity means that they are often costly and that authorized users need to undergo extensive training and familiarize themselves with their features before they are ready to employ them in a safe manner.

With regards to their use to protect vulnerable targets, in particular, the range of available counter measures may be significantly limited. For example, a given technology may represent an effective and reasonable solution against UAS used for terrorist purposes in a remote and deserted place while being totally inadequate to protect the airspace over an airport or a crowded event. Moreover, destroying a UAS that is flying over a densely populated urban area, or causing its operator to lose control of it, could cause the device to crash on the ground with severe damage to people and property, particularly when the downed UAS is weaponized and leads to an uncontrolled explosion. Additionally, the use of electronic counter-drone measures in environments with complex electromagnetic activity, such as urban areas, may be limited by the risk of interfering with radio frequencies supporting legitimate services.

- *UAS fatigue:* As emphasized in the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems "many UAS incidents will involve negligent, unwitting or careless misuse, with no terrorist intent. Over time, dealing with a succession of minor UAS incidents may spawn a sense of complacency among authorities and the general public. This may in turn cause officials and the public to overlook vulnerabilities, early warning signs, public reporting, or credible threats, thus increasing vulnerability to an actual attack" (Good practice 5, GCTF, 2019).



Box 3.
Vulnerabilities in IT infrastructure for UAS

A distinctive set of vulnerabilities can be present in the IT infrastructure set up by UAS manufacturers. The opportunities for hostile intrusions can be magnified by producers offering services based on a complex ecosystem made of several components and third-party applications meant to expand the functionality of the marketed device.

In 2018, a leading UAS manufacturer discovered a vulnerability in its cloud infrastructure. The vulnerability in question could have allowed an attacker to take over users' accounts and access private data such as photos and videos taken during a drone's flight, a user's personal account information, and flight logs including location data. Following the discovery of the vulnerability, the manufacturer did not only close it but also reworked its approach to how its IT systems manage trust and user authentication.

Source: www.wired.com/story/dji-drones-bugs-exposed-users-data/.

[3]

Risk mitigation and response: stakeholders' roles and good practices

This chapter examines the way in which individual stakeholders involved in the UAS ecosystem – both institutional and non-institutional actors – can contribute to mitigating the risk of UAS-enabled terrorist attacks, facilitate crisis management and recovery efforts, including by developing public-private partnerships (PPPs). In this sector, the creation of close and durable PPPs is critical due to the specific characteristics of markets for the development, manufacturing and commercialization of UAS devices and counter-UAS technologies, where private-sector actors play a leading role.

3.1 Member States

3.1.1 Policymakers

Government agencies are responsible for setting up an overall framework conducive to the prevention and management of UAS-related incidents, and the swift recovery and rehabilitation of sites and people affected by such incidents.

In parallel, government agencies need to provide the legal, institutional and collaborative working environment to leverage UAS technologies as tools to protect vulnerable sites exposed to terrorist attacks in general while preserving human rights.

In pursuing these broad objectives, it is critical that government actors involve the various groups in the UAS ecosystems (different user communities, UAS manufacturers, providers of counter-UAS solutions, academic and research institutions, civil society organizations, activists, etc.) in one or more stages of the policymaking process. Their involvement would be instrumental in ensuring that regulatory outcomes: (1) take into account the expectations and challenges faced by a broad base of end users; (2) reflect industry concerns; (3) account for relevant – including emerging – threats, attack modalities and scenarios detected by research institutions, the intelligence community, etc.; and (4) take into account the concerns and needs of civil society regarding the use of UAS in the protection of vulnerable targets.

Tool 3.
Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems – Global Counterterrorism Forum (GCTF), 2019
(www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3d&portalid=1)

The good practices contained in the Berlin Memorandum are addressed to governments in support of their efforts to identify, develop and refine policies, practices, guidelines, regulations, programmes, and approaches for countering the use of UAS for terrorist purposes. The Memorandum condenses the takeaways and experiences shared by governments, law enforcement agencies, multilateral organizations, private industry and other subject matter experts during four regional workshops held in Germany, Jordan, the Republic of Korea and the Netherlands in 2018 and 2019.

The Berlin Memorandum identifies 26 good practices in four broad areas:

- *Assessing the risk, assessing vulnerabilities and raising awareness:* States should integrate the potential terrorist use of UAS into their routine risk assessment procedures to identify vulnerabilities and protection gaps together with relevant stakeholders. States should take into consideration all potential ways terrorists may use UAS and should anticipate technological developments and other factors that might have an impact on the threat, and respond to new and innovative ways that terrorists may employ UAS technologies.

- *Enhancing information-sharing, engaging with relevant stakeholders and educating the public:* The multifaceted threat of terrorist use of UAS requires a comprehensive and coordinated approach that includes States, regional and international governmental organizations, and non-traditional stakeholders. National efforts to counter the threat of terrorist use of UAS should be complemented by appropriate regional and international measures as appropriate. States should also engage with the general public to promote education on responsible UAS use and foster appropriate responses to suspicious UAS.
- *Implementing policies and regulations, establishing crisis planning:* States should have in place clear and enforceable policies and regulations that deter and minimize the potential for proliferation and misuse of UAS by terrorists and other malicious actors, enable effective countermeasures against UAS, and enable effective investigations, prosecutions and sanctions following UAS incidents. Governments should also develop crisis management and mitigation strategies to react adequately to UAS incidents.
- *Developing tactical countermeasures and technical solutions:* States should implement and routinely review protection measures and other technical solutions, including necessary equipment and training of the relevant authorities, that allow them to identify and counter UAS flown with malicious intent. Before using countermeasures, States should, in cooperation with relevant stakeholders, evaluate and mitigate negative effects of countermeasures, while being mindful of the fact that they can be resource-intensive and require considerable training needs.

(continued)

Tool 4.
UAS Toolkit – International Civil Aviation Organization (ICAO)
(www.icao.int/safety/UA/UASToolkit/Pages/default.aspx)

Developed as a web-based initiative in cooperation with industry and ICAO's network of international expert partners, the Toolkit compiles best practices and regulations in support of Member States' efforts to develop effective operational guidance on the use of UAS. The Toolkit provides access to existing regulations from around the world; resources on technical and operational issues, including on training and education for UAS operators; and materials to guide countries' awareness campaigns.

3.1.1.1 Counter-UAS strategies

Addressing the terrorist threat posed by the use of UAS is a multi-stakeholder responsibility that requires coordination and unity of purpose. One of the overarching goals for Governments is to initiate, lead and sustain this coordination effort by clearly outlining the overall vision and approaches that should underpin countries' stance to protect societies from the use of UAS for terrorist purposes. This implies, crucially, determining the channels through which different departments with regulatory and/or operational mandates and responsibilities in the field of UAS need to join forces and synchronize their actions, as well as identifying the appropriate types and modalities of public-private partnerships (e.g., information-exchange platforms with industry, awareness-raising programmes for site operators, etc.).[25]

The terrorist threat posed by UAS may be considered and addressed in dedicated counter-UAS strategies[26] or in the framework of broader counter-terrorism/national security strategies, including those focusing on the protection of vulnerable targets. When multiple documents and institutional frameworks are employed, it is essential that the various elements form a coherent whole in terms of vision, approaches, procedures and expectations.[27] Finally, some countries may choose to incorporate their approach to preventing and countering UAS-related threats as a component of their overall strategy aimed at incentivizing the development of safe, growth-generating and socially useful UAS-based economies.[28]

25 Resolution 2370 Technical Guidelines also emphasize the need for a comprehensive, whole-of-government approach to counter UAS acquisition and use by terrorists and highlight the need for regular reviews through an inclusive, multi-stakeholder process. See submodule II, National policy or strategy (2.1.1).

26 The United Kingdom has followed this approach by developing a dedicated counter-UAS strategy (United Kingdom, 2019).

27 Some countries may develop counter-UAS strategies at the level of specific governmental departments. The United States Department of Defense (DoD), for example, has crafted a dedicated strategy (United States, 2021) following the observation that small UAS pose increasing hazards to its operations, personnel and facilities, whether those hazards are created by State- or non-State actors. Clearly, this type of agency-specific strategy needs to fit into broader governmental approaches relating to the management of UAS-related threats.

28 Transport Canada's Drone Strategy, for example, features an explicit security component. Adopted in 2021, the document provides Canada's strategic vision for UAS, focusing on raising awareness of the significance of UAS and outlining policy priorities to be attained by 2025 (Canada, 2021).

Procedurally, when they set about developing a counter-UAS strategy, countries should opt for initiating a whole-of-government consultation aimed at producing a focused, high-level strategic document.

Some of the priority issues that a national-level strategy needs to consider are:

- *Civil-military connection:* A critical dimension of the inter-agency coordination patterns is the collaboration between civil and military domains. In this regard, the Berlin Memorandum encourages countries to "take into consideration the experiences and lessons learned from national defense forces [as] many military branches have already gained experience in countering the use of UAS by violent non-state actors during instances of armed conflict"[29] (Good practice 11, GCTF, 2019).
- *Coordination between aviation-related authorities:* Any Government-level strategy needs to promote close communication and information-exchange channels between civil aviation authorities (CAA), air navigation service providers (ANSP) and agencies in charge of aviation safety and security. At a basic level, effective interaction between these agencies is necessary to ensure that UAS regulatory frameworks are relevant and up to date. Additionally, as emphasized by the Berlin Memorandum, "as countermeasures are likely to cause unintended consequences, particularly in relation to the safety of civil aviation and radiofrequency-based (communication) systems … [CAAs and ANSPs] can assist in mitigating consequences to the greatest extent" Good practice 13, GCTF, 2019). They can also "provide valuable early input on the consequences of countermeasures on aviation safety and operations."
- *Involvement of operators of vulnerable targets:* Governments need to determine what type of government programmes and initiatives should be in place to support

29 The Berlin Memorandum notes, however, that "not all lessons learned can be transferred from theatres of conflict to a counter-UAS strategy in a domestic setting outside the context of armed conflicts." Indeed, many of the systems were designed for the battlefield and are not viable options for use in domestic airspace above populated areas.

site operators in increasing their resiliency against terrorist-driven UAS attacks. Depending on budget availability, incentives can take a variety of forms including grants, funding schemes, tax breaks, etc. Governments may also support site operators by connecting them to available expertise such as specialized advice on risk and crisis management offered by competent national security or law enforcement units.

Box 4.
Recommendation for a whole-of-government UAS strategy – International Civil Aviation Organization (ICAO)

Given the complexity of the subject and the sheer number of government agencies involved, ICAO's UAS Toolkit recommends an approach whereby States put forward a whole-of-government UAS strategy seeking to achieve the following goals:

- A roadmap that identifies safety, security and economic objectives of the future UAS industry;
- A government interdepartmental UAS committee to share information and help departments operating UAS to plan their activities;
- A methodology to align the needs of the industry with government resources;
- Coordination activities to enhance industry stakeholders' access to funding to explore new technologies and market applications.

Source: www.icao.int/safety/UA/UASToolkit/Pages/default.aspx.

Additionally, when making efforts to protect civil aviation infrastructure from acts of unlawful interference carried out with unmanned aircraft, it is recommended that States also take into consideration measures described in Chapter 19, Protection of civil aviation infrastructure against unmanned aircraft, of the ICAO Aviation Security Manual (Doc 8973, Restricted).

Case study 1.
The European Union strategy on countering UAS in a counter-terrorism context

The current European Union approach is structured as a broad inter-agency and cross-sectoral endeavour leveraging the work of various European Union institutions and agencies, law enforcement and defence networks, and funded consortiums. Their activities and initiatives have given rise to a rapidly evolving legal, policy and institutional context whose main components are:

- The 2020 EU Security Union Strategy and the updated Counter-Terrorism Agenda for the EU (2020);
- The European Union's UAS regulatory framework for safe drone operations, enshrined in Regulations 2019/945 and 2019/947;
- Work in progress on the creation of a UAS traffic management system "U-Space" package;
- The Action Plan on synergies between civil, defence and space industries (2021);
- Initiatives spearheaded by the European Commission's Joint Research Centre on physical protection against UAS, including the protection of critical infrastructure;
- The EU Handbook for securing urban areas from non-cooperative UAS – currently the subject of targeted consultations and scheduled for public release in late 2021.

Source: UNOCT-organized Expert Group Meeting (29 June 2021).

Case study 2.
United Kingdom Counter-Unmanned Aircraft Strategy

Intended to be a forward-looking document, the Strategy is expected to evolve along with the underlying technology to keep ahead of the UAS-related threat. It sets out the actions that the Government plans to take to address the malicious use of small UAS[30] and reduce the risk posed by their highest-harm illegal use on the basis of four strategic outcomes:

1. Developing a comprehensive understanding of the evolving risks posed by the malicious and illegal use of UAS;
2. Taking a "full spectrum" approach to deter, detect and disrupt the misuse of UAS;
3. Building strong relationships with industry to ensure their products meet the highest security standards;
4. Empowering the police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance.

The Strategy has been shaped to complement CONTEST, the United Kingdom's counter-terrorism strategy, as well as the United Kingdom's serious and organized crime strategy.

Source: United Kingdom, 2019.

30 The United Kingdom Civil Aviation Authority defines "small UAS" as those weighing less than 20 kg. The scope of the Strategy is limited to small UAS in view of the significant barriers to obtain and operate heavier ones.

Case study 3.
Singapore's approach to UAS-related security risks

Although there have been no occurrences of direct, weaponized drone attacks in Singapore, country authorities recognize that UAS intrusions can still present other risks, such as safety risks when intruding into high-profile events with high human footfall. Also, in June 2019, UAS sightings around Changi Airport caused runway operations to be restricted temporarily, causing flight delays and diversions.

Singapore's overall approach seeks to balance safety/security risks with legitimate uses of UAS and relies on three pillars:

- **Regulation:** In 2015, Singapore's Parliament passed the Unmanned Aircraft (Public Safety and Security) Bill to regulate drone operations and, in 2019, the Air Navigation (Amendment) Bill to enhance drone controls. These pieces of legislation are based on three basic principles: (1) Certain drone flights require permits (e.g., within 5 kilometres of a civil/military aerodrome, or within a protected/restricted/danger area, or operating above 200 feet (approximately 60 metres) above sea level); (2) dangerous drone activities are prohibited (e.g., any discharge from UAS); (3) registration is required for UAS weighing over 250 grams).

  The applicable penalties are commensurate with the impact caused by illegal UAS operations (e.g., first-time offenders flying over protected areas without permits liable for penalties including a fine of up to $50,000, and/or imprisonment for up to two years).
- **Enforcement:** Authorities have been responding to, investigating, and prosecuting non-compliance with regulations.
- **Education:** Strong public education policies are implemented to promote responsible use of UAS and improve awareness of drone regulations.

Source: Presentation by Mr. Lee Peng Yang, Senior Assistant Director, Joint Operations Group, Ministry of Home Affairs, Singapore, at the UNOCT Expert Group Meeting (6–7 October 2021).

3.1.1.2 General UAS legal frameworks

Although countries adopt a variety of regulatory approaches to UAS operations within their territories, most of them prioritize a "safety-first principle". This typically translates into a series of requirements such as pilot licensing, aircraft registration, insurance and the creation of no-fly zones (typically around critical infrastructure). While in many countries these requirements are only mandatory for commercial UAS, some jurisdictions have recently extended binding registration schemes to small UAS used for recreational purposes.[31]

In developing the various segments of their regulatory frameworks, ICAO recommends

31 Resolution 2370 Technical Guidelines refer to the need to put in place adequate legislative and regulatory frameworks for the prevention and mitigation of threats posed by terrorist acquisition and use of UAS, and outline some of the challenges in this regard. See submodule II, National legislation and regulations (2.1.3).

that States "consult with key stakeholders early in the regulatory development process. Formation of a joint government/stakeholder UAS working group tasked with reviewing existing legislation and making recommendations for a new UAS regulatory framework could be effective. UAS stakeholders should include manned aviation operators, manufacturers and organizations. Once regulations have been drafted, soliciting feedback from both aviation and non-aviation stakeholders will help to ensure that the regulations capture all relevant requirements."[32] Furthermore, it is fundamental that drone-related "legislation keeps pace with the evolving threat, is responsive to operational experience, and directly informs training and guidance."[33]

Box 5.
Unmanned Aircraft System Traffic Management (UTM)

Existing air traffic management systems are ill-suited to handle the increasing traffic volumes generated by a wide variety of UAS, and their flying patterns. For this reason, an important aspect of the prospective regulatory landscape for UAS will be the creation of UAS traffic management (UTM) systems, which will be aimed at controlling low-altitude UAS traffic patterns, defining restricted airspace, and selectively granting or denying access to restricted areas.[34]

The safe development and deployment of UTM systems may also assist authorities in identifying which UAS are operating legally and those that may be operating illegally or with malicious intent. They could provide key information during incident response activities.[35]

However, as countries increasingly set up regulatory and operational frameworks independently of each other, a potential challenge will be the creation of several uncoordinated and incompatible UTM systems. Additional challenges include the potential for sensitive civilian or government information being unsafely transmitted as a result of incompatible UTM systems. Furthermore, UAS detection technologies (see section 3.1.2.2) will still be required at specific locations and events to deal with non-compliant devices. Issues of compatibility between UAS detection technologies and UTM might then become increasingly important in the future.

32 ICAO Toolkit, Additional Considerations (www.icao.int/safety/UA/UASToolkit/Pages/default.aspx).

33 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf.

34 UTM systems may be fixed or moveable depending on their uses. Fixed UTM systems would provide uninterrupted coverage for areas such as the congested, low-altitude airspace over big urban areas; portable systems would be more suited for transportation to particular sites on the occasion of specific events (e.g., a crowded site, a disaster-affected area).

35 For this purpose, ICAO developed UTM guidance material, which can be found at www.icao.int/safety/UA/Pages/UTM-Guidance.aspx.

Case study 4.
The European Union regulatory framework for UAS

In 2019, the European Union introduced a regulatory framework intended to spur the economic and social benefits offered by UAS while subjecting drone manufacturers and operators to a series of restrictions on the grounds of safety and public security, protection of personal data, respect for privacy, the environment and protection against noise. By adopting a risk-based approach, EU Regulations 2019/947 and 2019/945 do not distinguish between leisure or commercial activities. Rather, they take into account the weight of the UAS and the operation it is intended to perform. According to this concept, operations are classified as belonging to the "open", "specific" or "certified" categories depending on their assessed level of risk:

- Open category: Covers the lowest-risk operations. No authorization is required before starting a flight.
- Specific category: The drone operator needs to obtain an operational authorization from the national competent authority before starting the operation. To obtain such authorization, the operator is required to conduct a safety risk assessment, which will determine the requirements necessary for the drone's safe operation.
- Certified category: The safety risk is considered to be the highest, requiring a certificate for the drone operator and the aircraft as well as the licensing of the remote pilot(s).

Source: EU Regulations 2019/947 and 2019/945.

Case study 5.
United Arab Emirates' risk management framework for unauthorized aircraft within controlled airspace

In November 2016, the Civil Aviation Authority of the United Arab Emirates (UAE) introduced contingency measures for unauthorized aircraft within controlled airspace (Safety Decision 2016-16). The regulation provides guidance to air navigation service providers (ANSP) on how to tactically risk assess intrusions into controlled airspace and take mitigating actions while ensuring those measures are proportionate to the risk posed by the intruder.

The regulatory framework is structured into the following areas of procedural action:

- The establishment, implementation and maintenance of a safety management system by air traffic services units;
- A tactical risk assessment to determine the appropriate actions to be taken in the event of airspace infringement.

The full text of Safety Decision 2016–16 is available as a paper presented by the United Arab Emirates during ICAO's Thirteenth Air Navigation Conference: www.icao.int/Meetings/anconf13/Documents/WP/wp_097_en.pdf.

METEOROLOGY DRONES

DRONE DELIVERY

DRONE FLYING REGULATIONS

Tool 5.
Model UAS Regulations – ICAO
(www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx)

ICAO Model UAS Regulations are designed to support countries in establishing and refining their national guidelines for domestic UAS operations. They are the outcome of ICAO's review of existing UAS regulations worldwide, aimed at identifying commonalities and best practices consistent with the ICAO aviation framework.

The Model UAS Regulations are available for download from the ICAO website and are expected to be regularly updated to keep pace with the evolution and expansion of national UAS programmes. Countries can choose to adopt the model regulations in their entirety or pick and choose provisions to supplement existing national frameworks. The modern regulations cover the essential requirements for countries in terms of UAS certification and safe operation.

3.1.1.3 Supporting the development and proportionate use of counter-UAS (C-UAS) technologies

Governments have the overall responsibility to create an enabling environment for the development and appropriate use of C-UAS technologies.[36] From a broad policymaking perspective, at least three sets of issues are worth considering:

- The determination of which government/law enforcement agencies are mandated to carry out C-UAS operations and based on which legal safeguards and requirements.[37] In entrusting certain national authorities with C-UAS powers, Governments need to consider which conditions should be in place to ensure a proportionate and human rights-compliant use of such technologies. Relevant regulations should, for

36 Resolution 2370 Technical Guidelines provide an introduction to and overview of C-UAS technologies, including challenges and concerns in this regard. See submodule II, Counter-UAS systems and techniques (3.1); Capability, normative, and operational development for countering UAS (2.2); and Development of UAS countermeasures (3.8).

37 The way in which countries currently address this issue is not homogeneous; while some legal frameworks do define C-UAS authorities – sometimes in a fragmented and complex manner – others do not contain any dedicated provisions.

example, incorporate basic procedural and evidentiary standards – such as the need to demonstrate the probable cause or equivalent requirements – before law enforcement agencies are allowed to take disruptive action against threatening UAS. C-UAS policies may also consider whether disruptive law enforcement interventions should be preceded by a warning or notification which provides the UAS operator with a reasonable opportunity to take corrective action (e.g., having the device change direction, land outside the security perimeter, etc.).

- As C-UAS technologies are often not ready-for-use tools and require the acquisition of substantial technical skills, regulatory frameworks may condition their purchase and use by competent agencies on the passing of appropriate testing to ensure that they will be employed in a safe and competent manner.
- The ways in which government agencies will engage with industry stakeholders in charge of developing C-UAS. Such engagement should be broad in scope and aim, as a minimum, to ensure that the technologies eventually integrated into counter-UAS devices meet regulatory specifications and restrictions. Governments should also determine – depending on budget availability, competition rules in force, etc. – its policies for funding scientific and technological developments to support the C-UAS industry, including the possibility to help small companies and start-ups design innovative solutions.[38]

Case study 6.
The Courageous project: A methodology for choosing the right C-UAS technology

The Courageous project is implemented by the Robotics & Autonomous Systems lab, a research unit of the Belgian Royal Military Academy,[39] based on the rationale that as "UAS become more and more available, law enforcement agencies find themselves confronted with the novel task of having to police the access to the lower airspace. Commercial providers have already developed a wide range of solutions to this extent, but the capabilities of these systems are hard to benchmark. The result is that end users have a hard time in matching the right tools to the specific use cases that they encounter." In 2019, for example, over 100 commercial C-UAS systems were available, with performance claims often unsupported by evidence and different test methodologies making comparisons very difficult.

38 The UK Counter-Unmanned Aircraft Strategy, for example, envisages the creation of strong partnerships with the C-UAS industry aimed at, among others, producing a single government catalogue of approved domestic counter-drone capabilities. In turn, the catalogue is expected to be made available to partners to help them make effective procurement decisions (UK Counter-Unmanned Aircraft Strategy, p. 24).

39 With the support of the European Commission.

The Courageous project addresses these challenges by developing a standardized test methodology for UAS detection, tracking and identification systems. The methodology is based on a series of standard user-defined scenarios (e.g., prison and airport security, critical infrastructure protection, border security, drugs and human trafficking). For these scenarios, operational needs and functional performance requirements are extracted by the Courageous end users. Based on this information, an integral test methodology will be developed, allowing for a qualitative and quantitative comparison between different counter-UAS systems. The test methodology will be validated during three user-scripted validation trials.

Sources: https://mecatron.rma.ac.be/index.php/projects/isf-courageous/; and Intervention by Geert De Cubber, Royal Military Academy, Belgium, at the UNOCT-organized Expert Group Meeting (6–7 October 2021).

Case study 7.
Defence and Security Accelerator (DASA) funding programme – United Kingdom

In 2020, the Defence and Security Accelerator (DASA) – a cross-government initiative of the United Kingdom's Ministry of Defence – announced a competition for funding proposals that could develop C-UAS technologies and demonstrate how these can be integrated to form a capable system. All proposals needed to show how the featured technologies would be able to be matured into an operational system against threats posed by small commercial, improvised or military grade UAS and include evidence of:

- an innovative approach to development
- clear enhancement over existing C-UAS options
- an explanation of how technologies can be integrated into solutions
- an explanation of how the work can be exploited

Source: www.gov.uk/government/organisations/defence-and-security-accelerator.

3.1.1.4 Education and awareness

A significant proportion of UAS end users – especially for recreational purposes are not proactive in terms of accessing relevant laws and upholding security standards. An important role for government authorities is thus to ensure that (often) technically complex safety and security regulatory frameworks are brought to the attention of and made understandable to them.

Any awareness-raising programme needs to account for the extreme heterogeneity of members of the UAS community – in terms of age, gender, motivation and levels of education. Key information can be conveyed through a variety of means and techniques, including vendors' online platforms, social media, leaflets that UAS manufacturers deliver together with their products and user manuals, compulsory or voluntary training and awareness-raising events for UAS operators.[40]

Case study 8.
Drone Safety resource hub

Drone Safety is a resource hub maintained by the Government of Canada. It provides informational and educational materials for drone operators, ranging from the steps necessary to register a drone to obtaining a pilot certificate. An online form allows users to report a drone incident.

Source: https://tc.canada.ca/en/aviation/drone-safety.

40 Governments may also consider leveraging drone-focused publications and the media as channels through which to amplify users' security awareness, as envisioned by the UK Counter-Unmanned Aircraft Strategy. The same Strategy also plans to "encourage the public to report instances of drone misuse and equate wider vigilance campaigns with suspicious drone use, as much as other terrorist or criminal activity. By better publicizing prosecutions for drone offences we will reinforce this narrative and make it harder for people to claim ignorance when prosecuted" (United Kingdom, 2019, p. 21).

Tool 6.
Public Outreach: Education and Awareness – ICAO UAS Toolkit
www.icao.int/safety/UA/UASToolkit/Pages/Narrative-Considerations.aspx

To ensure the successful integration of UAS into the current manned aviation system, it is critical that pilots, operators, manufacturers, buyers, sellers, importers and the general public are all aware of UAS. Most importantly the remote pilot needs to accept responsibility and understand that he/she is responsible and accountable for the safe operation of the UAS. Slogans such as "YOU are now a REMOTE PILOT" or "YOU are in CONTROL" of your UAS can be incorporated into awareness campaigns. The message should also include a reminder of the risk to safety that flying a UAS close to an airport or aircraft could pose.

Education:
Education should be provided to manufacturers, importers and sellers of UAS in order for them to convey key safety information directly to the buyers of UAS. This awareness and/or education should include the following:

- Online reference to the specific State's UAS guidance or regulations, web links must be easily accessible;
- A simple, clear web-based handout of the dos and don'ts when operating UAS;
- Pamphlets or educational material regarding guidance and/or regulations should be provided to manufacturers, dealers and sellers of UAS, law enforcement agencies and academic institutions.

(continued)

Safety campaigns:
Information booths at conferences, airshows and trade shows may be effective. Consider utilizing existing events as UAS awareness platforms. Other entities that could provide a role in providing education and awareness are listed below. By using the services of these entities, the information can be transferred globally.

- Immigration offices, including travel advisories;
- Tourism bureaus;
- Social media including frequently updated web pages such as YouTube and blogs;
- Websites and a handbook explaining the regulation, leaflets, media communication campaigns can all be used to inform the general public and UAS operators;
- Registered operators may also be informed by email if the civil aviation authority establishes mailing lists;
- A frequently asked questions (FAQ) page may be useful, including a process to answer questions by email;
- Online situational awareness and flight planning tools;
- Regulatory authority's safety campaigns as part of their State safety programme/ aviation awareness.

3.1.1.5 Intergovernmental collaboration

Any overarching national policy aimed at countering the activities of UAS used for terrorist purposes should determine:

- How it can benefit from lessons learned and the experiences of other countries, including with respect to preserving human rights and fundamental freedoms;
- How local achievements in understanding and mitigating UAS-related threats and managing UAS-related crises can be usefully shared with the wider community;
- How to support investigative activities and criminal proceedings that are taking place in other countries about UAS-related terrorist acts or preparations thereof with transnational elements;
- How to ensure that the national policy is compliant with the rule of law and human rights.

The above objectives require that countries engage proactively with their foreign counterparts via bilateral, regional and/or multilateral forums and arrangements. The scope for setting up collaborative endeavours is particularly broad[41] and includes:

- The harmonization of definitions and classifications of UAS systems, related incidents and standards for the testing of UAS countermeasures. A baseline of shared terminologies and working standards will be instrumental in the compilation of internationally meaningful statistics and, consequently, for cross-country comparison

41 See Resolution 2370 Technical Guidelines, submodule II, International and regional cooperation including information-sharing (2.5).

purposes (e.g., in relation to the assessment of threat levels, the effectiveness of countermeasures, the presence of gaps in practices and policies, etc.) (Good practice 8, GCTF, 2019).

- The establishment of mechanisms for national aviation authorities to share experiences with each other with a view to aligning regulations, especially among neighbouring countries.
- The possible introduction – through multilateral initiatives to be pursued within the World Customs Organization – of a specific customs classification for UAS to improve the ability to detect suspicious UAS consignments.[42]
- As highlighted in the ICAO UAS toolkit, the initiation or strengthening of collaborative endeavours in the following areas:
  - Technical, safety, and operational requirements for the safe operation of UAS;
  - Research and development, including sharing outcomes and identifying opportunities to collaborate on future projects and, in particular, traffic management;
  - Information systems;
  - Enforcement and compliance strategies including partnerships with law enforcement agencies;
  - Programmes for training State personnel who are responsible for UAS oversight.
- Use of bilateral and regional arrangements and multilateral platforms to increase the exchange of law enforcement information about threats, modus operandi, the identity, whereabouts and activities of suspects, etc.
- The establishment of legal bases and channels – via domestic extradition/mutual assistance rules and/or criminal justice treaties and instruments – to ensure that evidentiary items can be easily exchanged and fugitives surrendered in support of criminal proceedings involving UAS-related terrorist attacks or preparations thereof.

Box 6.
Future international cooperation challenges on disrupting terrorist UAS

The advent of the Internet of Things, supported by 5G technology, may soon generalize the possibility to have UAS piloted via by the Internet without the need for any physical proximity between the aircraft and its operator (Palestini, 2020). Such a scenario is likely to multiply the number of jurisdictions involved in a single UAS incident and have significant impacts on countries' ability to cooperate in law enforcement and judicial matters. A jurisdiction from which a drone is being operated, for example, may need to be able to swiftly execute a request coming from the jurisdiction where the drone is flying threateningly, to identify and disable the pilot. Some of the measures that are currently needed to ensure Governments can effectively cooperate with each other against cybercrime may soon become key tools to stem hostile drone activity as well.

42 The lack of a specific customs classification standard for UAS means that legitimate UAS manufacturers currently use terms, such as digital cameras, to describe the content of their shipments via international routes.

3.1.1.6 Employing UAS to protect vulnerable targets

The same technologies that drive UAS employed for terroris purposes can also be used by public authorities and site operators to facilitate the achievement of important risk and crisis management objectives. There are many potential applications of UAS as tools to protect vulnerable targets from terrorist attacks (whether or not these attacks are carried out using UAS), and policymakers should encourage the proactive use of UAS for these purposes. Specifically in relation to the protection of vulnerable targets in non-conflict zones, the most relevant and direct uses of UAS appear to be the following:

- Spotting vulnerabilities that would not otherwise be visible or easily perceptible from the ground, especially in large sites (e.g., fragilities in the perimeter wall, sensitive areas left insufficiently protected from potential aerial attacks).
- Assisting in crowd management efforts, such as at major sporting events and concerts, for example by alerting security personnel about excessive numbers of visitors concentrated in certain areas.
- During the unfolding or in the immediate aftermath of a terrorist incident, supporting crisis management efforts. For example, UAS can facilitate casualty evacuation procedures or provide real-time information about the size of the affected area as well as the nature and extent of the damage; or they can assist first responders in bringing aid more rapidly and effectively to victims (e.g., by detecting bottlenecks and traffic jams in surrounding areas). UAS equipped with thermal cameras can also be used for day or night search and rescue operations by conducting searches for heat signals.
- Supporting community recovery efforts, for example by employing UAS as modes of delivery for food or the safe transfer

of medical materials that cannot not be easily supplied by traditional means of transport.

- Intelligence gathering, for example in relation to identifying or tallying the number of individuals at a scheduled event, as well as the suspected movements of people around and/or linked to vulnerable targets. When cross-checked with other available pieces of intelligence, for instance, imagery acquired by UAS may provide further confirmation of preparatory activity aimed at disrupting a scheduled event where large crowds are expected to gather.
- Detecting CBRN materials that terrorist groups may be trying to use against vulnerable targets. Various leaps in technology have been made allowing UAS devices to be equipped with sensors that can be set to detect certain harmful chemicals, biological agents or nuclear radiation.

The development and use of UAS for the above-mentioned applications come with some important caveats:

- When UAS are utilized to protect vulnerable locations as well as other sites – particularly in a surveillance mode – it is critical that they are employed within a framework of legality, necessity and proportionality to limit undue impacts on basic human rights, particularly the right to privacy.
- Attention should be paid not to allow gender, racial, religious and other biases to inform drone surveillance operations, in order not to further victimize and stigmatize vulnerable communities.
- The need to exercise restraint and observe all applicable procedural safeguards – in line with international standards and requirements – appears to be particularly pressing when UAS are equipped with facial recognition technologies.[43]

43 Effectively using facial recognition systems installed on UAS is still subject to a series of technical challenges, such as achieving the right angle to properly capture a face and being able to obtain good-quality visuals whilst moving or hovering. Both are considerably harder than getting a match from static footage. Despite the difficulties, however, UAS with advanced facial recognition capabilities are being developed by some technology companies specializing in surveillance services. While patent applications are being filed, law enforcement authorities in some countries are also considering the possibility of integrating such capabilities into their unmanned devices.

Case study 9.
Leveraging UAS to prevent terrorist attacks – Costa Rica

As it hosts a number of international events which bring a large influx of visitors, Costa Rica faces potential terrorist threats to its vulnerable targets. Part of the country's preventive action leverages UAS technologies:

- UAS are included in venue protection activities, especially for the purpose of spotting vulnerabilities that would not be visible from the ground.
- During major events, UAS footage is live-streamed to the command post to provide situational awareness not only of the venue but also of the surrounding areas.
- UAS are also used to patrol the country's borders, especially unauthorized entry points ahead of major events.
- Critical infrastructure, such as Costa Rica's pipelines, is also monitored by UAS technologies.
- Another common practice is fluent inter-agency communication, including with the National Civil Aviation Directorate, for the purpose of exchanging information and keeping each individual agency updated.

Source: Presentation by Ms. Mercedes Quesada, Head of UAS Operations, Intelligence Service, Costa Rica, at the UNOCT-organized Expert Group Meeting (6–7 October 2021).

3.1.2 Law enforcement

The law enforcement community plays multiple pivotal roles in deterring and investigating UAS-related terrorist conduct. By acting in an advisory capacity to support site operators and to the extent that they are authorized to employ counter-UAS technologies, law enforcement agencies are indispensable actors in the physical protection of vulnerable sites.

The following sections provide a snapshot of where – throughout the security cycle – law enforcement agencies can specifically intervene to mitigate risks, contribute to damage reduction in the event of crises and pursue alleged perpetrators, including by seeking to disrupt underlying criminal networks.

Box 7.
Upholding human rights and fundamental freedoms in UAS-based law enforcement operations

As UAS-related technology proliferates at remarkable speed, its use in the law enforcement and counter-terrorism context raises significant concerns from a human rights perspective.[44] Consequently, States should closely scrutinize the justification and necessity of UAS operations, whether at the stages of planning, execution, or subsequent investigation. At the same time, even as they collaborate with other States on law enforcement objectives, public authorities need to ensure that transfer and proliferation of drone technology is consistent with human rights protection. In particular:

1. The use of UAS domestically in law enforcement contexts, including the protection of vulnerable targets, must fully comply with States' obligations under international human rights law, including:
   (a) The right to life, to the extent that armed drone technologies are used, or UAS are used, to support broader law enforcement strategies underpinned by the use of force;[45]
   (b) The right to privacy, insofar as drone technologies are used for surveillance;
   (c) The freedoms of expression and association, which are indirectly affected by the kind of widespread and remote surveillance that drone technology enables.

(continued)

44 In 2020, the Special Rapporteur on extrajudicial, summary or arbitrary executions reported that at least 102 countries have acquired an active drone inventory, and around 40 possess, or are in the process of procuring, armed UAS.

45 The right to life is implicated both where UAS are armed and where unarmed UAS are used to support use of force on the ground by law enforcement agencies. Surveillance UAS are readily and cheaply armed, and drone manufacturers are reportedly actively marketing models armed with tasers, tear gas, and pepper spray to law enforcement agencies in the United States, South Africa, France and India.

2. The obligations to safeguard human rights entail practical implications at the stages of planning UAS operations and investigating any alleged violations after the fact:

   (a) Planning UAS operations: States must ensure that a certain action is necessary and proportionate to the intended objectives. Rigorous analysis has to be carried out prior to arriving at any decision about the use of UAS which may have targeting capacity. General plans and general orders to target identified significant individuals will not suffice without a direct link between the targets and imminent threats to others;

   (b) Investigating alleged violations of the right to life: The investigation must be prompt, effective and thorough. Persons who become aware of a potential violation of the right to life are required to report to their superiors quickly. Moreover, investigations and the persons conducting them must be, and must be seen to be, independent of undue influence.

3. States need to be mindful of the serious human rights concerns that attach to the onward transfer of drone technology to States which do not possess the requisite respect for human rights. In keeping with international law, States must ensure that they do not, whether intentionally or through failures of due diligence, facilitate the unlawful use by other States of armed drone technology.[46] Further, once sophisticated drone technology is shared widely worldwide, States face considerable challenges in seeking to control its spread to non-State actors.

Source: Remarks by Ms. Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, at the UNOCT-organized Expert Group Meeting (6–7 October 2021).

46 These concerns are particularly acute given that States routinely justify armed drone strikes on the basis of domestically defined counter-terrorism objectives, while, as consistently highlighted by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, States frequently use the fight against terrorism as cover for unlawful activities serving partisan domestic agendas.

3.1.2.1 Supporting operators of vulnerable targets

As the nature of UAS-related threats is still relatively unknown and/or underestimated, law enforcement agencies have an important role to play in helping operators of vulnerable targets appreciate and understand the specific threat scenarios affecting their premises and facilities. Within the risk management cycle, in particular, the scope of this support may include the following:

- Assistance in developing security plans, starting with the identification of threats and vulnerabilities;
- Guidance for site personnel on implementing plans, including training;
- Provision of expert advice on possible mitigation measures and available funding opportunities to help in performing security upgrades.

With regard to crisis preparedness, local law enforcement agencies should work in close partnership with site operators on the preparation of contingency plans in the event that weaponized UAS managed to circumvent the security measures in place. A main priority should be ensuring that the public and site personnel are evacuated from the threatened area as quickly as possible. To maximize the chances of an efficient evacuation, if necessary, the holding of regular exercises or drills on specific crisis scenarios can be encouraged and conducted under the supervision of law enforcement and site personnel in charge of security.

Moreover, in order to prepare for the unfolding of a crisis caused by drone use, it is recommended to develop a risk matrix for incorporation into security plans. Equipping crisis response workers, including law enforcement and security personnel, with adequate understanding prior to a crisis provides increased situational awareness.

Box 8.

Feeding UAS-collected information into the work of fusion centres

Fusion centres' ultimate goal is to allow enhanced information-sharing and inter-agency cooperation as they bring information together from multiple law enforcement and intelligence sources at the local, national and even international levels. In this context, UAS could be yet another source of valuable counter-terrorism-related information for fusion centres to collect and process. The intelligence, surveillance and reconnaissance (ISR) capabilities of UAS, in particular, could be especially beneficial to fusion centres when gathering general intelligence and, more specifically, border-related information, as well as information instrumental to the protection of vulnerable sites and critical infrastructure.

For example, a primary responsibility of Belgium's fusion centre – the Coordination Unit for Threat Analysis – is setting the national threat level and the production of coordinated threat analyses for national and European Union critical infrastructure. Information obtained via UAS could usefully contribute to the threat analysis exercise and prove beneficial in establishing a national threat level.

A potential challenge arising out of the use of UAS working in conjunction with fusion centres is the possibility of hacking. As UAS units would be part of the network that relays information to a fusion centre, they could become breach points, giving hackers access to stored information. The risk could be significantly mitigated through consistent analysis and hardening of potential security flaws within the software in use.

Source: Commercial Unmanned Aircraft Systems in Counter-Terrorism Contexts, UNOCT-organized Side Event at the Virtual Counter-Terrorism Week, 29 June 2021 (UN WebTV, https://media.un.org/en/asset/k1g/k1gt7x766e).

3.1.2.2 Protecting vulnerable targets using counter-UAS (C-UAS) technologies

At a basic level, C-UAS technologies can be divided into detection and disabling/interdiction technologies depending on their purpose.[47]

- *UAS detection technologies:* Compared to visual sightings, these technologies provide a significantly more precise and reliable means to identify the presence of a threatening UAS within a certain range. They can be based on radio frequency (RF) analysis, acoustic sensors, optical sensors or radar. Each of these technologies have advantages and disadvantages, and it is the responsibility of authorized law enforcement/security personnel to fully assess them based on factors such as cost, ease of deployment and the context in which they are supposed to operate (e.g., levels of radio frequency congestion and noise, light and atmospheric conditions).[48] A potential way in which C-UAS detection technologies may be circumvented is by using material such as aluminium to cover a UAS's GPS. This highlights the need for operators of vulnerable targets to keep relying on multiple levels of security – including human and visual observation – even when highly performing C-UAS technologies are being employed.
- *UAS disabling/interdiction technologies:* Once the presence of a threatening UAS has been detected, authorized security and/or law enforcement personnel need to take quick decisions about the most appropriate measures to be deployed with a view to preventing the threatening

47 Resolution 2370 Technical Guidelines also contain an overview of different detection and disabling/interdiction technologies, including considerations for law enforcement agencies when employing the different technologies at their disposal. See submodule II, Counter-UAS systems and techniques (3.1).

48 When detecting the signals by which UAS are controlled, for example, the performance of radio frequency-based devices decreases exponentially in densely populated areas, where the spectrum becomes noisier and more congested. The acoustic sensors (microphones) offer limited detection capabilities in noisy environments, while optical detection technologies may be hampered by low light conditions. Radar systems are the primary means for detecting long-range objects. They are also capable of spotting low-flying and small UAS, but they often have problems distinguishing between a bird and a small drone (Association of the United States Army, 2021).

device from causing any harm to people and/or property. UAS disabling/interdiction technologies fall within two broad categories: kinetic and non-kinetic. The former are designed to remove or reduce the threat posed by the flying object; they typically involve the use of net guns, projectile devices or laser weapons. By contrast, non-kinetic techniques are used to interfere with the UAS signal (e.g., high-power microwave); they often rely on the emission of radio frequency signals to prevent the UAS from being controlled properly.

Many C-UAS technologies are typically not available to operators of vulnerable sites, particularly those aimed at disrupting UAS operations. The use of disabling/interdiction technologies is thus often the prerogative of law enforcement agencies and other authorized governmental or security personnel. Authorized officials need to be familiar with the pros and cons of available solutions and ensure that their deployment is consistent with applicable legal frameworks, as well as the particular settings in which they would need to be used. Close interaction with operators of vulnerable targets is needed to understand sites' physical and technical features as well as those of surrounding areas.[49] Furthermore, it is recommended that C-UAS technologies be routinely assessed to determine whether their inclusion in the safety protocols assists in security development as opposed to creating a demand that cannot be maintained. For a major event, the deployment of C-UAS technologies will also hinge on a good understanding of the dynamics of the event itself, in terms of its various phases, expected crowd movements, arrival and departure of dignitaries, etc.

Box 9.
UAS and point of origin raids

Once a UAS has been detected and neutralized, various technologies can be utilized to trace the UAS signals back to the point of origin and to the point from which it was being remotely piloted. This C-UAS measure potentially allows law enforcement authorities to not only disable a hostile UAS but also apprehend those responsible for operating it, providing critical information about terrorist operatives and command and control bases.

UAS could also be coordinated in tandem with fusion centres to make point of origin raids more efficient. Information obtained or collected by Member States on terrorists in point of origin raids could then be analysed and processed at a national fusion centre (see box 8) for timely and accurate distribution to the relevant law enforcement bodies or intelligence agencies.

Source: Commercial Unmanned Aircraft Systems in Counter-Terrorism Contexts, UNOCT-organized Side Event at the UN Virtual Counter-Terrorism Week, 29 June 2021 (UN WebTV, https://media.un.org/en/asset/k1g/k1gt7x766e).

49 For example, some technologies may be more suitable for deployment in a rural environment, whereas others will be better placed for use in an urban context.

Case study 10.
Testing and assessing drone countermeasures – INTERPOL and the Norwegian Police

From 28 to 30 September 2021, INTERPOL and the Norwegian Police carried out a three-day exercise that brought together law enforcement, academia and industry experts from Europe, Israel and the United States. The purpose was to test and assess 17 drone countermeasures to ensure the safety of an airport environment through the detection, tracking and identification of UAS and their pilots.[50]

Each countermeasure was assessed and graded against specified criteria. This will allow for the results to be consolidated in an INTERPOL Drone Countermeasure Framework, which is expected to constitute a global focal point for collaboration and knowledge-sharing for law enforcement agencies across INTERPOL's 194 member countries.

The exercise was held at the Oslo Gardermoen Airport while it was in active operation. To be used within the airport, each system had to be licensed and approved by the regulator as well as cleared by the airport operator. The complexity of the exercise required close collaboration with the airport owner, the Norwegian Communications Authority, the Civil Aviation Authority and UAS Norway to ensure that all systems and tests were held to a required standard and did not affect airport operations.

(continued)

50 The tested drone countermeasures were divided into 4 groups – passive, active, multisystem and effector systems – and were evaluated for detecting, tracking and locating a drone as it entered restricted airspace. During the exercise, there were over 2,000 active aircraft movements.

In addition to the exercises, workshops and presentations to address drone incursions with a view to evidence retention were also held. These sessions saw participants share best practices and discuss possible future solutions for drone incursions.

Sources: www.interpol.int/News-and-Events/News/2021/INTERPOL-carries-out-full-scale-drone-countermeasure-exercise; Intervention by Mr. Christopher Church, Senior Mobile Forensics Specialist, INTERPOL, at the UNOCT-organized Expert Group Meeting (6–7 October 2021).

Case study 11.
Police making use of UAS – Catalonia, Spain

The Mobile World Congress, held in Barcelona in 2018, represented the first opportunity for the autonomous police service ("Mossos d'Esquadra") of Catalonia, Spain, to deploy a UAS surveillance system ensuring event safety and security. The deployment was possible under the new Spanish Drone Law (Royal Decree 1036/2017), which allows security forces to use unmanned devices in a variety of operations, especially in controlled airspace, over people and buildings, and at night. Unmanned aircraft deployed by the regional police force take pictures and videos live over the areas under surveillance.

Regional police officers in Barcelona have also coordinated with the Spanish airports company (AENA – Aeropuertos Españoles y Aeronavegación Aérea) and with ENAIRE (air traffic services provider in Spain) to carry out operations close to Barcelona Airport–El Prat, within an operating area with a defined height of 50 metres and in close coordination with helicopter services, while being permanently in contact with Barcelona Airport Control Tower.

Source: www.unmannedairspace.info/uncategorized/barcelona-security-forces-pioneer-urban-drone-services-spain/.

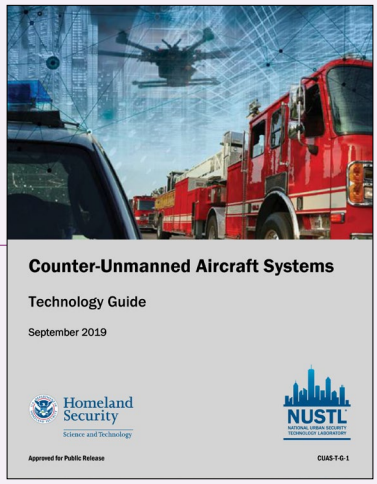
Tool 7.
Good Practices and Safeguards for the Deployment of C-UAS – Department for Transport, United Kingdom, 2018
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729458/taking-flight-the-future-of-drones-in-the-uk.pdf)

A consultation document developed by the United Kingdom Department of Transport in 2018 recognizes the need to put in place a series of safeguards to ensure the appropriate use of UAS technology, both for detection and disabling/interdiction purposes:[51]

- Drone technology is limited to use by trained and/or licensed operators;
- There is a clear purpose and scope for use of the technology, and operational policy specific to each side which is in line with appropriate legislation, e.g., a defined code of practice;
- Where applicable, a full risk assessment is conducted in line with health and safety legislation;
- A memorandum of understanding with the relevant regulatory bodies could be put in place where appropriate, covering dispute resolution mechanisms and resolving difficulties arising from malfunctioning or misuse of the technology;
- Any data captured from drone detection technology is managed in accordance with the appropriate legislation, e.g., data protection regulations.
- The technology is only deployed in line with an operational requirement where its use is deemed necessary and proportionate, in line with appropriate legislation, including human rights legislation, for example article 8 of the European Convention on Human Rights;
- The technology has undergone fit-for-purpose testing to minimize incidental interference;
- Regulatory bodies with responsibility for oversight of the technology deployed are informed when the drone technology is installed and where possible, prior to its installation;
- Depending on the nature of the side or event, organizations warn the public (through use of public communications, community engagement and signage) that unauthorized drone use will be monitored and enforcement action may be taken;
- There is appropriate insurance in place.

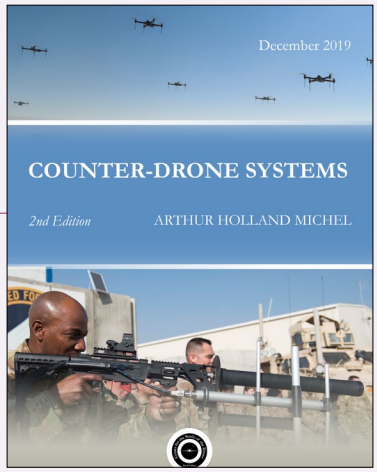
51 See *Taking Flight: The Future of Drones in the UK*, paras. 7.21 and 7.38.

Tool 8.
Counter-Unmanned Aircraft Systems: Technology Guide – United States Department of Homeland Security, 2019
(www.dhs.gov/publication/st-c-uas-technology-guide)



The Technology Guide is intended to educate the first responder community on C-UAS technology. It provides an overview of small unmanned aircraft system technologies, including key components enabling their operation. The information provided in this guide includes technical, scientific and engineering expertise offered by the National Urban Security Technology Laboratory as well as information gathered from Internet research, industry publications and manufacturers' data.

Tool 9.
Counter-Drone Systems – Center for the Study of the Drone, Bard College, 2019
(https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf)



This report provides background information on the growing demand for C-UAS technology and how it works, presents a database of known C-UAS products from around the globe and explains some of the challenges surrounding this technology. The analysis is based on open-source research of technical and policy reports, written testimony, news and analysis pieces, and manufacturer information; background interviews with government and law enforcement officials, industry representatives, and subject matter experts; and participation in both public and closed conferences and workshops.

3.1.2.3 Investigating UAS-related incidents

While investigators of UAS-related attacks need to comply with generally applicable procedures established in domestic criminal legislation (e.g., for the use of investigative techniques, arrest and arrest warrants, the application of evidentiary thresholds, etc.), they are often confronted with scenarios and challenges that are not necessarily present in ordinary criminal or counter-terrorism investigations. It is important for law enforcement agencies to appreciate the peculiarities of drone-related attacks and mobilize an appropriate set of investigative skills, particularly

when managing the crime scene and investigating the underlying criminal or terrorist networks:

- *Managing the crime scene:* Investigations into drone-related incidents need to be carried out as early as possible when the crime scene is still likely to have not been compromised. Once they are recovered from the ground and made inoffensive, UAS may become valuable sources of evidence in support of criminal proceedings. While digital forensic experts have a critical role to play in extracting data such as speed, height, GPS coordinates and flight records from seized UAS, other experts may look for more traditional physical data left on the UAS components – including abandoned control devices – such as fingerprints and samples of biological material. Equally, perpetrators may have left valuable evidentiary items at the sites from which they have waged the attack, particularly when they were in a hurry to leave their workstation.[52]

Box 10.
The potential danger of grounded UAS – Northern Iraq

Law enforcement and/or other authorized officers need to handle grounded UAS with extreme care as UAS can be potentially used for offensive purposes even when they appear to be innocuous on land. This was the case in northern Iraq, when Kurdish militias gunned down a small drone the size of a model airplane, mistaking it for one of the many UAS that Da'esh used in the area for reconnaissance purposes. Believing that the device would provide information about drone-based terrorist activity, it was subjected to further scrutiny. What the examiners did not expect, when they disassembled the drone, was a detonation triggered by a small improvised explosive device hidden inside the device.

Source: Staniforth, 2017.

52 See Resolution 2370 Technical Guidelines, submodule II, in particular, UAS incident scene: safety and security (3.2); Recovery and preservation of evidence (3.3); Technical exploitation of recovered UAS and components (3.4); and Information management (3.5).

- *Investigating underlying networks:* In most UAS incidents, "an attacker will have had assistance from others, in the form of a broader terrorist network or group, who helped with the procurement of UAS technology, the selection of targets, the perpetration of the attacks, or in the aftermath of an attack. Identifying such networks is critical to preventing further attacks by the same or affiliated groups, whether by UAS or other weapons" (Good practice 20, GCTF, 2019). In the process of unveiling the breadth and ramifications of the criminal operation that resulted in a UAS attack – and unless the perpetrators used bespoke UAS – important investigative leads may be obtained from operators' licensing and UAS registration records as well as export control documents.[53]

  To the extent allowed by available resources, investigations should look into the underlying network of aiders and abettors as well as those involved in the preparatory stage of the attack. An in-depth inquiry may highlight the presence of transnational elements and connections, requiring a willingness and ability of investigators to obtain information and evidentiary items from foreign counterparts, including via mutual legal assistance channels.

Box 11.
The IBACS conspiracy – several countries

Investigations carried out in at least four countries (Bangladesh, Denmark, Spain and the United Kingdom) revealed the complex mechanisms underpinning Da'esh UAS programme as well as its extensive transnational nature. As part of this scheme, in 2015, several IT, electronics and web services businesses (IBACS IT Solutions) were set up in the United Kingdom, Bangladesh and Spain as front companies to purchase and move UAS-related equipment to Da'esh. The purchases were made from at least nine different companies located in the United States and Canada. To make their activities appear legitimate, the conspirators employed cover names and relied on encrypted messaging applications to avoid detection from law enforcement agencies.

Source: Rassler, 2018.

Case study 12.
The power to stop and search for UAS

In 2018, the United Kingdom Home Office released a public consultation document entitled "Stop and Search: Extending police powers to cover offences relating to unmanned aircraft (UAS), laser pointers and corrosive substances". The document contains the

53 See Resolution 2370 Technical Guidelines, submodule II, in particular Identification of perpetrators (3.6).

following hypothetical scenario to illustrate a typical case where law enforcement authorities' lack of specific powers of stop and search may result in increased site vulnerabilities to UAS-related attacks:

"The police received calls on multiple occasions from the public saying that they had seen an individual flying a drone in a congested area, an offence under the Aviation Navigation Order 2016. The police have a description of the individual and the location. Officers patrolled the area during a time that most calls reporting the incident have been made, and they identify an individual matching the description. However, the individual is not flying a drone but has a large bag in their possession. The officers approach the individual and ask him what he is doing in that location. During the interaction, his manner is evasive and he appears to be nervously holding shut the bag. Due to the location, the time and the description of the individual, together with the individual's behaviour, the officers determined that they had reasonable grounds to suspect the individual is in possession of a drone which he has used to commit the offence of flying a drone in a congested area under the Aviation Navigation Order 2016. Having had the grounds and object of the search fully and clearly explained to the individual, the officers conducted the search, resulting in the seizure of a drone and associated items."

Source: United Kingdom Home Office, 2018.

Tool 10.
Framework for Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners – INTERPOL, 2020
(www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf)

This manual provides technical guidance in managing and processing a drone-related incident. It is addressed to two core audiences: first responders and police officers who attend incidents; and the digital forensics practitioners who process post-incident electronic evidence. Prosecutors, judges and lawyers may also benefit from it.

The advice featured in the manual is intended to be used as a reference for both strategic and tactical levels and is complemented by extracts from the Crime Scene Investigation Guide published by the United States National Forensic Science Technology Center.[54] It includes sections on drone components; drone payloads; drone data; how and where to find evidence sources (phone, remote, SD card, internal storage); safety procedures; precautions before approaching a drone; safety precautions when handling a drone; first aid and emergency procedures; drone seizure process; digital forensic investigation; fingerprint preservation; and the collection and preservation of digital evidence.

3.1.2.4 Customs and border enforcement

From a customs and border enforcement perspective, UAS appear relevant in at least three domains related to the prevention of terrorism:[55]

- The detection and seizure of UAS and related components smuggled to be used for terrorist purposes;
- The detection and seizure of UAS as a means of transport for arms, goods, equipment, cash, etc., to be used in the preparation of terrorist acts;
- The use of UAS as enforcement tools by border agencies to monitor cross-border activity, including unauthorized individuals crossing borders in remote and porous stretches between established ports of entry.[56]

Handling dual-use items (e.g., physical components, technologies' software) is a distinctive challenge for customs authorities.[57] The difficulties appear substantially similar to those created by trade in substances that may also be employed for manufacturing

54 See https://nij.ojp.gov/topics/articles/crime-scene-investigation-guides-law-enforcement.

55 See Resolution 2370 Technical Guidelines, submodule II, Customs and border controls (2.3.1).

56 UAS can be used to provide key visual information, helping to monitor porous borders against potential terrorist threats by detecting anomalies occurring over vast distances. Also, when they are equipped with infrared or thermal sensors, UAS can assist patrolling teams in securing border areas at night.

57 The Missile Technology Control Regime (MTCR) and the Wassenaar Arrangement are the two multilateral regimes laying the normative framework for UAS export controls. The MTCR, in particular, is a 35-member export licensing initiative aimed at preventing the proliferation of unmanned systems capable of delivering weapons of mass destruction. The Wassenaar Arrangement engages its 42 participating countries to prevent, among others, terrorist acquisition of dual-use items by applying export controls to all items included in the Dual-Use Goods and Technologies List and the Munitions List, the objective being to prevent unauthorized transfers or re-transfers of those items.

improvised explosive devices, such as ammonium nitrate. In this domain too, any achievement hinges on the ability of border and customs agencies to share and process accurate advance information about incoming items and develop red flags.[58]

3.1.3 Intelligence agencies

Countries' ability to understand the dynamics and mechanisms of illegal UAS supply networks, pinpoint the actors involved and identify the paths – both online and offline – followed by people and goods is a fundamental step in the overall risk mitigation effort. At the same time, the mobilization of resources needed to disrupt the supply and procurement chains for terrorist-driven UAS activity hinges upon countries' ability to collect and process significant amounts of high-quality intelligence. This intelligence can be gathered from a variety of sources and should be processed by cross-checking all available data.

With the appropriate regulatory frameworks in place, for example, UAS vendors may be required to conduct due diligence on potential customers and report suspicious transactions to the competent authorities (see section 3.2.3). This could provide valuable information, potentially opening up new investigative paths, confirming the validity of existing ones and/or providing fresh details about ongoing operations and the identities of the people involved.

Critical information may also be obtained on the ground by collecting and analysing photographic and documentary evidence, including from conflict zones. In some cases, governments have relied on the services of private-sector organizations whose task is to document – through the work of field-based investigative teams – the presence of illicit weapons, ammunition and related materiel in conflict-affected locations, and trace their supply sources. For example, recent research

58 Resolution 2370 Technical Guidelines look into types of UAS subsystems that States may consider regulating. See submodule II, Control of UAS and key subsystems (2.3.2).

into the acquisition, development and use of weaponized UAS by Da'esh in Iraq and the Syrian Arab Republic shed light on its extensive network of suppliers for software and hardware components used to assemble UAS. This research also illustrated how terrorist groups tap into international, markets, particularly online, for the supply of UAS and UAS-related components, which explains intelligence agencies' increasing attention on monitoring Internet-based transactions (see box 12).

Box 12.
Da'esh's UAS procurement network

Investigative work conducted by Conflict Armament Research (CAR)[59] on recovered commercial UAS used by Da'esh in Iraq sheds light on how nine of them were procured. The investigation started by connecting the UAS' serial numbers to some of the vendors from which they were purchased.

According to in-depth analysis conducted by the Combating Terrorism Centre at West Point on Da'esh's UAS programme, "one of the fundamental takeaways from [the CAR investigation] was the complexity regarding how Islamic State drones were sourced, as seven of the nine commercial drones were purchased from different distributors or websites located in/operated out of [five States]. … Another interesting takeaway was the layered nature of how the nine Islamic State drones were being acquired, as in a number of the cases studied, the commercially available drone was purchased in one country, activated in a second country, and then finally used in a third country – Iraq or Syria."

Source: Rassler, 2018.

59 CAR is a United Kingdom-based investigative organization that tracks the supply of conventional weapons, ammunition and related military materiel into conflict-affected areas.

3.2 Non-government actors

By partnering with institutional actors, UAS software developers, manufacturers of hard parts and C-UAS technologies can all contribute, from their respective market segments, to making the access and use of UAS for terrorist purposes more difficult. On the other hand, UAS users, operators of vulnerable sites, the public and civil society organizations are in a position to take significant mitigation action as a result of targeted sensitization campaigns, the right mix of incentives and the creation of adequate channels of communication with law enforcement and other governmental authorities.

3.2.1 Operators of vulnerable targets

The owners and managers of vulnerable sites can take a series of important actions to protect their locations from the risk of terrorist-driven UAS activity:

- *Include UAS-related threats and vulnerability assessments in site security plans:* It is paramount for operators of vulnerable targets to ensure that specific UAS threat and vulnerability assessments are integrated into their general terrorist risk management cycle. Valuable insight for the elaboration of security plans can be obtained by observing how UAS have previously affected similar sites, in the same or other countries. Past incidents may provide key threat- and vulnerability-related information, enabling site operators to fine-tune the selection of the most appropriate mitigation measures.[60]
- *Determine the nature and level of the threat to the site:* While all open-air sites are likely to require the implementation of solid counter-drone measures, sites that only have some open access points (e.g., the windows of a museum) may only need to consider the extent to which UAS can be remote piloted and penetrate narrow passages.
- *Follow developments in the drone market:* The knowledge that site operators can acquire about UAS technological advances will help them to better gauge the nature and extent of the risk. Staying up to date about new features and capabilities of recreational or commercial UAS as they enter the market may be important elements for consideration.
- *Select the most appropriate detection and mitigation options:* In determining the most appropriate risk-mitigation measures, there is no standard, one-size-fits-all solution. As hundreds of different solutions are currently available on the market, it is often difficult for end users to determine which ones are the most appropriate. Choices will depend on the unique risks identified within a specific operating environment as well as financial considerations. In this context, launching sites in surrounding areas also need to be made part of the equation. Likely locations from which an operator could pilot drones should be identified, [61]monitored and taken into account in security plans.
- *Implement non-technology-based C-UAS options:* Under most regulatory frameworks,

60 UAS-related threats need to be seen as potentially dynamic, and not necessarily static. Plans for crisis management should be adjusted accordingly. For example, a drone may land at a vulnerable point of a certain site and, immediately afterwards, move to another vulnerable point of the same facility, or even pursue crowds while they are being evacuated. Also, threat assessments should not exclude the possibility that small UAS can be smuggled into a site and activated from within.

61 These may include roads with easy escape routes, elevated places offering a good view over the site to be protected, parking spaces, etc.

site operators do not have the authority to disable, disrupt, or seize control of UAS.[62] As a result, it is essential for them to understand the extent to which use of specific C-UAS technologies may be prohibited or otherwise limited.[63] At the same time, depending on the applicable legal framework, site operators may be in a position to autonomously implement an array of mitigation tactics that do not involve using C-UAS technologies. These include:

- *Concealing or disguising vulnerable assets:* Vulnerable assets may be fully or partly protected from aerial view by non-transparent screens, foliage, etc. Potential UAS launching sites in surrounding areas may be made less enticing by covering them from view, adding lightning and access control measures. These measures may require coordination, authorization and intervention from the owners and managers of the areas hosting the potential launching sites, such as municipalities.
- *Site surveillance:* Open-air areas such as courtyards and rooftops may be regularly checked for the presence of UAS or UAS-delivered items. This underscores the need to have active mitigation measures in place against drone interference not only at the time when crowds gather or an event takes place. UAS may drop dangerous devices or be engaged in surveillance at times when the targeted facility is not being used or open to the public.
- *Line of sight analysis/visual detection:* This method of detection involves human observation of the skyline for any potentially threatening UAS. When a UAS is spotted on or near a sensitive location, site operators have a key role in quickly alerting security/law enforcement personnel. Line of sight analysis should be used not only when technological detection tools are unavailable but also in conjunction with such tools in view of their fallibility.
- *Communication/warning tools:* Warnings and signals may be posted in surrounding areas and transport hubs with the aim of informing and reminding the public about prohibitions to fly UAS over certain vulnerable targets. While such measures may not discourage malicious actors, they are likely to reduce the number of UAS flown out of negligence. This, in turn, would enable law enforcement and security personnel to focus resources and attention more effectively on fewer problematic events. Public outreach efforts may also provide telephone numbers for reporting suspicious sightings and utilize operators' official websites as well as their social media accounts.[64]
- *Increase UAS detection and handling capabilities:* Site personnel can be informed about how to assess risks associated with the illegal use of UAS in relation to sites' operations as well as how to visually detect and report incidents.

62 While the use of technologies aimed at disabling or interdicting UAS may raise complex technical and legal challenges, a number of UAS detection tools (e.g., based on radar technology) may, be less problematic from this point of view and available to site operators, albeit often at a cost. UAS detection solutions may enable site operators to ascertain critical factors such as the speed, size, payload capacity and navigation modality of a threatening object. On this basis, inferences can be made about issues such as the level of risk of collateral damage to people or property, which will in turn influence the choice of the appropriate mitigation measure.

63 In the United States, for example, UAS are considered aircraft and are given similar protections to commercial or passenger aircraft. As a result, under United States federal law, it is generally illegal for private organizations or individuals to interfere with UAS in flight, such as by jamming their signals.

64 In order to post warning signs and notices at locations – including virtual locations – that are not under the control of or managed by site operators, the latter will need to reach out to other landowners, website managers, etc.

They should also be trained on how to approach suspicious UAS both in flight and on the ground. Depending on how site employees handle a crashed UAS, for example, the ensuing inquiry and forensic investigation may be jeopardized, the evidentiary chain of custody may be broken, etc. (see section 3.1.2.3). While waiting for law enforcement authorities to intervene, site personnel may be instructed to simply take records of the UAS incident via photograph or video.

- *Partner with law enforcement and other public authorities:* In preparing for incursions by hostile UAS, site operators may feel unfamiliar with the approaches and techniques needed to address what appears to be a new type of threat. As the learning curve may indeed be steep, it is crucial that they take maximum advantage of the expertise and advice available from local public authorities from the early stages of the security planning process with a view to understanding risks, challenges and mitigation options. Funds and grants may also be available from governmental authorities. While some funding opportunities may be earmarked to specifically enhance site protection against UAS-related threats, others may be generally aimed at upgrading security features against terrorism-related attacks including – albeit not limited to – attacks using UAS.

  Overall, operators of vulnerable targets are expected to significantly benefit from partnering with public authorities to determine the solutions against hostile drone activity that best fit local circumstances based on applicable legal frameworks and budgetary constraints.

Tool 11.
Aviation Security Global Risk Context Statement (RCS), Doc 10108 – ICAO

In recognition of the importance of a risk-based approach to aviation security, the first edition of the Risk Context Statement (RCS) was developed in 2012 by the ICAO Aviation Security (AVSEC) Panel Working Group on Threat and Risk (WGTR). The current edition of RCS offers a methodology and a framework to inform and support ICAO Member States' processes for national and local aviation security. It also provides an overview of the current global aviation security threats (including the ones posed by UAS) and presents high-level global risk assessments to help inform States' national civil aviation security programmes. Finally, it assists ICAO in improving and updating Annex 17 – Security Standards and Recommended Practices (SARPs) and guidance material.

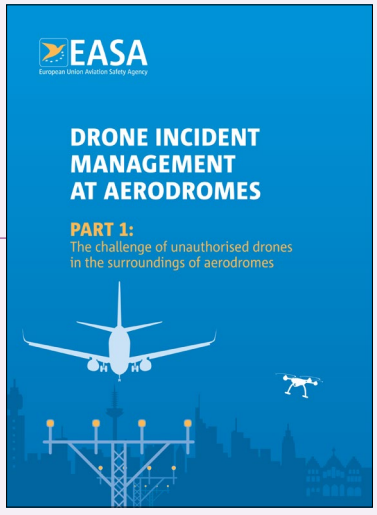
The WGTR updates the RCS on an annual basis and provides analysis and advice on risks to aviation to the Aviation Security Panel. The work of WGTR relies on experts' input as well as the effective and timely reporting and sharing of information by ICAO Member States.

(continued)

ICAO recommends that RCS should be made available to those who are responsible for conducting national and other aviation security risk assessments and aviation security decision makers, practitioners and other relevant stakeholders. Procedures for handling, transmission and storage of this document must be applied in accordance with each Member State's regulations for sensitive aviation security information.

Source: Presentation by Mr. Sylvain Lefoyer, Deputy Director, Aviation Security and Facilitation, ICAO, at the UNOCT-organized Expert Group Meeting (6–7 October 2021).

Tool 12.
Drone Incident Management at Aerodromes – European Union Aviation Safety Agency (EASA), 2021
(www.easa.europa.eu/drone-incident-management-aerodromes-part-1)



The EASA Manual provides guidance on how to develop arrangements and procedures which support quick, effective, and proportionate UAS incident responses. This includes, crucially, the setting up of a joint working group with law enforcement, air operators, air traffic control, etc., as a prerequisite to

achieve robust decision-making outcomes in emergencies. The document also aims to strike a balance between the opportunities represented by UAS and the necessary obligations on drone manufacturers and operators, in terms of safety, respect for privacy, the environment, protection against noise, and public security.

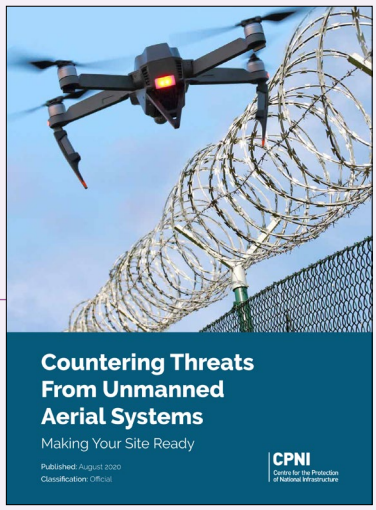
Addressed to all the stakeholders with responsibilities for aviation safety and security, the Manual is composed of three parts: Part one, The challenge of unauthorized drones in the surroundings of aerodromes; Part two, Guidance and recommendations; Part three, Resources and practical tools.

Only Part one of the Manual is publicly available through the EASA website. The full manual can be obtained upon request by aviation actors, law enforcement and national civil aviation authorities by contacting EASA.

Tool 13.
Protecting Against the Threat of Unmanned Aircraft Systems: An Interagency Security Committee Best Practice – United States Department of Homeland Security, 2020
(www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf)

The best practice document outlines awareness and mitigation measures for use by security professionals in charge of site protection against malicious and unmanned aircraft systems operations. The topics covered include an overview of UAS; threats posed by UAS; vulnerability assessments; protective measures and activities; how to develop a facility response plan for UAS incidents; how to increase workforce awareness; and how to engage with community partners.

Tool 14.
Countering Threats from Unmanned Aerial Systems: Making your Site Ready – Centre for the Protection of National Infrastructure, 2020
(www.cpni.gov.uk/system/files/documents/40/14/c-uas-branded-doc-public-V4.1.pdf)



This tool is an introduction to developing a site-specific counter-unmanned aerial system strategy and plan.

A range of countermeasures are discussed that a site can introduce to mitigate the risk of UAS threats, including how to reduce negligent and reckless UAS use; physical hardening; an introduction to technical options; and how to develop an effective operational response.

3.2.2 Manufacturers of UAS and key subsystems

The dynamics of a thriving market and sustained demand for commercial and recreational UAS are driving manufacturers of UAS and key subsystems to constantly upgrade their products by increasing their performance and making them more user-friendly. In responding to the market logic and trying to surpass their competitors, UAS manufacturers should leverage all available technological innovations to make their products less prone to exploitation by hostile actors. Currently, two main groups of mechanisms appear to be used for this purpose:

- *Installation of geofencing capabilities:* these provide a basic security feature to ensure that UAS cannot be operated over certain air spaces such as airports, penitentiary facilities, power stations, etc. Software that supports geofencing functionalities can be easily updated based on changes in local circumstances. For example, it can receive instructions not to fly over a certain space where a crowded event is in progress or is about to take place. Geofencing does not offer a "silver bullet". It is clearly vulnerable to hacking, and even the most effective and hardest-to-manipulate feature may well be circumvented by using a bespoke drone. Still, geofencing can represent an important first line of defence against malign activity undertaken by improvised actors, or those who do not possess enough time or any significant cyber capabilities.
- *Transmission of UAS identification information:* UAS manufacturers have been experimenting with technology for the continuous radio transmission of UAS identification information. Similar to a licence plate, an identification code released by UAS can assist security and law enforcement personnel at the receiving end in distinguishing between lawfully and unlawfully operating UAS. While the transmission of drone identification data would not offer any conclusive evidence about whether a specific flying object presents a danger or not, it may help to rank threats and thus supporting decision-making processes that often need to be completed within tight time frames.

Box 13.
UAS manufacturers and geofencing solutions

After creating its first no-fly zones feature for its UAS in 2013, a leading UAS manufacturer introduced its geofencing system three years later, adding real-time updates and new off-limits areas. The system relies on navigation satellite signals to automatically keep flying UAS away from sensitive locations such as airports, prisons, nuclear power plants and high-profile events. In some locations, a UAS cannot take off inside or fly in a geofenced area without special authorization. UAS pilots with verified DJI accounts can unlock certain areas if they have legitimate reasons and possess the necessary approvals, but more critical areas require additional steps to be unlocked. Under the approval process, professional UAS operators who are authorized to fly to sensitive locations can receive unlock codes within 30 minutes by submitting an online application.

Source: www.dji.com/newsroom/news/dji-refines-geofencing-to-enhance-airport-safety-clarify-restrictions.

A major issue associated with some security-related technological solutions is that they are manufacturer-specific. The risk lies in the creation of compartmentalized environments where different technologies only work for specific UAS models or brands. This clearly underscores the need for UAS manufacturers to roll out such solutions in close coordination not only with public authorities, but also – critically – other UAS manufacturers to ensure maximum reliance on common standards and protocols as well as human rights-compliant approaches.

In addition to deterring illegal UAS activity by integrating the most advanced technological solutions in their new devices, UAS manufacturers are instrumental in sharing technical information about future products with regulatory and government agencies.[65] By gaining advance notice of projects in the pipeline, government entities – and, in time, operators of vulnerable targets – will be in a better position to anticipate threats and prepare more accurate mitigation and contingency plans.

At the same time, any channel or mechanism for private-public information exchange in this area will have to reassure participants that adequate levels of confidentiality will be maintained. Effective flows of information will have to be conditioned on guarantees that intellectual property protections are upheld, and that sensitive commercial information will not be disclosed in ways that provide an unfair advantage to competitors.

Case study 13.
Commercial Unmanned Aircraft Association of Southern Africa (CUAASA)

Originally established to support its members to obtain a sound legal basis for their operations in anticipation of a new legal framework for UAS operations in Southern Africa, CUAASA aims to serve, promote, watch over, advance and mutually protect the interests of the commercial remotely piloted aircraft (RPAS) industry. Members include various high-tech manufacturing and sales companies, drone and legal service suppliers as well as a provider of drone pilot training courses. In addition to acting as a link between industry and relevant public bodies within the Southern African region, CUAASA has a mandate to assist its members to promote safety, raise the standard of operations and to prepare its members for the forthcoming legal framework.

When joining CUAASA, members agree to:

- Perform RPAS activities legally, ethically, professionally and, where applicable, within the relevant permissions governing the airspace in which the member is flying;
- Promote and further the development of the industry and CUAASA;
- Report incidents to the police, the Civil Aviation Authority (CAA) or relevant industry body in order to help the industry grow in the right direction.

CUAASA members need to accept and adhere to a code of conduct which provides a set of guidelines and recommendations for safe, non-intrusive RPAS operations. The code of conduct is around the principles of safety, professionalism and respect and commits to respect the rights of other users of the airspace, the privacy of individuals and the concerns of the public as they relate to unmanned aircraft operations. The code also seeks to provide manufacturers and users with a checklist for operations and a means to demonstrate their commitment towards safe and responsible industry growth.

Source: https://cuaasa.wixsite.com/cuaasa.

65 The Berlin Memorandum includes this measure, among others, that Governments are encouraged to take to "establish and enhance coordination with private industry and other non-traditional stakeholders" (Good practice 14, GCTF, 2019).

Case study 14.
Drone Industry Action Group (Drone IAG)
(www.arpas.uk/drone-iag/)

Drone IAG is a multi-stakeholder forum gathering drone industry stakeholders in the United Kingdom in an effort to engage with governmental agencies as well as academia, research and technology offices, regulators, investors and end users. It seeks to understand sector opportunities and challenges and identify actions needed to address and overcome them. Drone IAG members are expected to play an active role in implementing its overarching objectives:

- Foster innovation and collaboration that will support the growth of commercial drone applications and wider use of drone technologies and solutions in the United Kingdom;
- Facilitate the adoption of UAS in a wide range of uses across the United Kingdom public and private sector, as well as monitoring, reviewing and inputting to appropriate standards;
- Develop opportunities for adoption of UAS and facilitate coordination, collaboration and exploitation of technology and an air traffic management system in the United Kingdom that integrates UAS and wider general aviation;
- Enable an industry-led voice into Government and establishment of a framework that mitigates the misuse of UAS and addresses societal concerns;

(continued)

- Respect the rights of other users of the airspace;
- Respect the privacy of individuals;
- Respect the concerns of the public as they relate to unmanned aircraft operations.

Current Drone IAG working groups include:

- Operating Safety Cases – To develop possible improvements to the Civil Aviation Authority's current risk assessment procedure;
- DevSpace – To propose solutions to the challenges of testing novel or complex applications;
- Public and commercial perceptions – To handle issues around public attitudes and routes to increased awareness of drone services in relevant sectors.

Case study 15.
Detecting vulnerabilities: The Bug Bounty programme

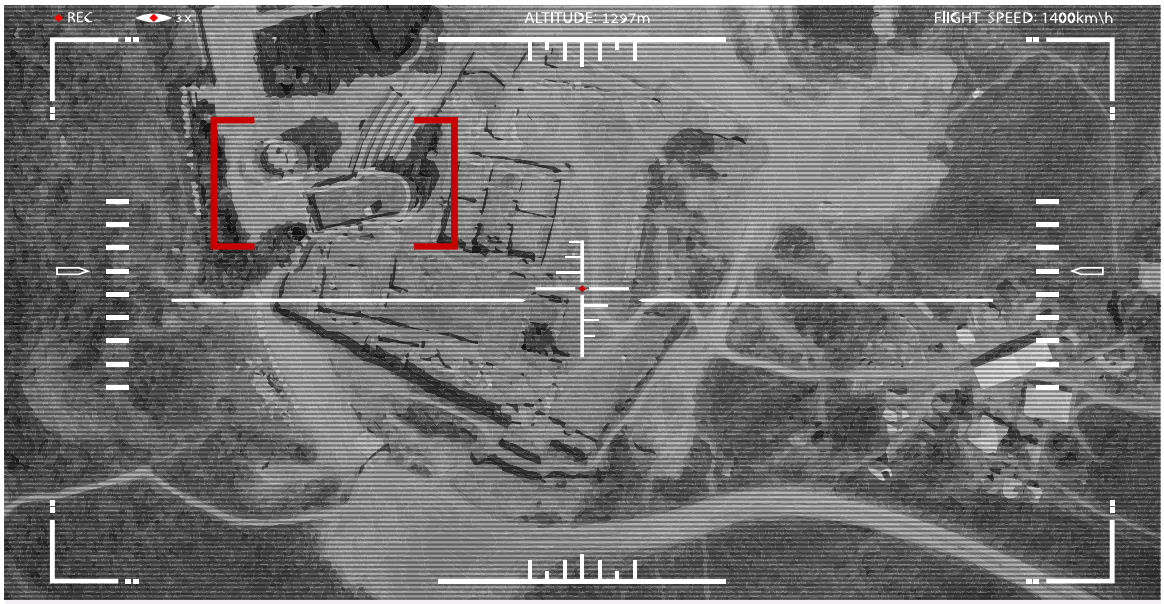
A leading drone manufacturer has implemented the Bug Bounty programme whereby external security researchers are encouraged to contribute to the strengthening of its data security by actively looking for and reporting system vulnerabilities. Eligibility to participate in the programme requires compliance with a number of requirements; for example, participants must not be the author of the vulnerability itself; they must not endanger flights or public airspace security in any way; they must not make use of or exploit the vulnerability for any reasons to further probe additional security issues. Eligible participants may be granted a monetary reward calculated on the basis of the estimated risk and impact of the reported vulnerability.

Source: https://security.dji.com/policy?lang=en_US.

3.2.3 UAS vendors and retailers

As the closest link to customers within the UAS ecosystem, vendors and retailers are often in a privileged position to shape users' perceptions, provide clear and user-friendly information about safety and security issues as well as applicable laws and regulations. Vendors' street shops and websites can provide and display governmental leaflets, banners and other officially-cleared security-related material, when available.

UAS vendors and retailers can significantly contribute to preventing UAS and related equipment from falling into the hands of hostile actors. The regulatory frameworks of some countries may already require that vendors and retailers undertake due diligence action in this regard, including by verifying the identities of prospective customers and keeping transaction records.



Box 14.
Red flags and lack of due diligence in the IBACS case

The IBACS case involved the purchase of several UAS devices by companies affiliated with Da'esh; it provides suggestions as to how the legitimate companies involved in these transactions could have potentially avoided the supply of UAS-related material to Da'esh by conducting basic "know-your-customer" verifications. Indeed, the transactions were surrounded by a set of unusual circumstances that should have raised immediate suspicions, including:

- The nature of the items being purchased (drone, remote control airplane, rocket components, counter-surveillance equipment);
- The place where those items had to be shipped (near the border of territory then controlled by Da'esh);
- The timing of the purchase (when Da'esh was making headlines in the global media).

Arguably, "this dynamic … raises some important questions about the internal review of purchases at this specific companies and/or the policies … retailers have in place to detect and prevent suspicious transactions, as well as the apparent lack of regulations that exist to police the distribution of these types of components, especially when the items are set to be delivered to locations immediately adjacent to active war zones." Also, "the network's list of purchases highlights another issue that likely should have raised red flags or facilitated greater scrutiny of the purchases being made: the quantity of items being purchased or the number of transactions made within a short period of time." At one point, for instance, "[one of the conspirators], sometimes using different names, made 11 repeat purchases of the same batch of goods on the same day from the same company – , all to be delivered to Sanliurfa, Turkey, – for a total, one-day sale of more than $16,000 in drone parts."

Source: Rassler, 2018.

Case study 16.

Dronesafe Certification Programme for retailers in the United Kingdom

A leading drone manufacturer has implemented the Bug Bounty programme whereby With the number of drone purchases rising year on year, this initiative sought to stimulate a safer use of UAS and increase people's awareness on when, where, and how they can use them safely. As part of the programme, which ran until 2021, users were encouraged to look out for the Dronesafe symbol to ensure they were making their purchases from a trustworthy and responsible supplier. To be awarded a Dronesafe certificate, retailers had to declare that they were:

- Providing customers with a copy of the Drone Code in the box of any drone weighing over 250 g;
- Alternatively, a copy of the Drone Code must be presented to customers at the point of sale;
- Prominently displaying the Drone Code instore;
- Providing clear advice to customers on following the Drone Code;
- Adding links to the dronesafe.uk site to online drone product pages.

Finally, each store needed a knowledgeable drone person on its staff who could answer customer queries and train fellow colleagues.

Retailers could apply to join the initiative by declaring to the Civil Aviation Authority (CAA) that they met the above criteria. On receipt of their application, the CAA would contact the retailers to confirm whether they could then display the Dronesafe logo.

3.2.4 Providers of Counter-UAS (C-UAS) technologies

Providers of C-UAS solutions design and develop technologies for authorized entities under national legal frameworks to detect, identify, track and disable or interdict illegal UAS operations. Such technologies have been actively used to protect vulnerable targets worldwide. During the 2018 FIFA World Cup in the Russia Federation, for example, authorities and security forces deployed C-UAS systems at the match venues to deter potential drone attacks. Another anti-UAS system was stationed to protect VIPs and infrastructure at the 2018 G20 Summit in Buenos Aires.[66]

It is essential for providers of C-UAS solutions to develop very close lines of communication with government and law enforcement agencies that will potentially employ those technologies. Collaborative efforts are critical to ensure that industry stakeholders stay abreast with rapidly evolving legal requirements and constantly develop and adapt their technologies to address new and emerging UAS-related threats and ensure that solutions are developed in a human rights-compliant manner.

3.2.5 UAS users

The number of end users of UAS-related products and services is expanding exponentially as new individuals, companies and organizations adopt UAS technology for a variety of recreational, commercial and other professional purposes.[67] In all cases, UAS operators have the overarching responsibility to handle their devices in full compliance with the safety and security standards and

66 The system featured a 3D X-band radar to detect potentially threatening objects, electro-optical/infrared camera to classify them and a jammer for disabling purposes.

67 This category of stakeholders includes entities that own fleets of UAS and conduct flight operations to execute projects on behalf of their clients, integrating a new business model known as "UAS as a service" (see box 15).

requirements in force; this includes registering them, obtaining the necessary licences and undergoing required testing.

For one thing, compliant UAS operators reduce the risk of endangering people and property and limit their own exposure to personal liability. For another, a responsible community of end users ensures fewer instances of negligent use of UAS in restricted airspace. This, in turns, enables law enforcement agencies and security personnel – including those involved in the protection of vulnerable sites – to direct limited resources and detection capabilities to a narrower range of potentially threatening UAS events.

Users can also significantly reduce the risk of their own devices being hijacked or otherwise diverted for hostile purposes. Key mitigation action often includes observing basic cybersecurity norms such as regularly updating UAS software, choosing strong passwords, ensuring that ground control devices, including smartphones and laptops, are less vulnerable to malware, and using a virtual private network (VPN) to prevent hackers from accessing Internet-based connections.[68] Also, UAS that feature a Return to Home (RTH) functionality allow users to recover them in the event of hijacking as the device will automatically return to the "home point" if the signal is lost or jammed[69] (Kaspersky, 2021).

Box 15.
"UAS as a service"

In recent years, some government agencies have begun to rely on private companies for the deployment of sophisticated UAS in surveillance and monitoring operations. The "UAS-as-a-service" concept represents a novel dimension of public-private partnerships in the UAS ecosystem. When it is underpinned by a legal framework that supports ethically and legally sound principles, it allows governments to focus on results rather than assets, to use the most appropriate assets on a case-by-case basis, and to employ flexible contractual frameworks in line with the operational flexibility made available by the service.[70]

The concept may be especially interesting for law enforcement agencies that are not sufficiently equipped with state-of-the-art UAS technologies or lack the technical expertise for handling them. Also, it may suit the needs of countries whose limited financial availabilities would not allow them to buy, employ and sustain the costs of managing their own UAS fleet.

68 A VPN acts as a secure gateway to the Internet, encrypting the connection.

69 As the RTH mode depends on GPS to operate, this feature may not, however, work in the event of "GPS spoofing", i.e., when the device's GPS tracker is tricked into thinking that the device is located somewhere else.

70 For example, the United Kingdom Home Office has employed the UAS-as-a-service model as a key asset to help prevent illegal migration and illegal fishing activities.

3.2.6 Users of vulnerable targets

Based on clear and simple guidance provided by law enforcement and/or security personnel, visitors to tourist and iconic sites, spectators at open-air events, and other users, can play important roles in managing UAS-related threats to vulnerable sites. For example, some of these sites may not be equipped with C-UAS technologies aimed at detecting threatening UAS. Others may deploy technology-based solutions that are insufficient or underperform in certain light or weather conditions. In all these cases, the general public's ability to spot and report troubling situations may be a crucial asset as part of a multilayered security environment.

3.2.7 Civil society organizations (CSOs)

CSOs can leverage their position by better connecting the public with the authorities responsible for drone safety and security matters. For example, they can act as intermediaries by ensuring that regulatory frameworks and public policies about drone-related threats and prevention issues are brought to the attention of the public. Additionally, independent grass-roots organizations can be instrumental in effectively expressing and channelling civil society's concerns and ideas to the policymaking, regulatory and law enforcement communities. Their contribution can be sought at various stages of the policy and lawmaking processes, including the assessment of tradeoffs and risks, the drafting process and in rules dissemination.

Beyond the communication aspect, they can be engaged in materially supporting recovery efforts and providing assistance to victims following a drone-based terrorist attack. Some NGOs actively use UAS as support tools in the event of a crisis, whether or not UAS were involved in the incident (see case study 17).

Case study 17.
Drones Without Borders
(www.droneswithoutborders.org/)

Founded in 2019, Drones Without Borders is an NGO whose mission is to leverage UAS technology to provide real-time technical monitoring and information to emergency and disaster responders and other partners on the ground in response to crises, whether natural or human-caused.

Conducting its mission under the three operational clusters of impact assessment, needs verification and humanitarian advocacy, Drones Without Borders is involved in crisis management and recovery efforts by focusing on vulnerable persons affected by situations of emergency.

References

Association of the United States Army, 2021. The Role of Drones in Future Terrorist Attacks (www.ausa.org/publications/role-drones-future-terrorist-attacks#).

Canada, Department of Transport (Transport Canada), 2021. Transport Canada's Drone Strategy to 2025 (https://tc.canada.ca/en/aviation/publications/transport-canada-s-drone-strategy-2025).

Europol, 2021. European Union Terrorism Situation and Trend Report (www.europol.europa.eu/tesat-report).

Global Counterterrorism Forum (GCTF), 2019. Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems (www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fI%3D&portalid=1).

Kaspersky, 2021. Security and drones: what you need to know (www.kaspersky.com/resource-center/threats/can-drones-be-hacked).

Ley Best, Katharina and others, 2020. *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools*, Rand Corporation (www.rand.org/pubs/research_reports/RR2972.html).

Moore, Jack, 2016. Rio Olympics: Al-Qaeda Jihadis Call for Attacks on American, British, French and Israeli Athletes, *Newsweek*, 22 July 2016 (www.newsweek.com/al-qaeda-jihadis-call-attacks-american-british-french-israeli-athletes-rio-483145).

Palestini, Claudio, 2020. Countering drones: looking for the silver bullet, *NATO Review* (www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html).

Rassler, Don, 2016. Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology, Combating Terrorism Center at West Point (www.jstor.org/stable/resrep05632).

_____, 2018. Islamic State and Drones: Supply, Scale and Future Threats, Combating Terrorism Centre at West Point (https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf).

Staniforth, Andrew, 2017. Attack of the drones: Emerging threats from Unmanned Aerial Vehicles, TRENDS Research & Advisory (https://trendsresearch.org/insight/attack-of-the-drones-emerging-threats-from-unmanned-aerial-vehicles/).

United Kingdom Home Office, 2018. Stop and Search: Extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers and corrosive substances: Government consultation (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739629/06_09_18_Stop_and_Search_Consultation_Document_.pdf).

_____, 2019. UK Counter-Unmanned Aircraft Strategy (www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy).

United Nations, Security Council, Final report of the Panel of Experts on Libya established pursuant to resolution 1973 (2011), 8 March 2021 (www.un.org/securitycouncil/sanctions/1970/panel-experts/reports).

United States Department of Defense, 2021. Counter-Small Unmanned Aircraft Systems Strategy (https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf).

For more information, please visit:

www.un.org/counterterrorism/vulnerable-targets

2118451-5

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM