Building Resilience against Terrorist Attacks Involving Uncrewed Aerial Systems

Christina Schori Liang

April 2023

GCSP Policy Brief No.5

GCSP
Geneva Centre for Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation serving a global community of organisations and individuals. The Centre's mission is to advance peace, security and international cooperation by providing the knowledge, skills and network for effective and inclusive decision-making through executive education, diplomatic dialogue, research and policy advice.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Head of the Geopolitics and Global Futures Programme, and Mr Tobias Vestner, Head of the Research and Policy Advice Department, and managed by Ms Christine Garnier Simon, Administration and Coordination Officer, GCSP Geopolitics and Global Futures.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-408-0

About the author

Dr Christina Schori Liang is Head of Terrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy in Geneva, Switzerland.

She offers training and strategic policy guidance both in Geneva and for security actors worldwide including the United Nations, the European Commission, NATO, and the OSCE.

Dr Liang gives policy guidance on extremists and non-state armed groups. Since 2015, she has been a Visiting Professor at the Paris School of International Affairs, Sciences Po, Paris.

She holds a doctorate in International Relations and an MA in History and International Politics from the Graduate Institute of International and Development Studies, Geneva, Switzerland.

Introduction

Uncrewed aerial systems (UAS) are remotely piloted, pre-programmed, or controlled airborne vehicles. They are also referred to as unmanned aerial vehicles (UAVs) or, more commonly, drones.[1] Drones are becoming increasingly important for commerce, recreation and research, but their proliferation has also introduced new risks to public safety and international security. In the military sector, drones can perform an array of tasks such as surveillance, reconnaissance, targeting support, and direct or indirect attacks.

Remotely piloted systems were first used during the First World War. During the Cold War devices of this kind were further developed, but their use was restricted to reconnaissance missions.[2] In the United States, the terrorist attacks of 11 September 2001 and the subsequent "Global War on Terror'" increased the use of these systems by both the intelligence community and armed forces. In 2001-2002 UAS strikes in Afghanistan[3] and Yemen[4] marked the start of increasingly drone-oriented military operations. Both states and non-state actors possess the ability to acquire drones and the latter in particular can assemble and operate off-the-shelf drone technology. Drones are currently the "weapon of choice" for tracking and attacking insurgents and terrorists in a wide variety of insurgency-affected contexts. Most prominently, however, the current Russia-Ukraine conflict has been described as the "first full-scale drone war".[5]

According to the Center for the Study of the Drone, 113 states have military drone programmes.[6] Analysts conservatively estimate that 65 non-state actors are now able to deploy drones, while the figure is likely to be much higher.[7] In the last decade there has also been a rapid expansion of the number of smaller drones on the market for civilian use, in particular mini and micro drones weighing between 200 g and 50 kg. By 2024 the drone

[1] Strictly speaking, a UAV or drone is part of a UAS, which includes the UAV/drone, the person controlling it and the means of communication that allows the UAV to be controlled (Drone Academy Asia, "What Is the Difference between a Drone, a UAV and a UAS?", n.d.). However, the ever-increasing use of these systems has led to the three terms (UAS, UAV and drone) becoming effectively equated.

[2] United States General Accounting Office, *DOD's Use of Remotely Piloted Vehicle Technology Offers Opportunities for Saving Lives and Dollars*, Washington, DC, 1981.

[3] C. Woods, "The Story of America's Very First Drone Strike", *The Atlantic*, 30 May 2015.

[4] CNN, "U.S. Missile Strike Kills al Qaeda Chief", 5 November 2002.

[5] I. Khurshudyan et al., "Russia and Ukraine Are Fighting the First Full-scale Drone War", *Washington Post*, 2 December 2022.

[6] D. Gettinger, *The Drone Databook*, Center for the Study of the Drone, Bard College, 2022. Also see A. Callamard et al., *Use of Armed Drones for Targeted Killings*, Report of the UN Special Rapporteur on Extrajudicial, Summary, and Arbitrary Executions, A/HRC/44/38, 15 June-3 July 2020.

[7] K. Chávez and O. Swed, "The Proliferation of Drones to Violent Nonstate Actors", *Defence Studies*, Vol.21(1), 2021, pp.1-24.

market is expected to reach nearly USD 43 billion.[8]

The United Nations Security Council (UNSC) Counter-Terrorism Committee (CTC) has identified UAS as one of the key terrorist threats facing human security, and has already requested that action be taken to mitigate the threat of UAS falling into the hands of terrorists. UNSC Resolution 2370 (2017) (and later Resolution 2482 (2019)) "condemn[s] the continued flow of weapons, including small arms and light weapons, military equipment, unmanned aircraft systems (UASs) and their components ... and encourage[s] Member States to prevent and disrupt procurement networks for such weapons, systems and components".[9] UNSC Resolution 2617 (2021) noted with concern the increasing global misuse of UAS by terrorists to conduct attacks against commercial and government infrastructure and public places.[10]

Drones offer great benefits for society, but also pose immense security challenges. This Policy Brief will outline the challenges posed by drone technologies and the legal and operational security measures that can be taken to address them.

Security challenges

Threats posed by UAS

Drones offer a range of important civilian services, including industrial inspections, crop monitoring and treatment, and rescue and disaster relief operations.[11] However, their widespread availability, increased range and growing sophistication have led to increased use by nefarious actors worldwide. UAS are available in a wide variety of sizes, weights and navigation methods allowing for different operational purposes (see Annex, Table 1).

Armed non-state actors are increasingly using drones for reconnaissance, lethal attacks and targeted assassinations, both in and outside zones of armed conflict, with devastating humanitarian consequences for affected civilian populations.[12]

UAS are attractive for terrorists because they are increasingly accessible,

[8] https://droneii.com/the-drone-market-2019-2024-5-things-you-need-to-know.

[9] UNSC (United Nations Security Council), Resolution 2370 (2017), S/RES/2370 (2017), 2 August 2017.

[10] UNSC, Resolution 2617 (2021), S/RES/2617 (2021), 30 December 2021.

[11] UAS can also assist in the immediate aftermath of a terrorist incident by supporting crisis management efforts. For example, UAS can facilitate casualty evacuation procedures, provide real-time information about the size of the affected area and the nature and extent of the damage, or assist first responders to bring aid more rapidly and effectively to victims.

[12] WILPF (Women International League for Peace & Freedom), *The Humanitarian Impact of Drones*, International Disarmament Institute and Article 36, October 2017.

relatively affordable and require minimal training. Terrorists have deployed drones to attack military assets, diplomatic sites, international trade, energy infrastructure and civilian centres.[13]

While high-technology military armed drones still remain largely inaccessible to non-state actors (e.g. MQ-9 Reaper, RQ Global Hawk, etc.), the possibility of weaponising civilian drone technology provides terrorists with limited aerial military capacity.[14] Weaponised UAS are increasing in range and precision and rogue actors are capable of striking targets increasingly further away.

Deployment of and access to UAVs

Terrorists' use of drones is concerning for several reasons. Firstly, weaponised drones are increasing in range and precision, making them ideal for attacks on military and other targets deep in state territory. Terrorist groups can deploy drones at distances of up to 1,500 km to strike targets across national borders.

Secondly, civilian infrastructure, which may be far from zones of conflict, is now vulnerable to lethal drone strikes. Drones can travel through congested civil airspace to reach their target. Since 2020 drones have been used to target energy infrastructure, international shipping, international airports and the civilian centres of capital cities.[15]

The third concern is the growing issue of saturation drone strikes. Working in partnership with other unarmed UAVs, weaponised drones can be used to pinpoint and destroy air-defence systems, opening the gates for incoming volleys of rockets, missiles and other armed drones.

The fourth growing concern is the ubiquitous nature of drones. As of 2022, more than half a million drones were in private hands in the United States alone.[16]

The ability of terrorist groups to acquire, develop and use UAS is facilitated by several factors: (1) the unregulated 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

[13] UNSC, "Letter Dated 25 January 2022 from the Panel of Experts on Yemen Addressed to the President of the Security Council", 2022.

[14] A. Harper, "Drones Lower the Battlefield for Extremists", *The Interpreter*, 20 April 2018; G. Lasconjarias and M. Hassan, "Fear the Drones: Remotely Piloted Systems and Non-state Actors in Syria and Iraq", IRSEM Research Paper No. 77, 4 September 2019.

[15] J. Rogers, "Last Month, Three Drones Attacked an Israeli Tanker. Here's Why That's Something New", *Washington Post*, 19 August 2021. Also see UNCTED (UN Counter-Terrorism Committee Executive Directorate), "Greater Efforts Are Needed to Address the Potential Risks Posed by Terrorist Use of UAS", January 2021.

[16] B. Edwards, "Killer Drones: How Commercial Drones are Changing the International Security Environment", *Regional Threats Journal*, Issue 09, 10 July 2022.

(peroxide, ammonium nitrate, etc.); and (4) the wide availability on the Internet and social media of drone-related technical expertise provided by extremists, hobbyists and individuals.

Terrorists have found innovative ways to weaponise drones. Smaller UAVs are able to carry payloads of explosives weighing up to 8 kg/17.6 lbs. while there is evidence of larger UAVs being able to carry up to approximately 181 kg/399 lbs. Weaponised drones carrying explosives or chemical or biological agents will be increasingly within the reach of virtually any state, non-state actor and individual.

Non-state actors' use of UAS in conflict zones

A wide range of non-state actors have used drones in combat, including the Afghan Taliban, Boko Haram, Hamas, Hezbollah, Houthi rebels and the non-state group Islamic State (IS). Smaller drones are used for intelligence, surveillance, and electronic warfare measures, and assist in target acquisition to increase the precision and lethality of ground-based systems. Drones are used as decoys to distract security actors while strikes are directed elsewhere. Drones are also used to perpetuate and extend the psychological dimension of terrorism by spreading fear.

IS has repeatedly employed UAVs in conflict zones to discharge small grenade-size bombs. Although the use of such devices did not change the outcome of a particular conflict, it laid bare the potentially deadly impact of misusing unsophisticated UAS created for hobbyist or recreational purposes.

IS conducted strikes with drones carrying explosives that were used to kill enemy combatants in northern Iraq.[17] The group formed what it called an "Unmanned Aircraft of the Mujahedeen" unit.[18] In 2017 IS pinned down Iraqi security forces during a 24-hour period in Syria using commercial and homemade drones, executing 70 drone missions.[19] IS has also distributed online guidance on the use of drones and propaganda calling for attacks involving drones.[20] The group has used front companies to acquire commercially available low-cost, high-tech UAS in Asia, Canada and the United States and subsequently converted them for lethal use. Al-Qaeda was also reported to be actively attempting to develop UAS with greater payloads for the delivery of larger improvised explosive devices (IEDs).

[17] T. Gibbons-Neff, "ISIS Used an Armed Drone to Kill Two Kurdish Fighters and Wound French Troops Report Says", *Washington Post*, 11 October 2016.

[18] In 2017 IS boasted that its drone attacks had killed or wounded 39 soldiers in one week (UNCCT (UN Counter-Terrorism Centre) and UNICRI (UN Interregional Crime and Justice Research Institute), *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*, 2021).

[19] D. Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats*, Combating Terrorism Center, West Point, July 2018.

[20] UNCCT and UNICRI, 2021.

Groups are also able to acquire new technologies on the dark web.[21]

Reports from the UNSC CTC on the "Threats Posed by Misuse of Unmanned Aerial Systems (UAS) by Terrorists " maintained that in early 2021, IS and al-Qaeda affiliates demonstrated a growing capability in the use of drones in parts of West and East Africa. In East Africa al-Shabaab uses drones for reconnaissance and surveillance. There is concern that al-Shabaab could launch attacks on aircraft and civil aviation infrastructure.[22]

Drones can be armed with conventional weapons and potentially with biological, chemical, radiological and nuclear agents.[23] In 2015, a man flew a drone carrying radioactive sand onto the roof of the Japanese prime minister's office. In 2016, the potential grave risks of drones were highlighted at the Nuclear Security Summit. Since radiological material can be found in 130 countries, there are fears that this scenario could become a reality. In 2019, France's UCLAT[24] warned of "'a possible terrorist attack on a football stadium'" by using a drone to disperse a biological warfare agent.[25]

Targeted killings

Drones are also being used for targeted killings, until now mostly effectively by states, but most likely increasingly by terrorists and criminal groups. In August 2018, Venezuelan president Nicolás Maduro was the target of a failed assassination attempt using two GPS-guided, explosives-laden UAVs. In 2021, Iraqi prime minister Mustafa Al-Kadhimi escaped an assassination attempt when an explosives-laden drone targeted his residence. In 2021, a Taliban drone unit organised the targeted assassination of Piram Qul, an important ethnic Uzbek warlord.[26]

Policy implications

In 2020, the UN Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement Relating to Counter-Terrorism, launched a project to develop and promote technical guidance for UN member states to facilitate and support the implementation of Security Council Resolution 2370 (2017),[27] relevant subsequent resolutions,

[21] UNSC CTC (Counter-Terrorism Committee), "CTED's Tech Sessions: Highlights on 'Threats Posed by Misuse of Unmanned Aerial Systems (UAS) by Terrorists'", Special Meeting, Mumbai, India, 28-29 October 2022.

[22] Ibid.

[23] Rogers 2021; UNCTED, 2021.

[24] *Unité de coordination de la lutte anti-terroriste (UCLAT)* is a French government organisation consisting of representatives from all active branches of the National Police.

[25] This warning from a confidential UCLAT report was repeated in UNAOC (UN Alliance of Civilizations), *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies,* 2021, p.36.

[26] F. Qazizai, "The Drone Unit that Helped the Taliban Win the War", *New/Lines Magazine*, 15 September 2021

[27] UNSC, 2017.

good practices and international standards, especially as they pertain to preventing terrorists from acquiring UAS.

Building an international counter-UAS community

Through UNSC Resolution 2370 the UN established a global network of practitioners, subject matter experts, and relevant decision-makers who share a common focus on counter-UAS (C-UAS) technology, acquisition, planning, policy, doctrine, and standards. The aim of this community was to analyse how terrorists were using UAS and to understand how UAS could act as an effective counter-terrorism tool. In 2022, the United Nations Security Council Counter-Terrorism Committee held a special meeting in India that focused on "Countering the use of new and emerging technologies for terrorist purposes," including UAS, terrorist financing, and the internet and social media.[28]

Multiple organisations cooperate on UAS, including the UN Counter-Terrorism Executive Directorate (UNCTED), UN Office on Drugs and Crime (UNODC), UN Institute for Disarmament Research, International Organization for Migration, INTERPOL (specifically the INTERPOL Drone Expert Group), European Union (EU) Commission, and Global Counter-Terrorism Forum, which published the "Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems".[29] The World Customs Organization, International Civil Aviation Organization (ICAO) and UN Office for Counter-Terrorism (UNOCT) also work on preventing terrorists from abusing UAS.

National approaches

Several states have argued that UAS require a whole-of-government approach to further enhance research and knowledge on this threat and support partnerships with the private sector, academia, civil society, and UN agencies. A comprehensive whole-of-government strategy is needed to avoid variations in policies, the development and use of different standards, and the procurement and/or deployment of differently capable C-UAS systems.

Likewise, the fragmented or inconsistent application of policies to deal with UAS-related threats poses significant challenges to a state's ability to adequately counter such threats. Upstream measures often focus on activities aimed at preventing terrorists from acquiring UAS and their components, while downstream measures deal with the mitigation of the effects of, and response to, a particular UAS-related incident. Both levels of policy must be implemented in concert; none of them on their own will suffice to prevent and mitigate terrorists' acquisition and use of UAS and components.

[28] UNSC CTC, 2022.

[29] GCTF (Global Counter-Terrorism Forum), "Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems", n.d.

UNCTED presented a diagram at the Special Meeting of the CTC on countering the use of new and emerging technologies for terrorist purposes in New Delhi in October 2022[30] that outlines the multidimensional responses to threats posed by the misuse of UAS (see Annex, Figure 1). It highlights how states can reliably prevent terrorists and other nefarious actors from acquiring and using UAS and their components. The general premise is that by implementing effective upstream measures, fewer downstream measures will be required. This is further reinforced by a critical feedback loop through which downstream measures inform strengthened upstream measures.

UN response

UN Security Council Resolution 2617[31] recognises the increasing misuse of UAS globally, including "the misuse of unmanned aerial system by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places". It laid the groundwork for subsequent resolutions. UNSC Resolution 2617 calls for continued and enhanced cooperation among UNCTED, ICAO, UNODC, UNOCT, INTERPOL, and other relevant bodies on technical assistance and capacity-building to create synergies among counter-terrorism efforts. The UNSC is working on establishing non-binding guiding principles to assist UN member states that will include drafting recommendations to counter terrorist exploitation of UAS while respecting human rights and fundamental freedoms.

UNOCT has developed a good practices guide[32] on protecting vulnerable targets from drone attacks, in light of the fact that commercial or hobbyist drones are being shaped into weapons. 3D printing technology also results in the prospect of extremists being able to rapidly manufacture UAS spare parts.

A joint UNOCT-Conflict Armament Research project is under way to assess global trends regarding UAS use and misuse. The next steps will be to classify types of UAS (hobbyist, commercial, military, etc.) and establish a registration system so that they can be tracked.

[30] UNSC CTC, 2022, Session III: Developing Multidimensional Responses to Threats Posed by Misuse of UAS and Enhancing States Capabilities to Reliably and Sustainably Prevent Terrorists and Other Nefarious Actors from Acquiring and Using UAS and Its Components".

[31] UNSC, 2021.

[32] UNOCT (UN Office of Counter-Terrorism), *Protecting Vulnerable Targets from Terrorist Attacks Involving Unmanned Aircraft Systems (UAS)*, 2022.

Oversight mechanisms and standards

Academics are working towards building up a robust drone technology control regime.[33] An international UAS import/export control regime will require international leadership to help prioritise state commitments[34] to prevent the illicit transfer of drone technologies to non-state groups. It would mean that participating states would pledge to uphold international law and human rights in their use of drone systems; take collective action against those who breach these rules; and limit the global proliferation of the next generation of weaponised drones through licensing, tariffs, tracking, legal action, and/or quotas on specific dual-use systems such as those augmented with advanced artificial intelligence (AI), autonomous, and swarming technologies.[35] For the past five years the Drone Manufacturers Alliance Europe has contributed to the creation of the EU's first set of drone rules. In 2022, the European Commission finalised the European Drone Strategy 2.0,[36] which builds on the EU's safety framework for operating and setting the technical requirements for drones, and is the world's most advanced.

Policy recommendations

Designing a national action plan on UAS

In the interests of countering rogue actors' acquisition and use of UAS, the UNSC could ensure that UN member states adopt their own respective national action plans on UAS, in line with UNSC Resolution 1267, which calls on member states to consider developing a national action plan of action to prevent violent extremism. Each state should consider having an overarching policy based on a whole-of-government approach. A typical blueprint strategy for a national action plan on UAS could encompass the following key recommendations. Each state should:

1. create a government interdepartmental UAS committee to share information and help departments operating UAS to mitigate related threats;

2. identify the competent and responsible state authorities authorised to detect and, if necessary, intercept and/or disable UAS and their

[33] A. Callamard and J. Rogers, "We Need a New International Accord to Control Drone Proliferation", *Bulletin of the Atomic Scientists*, 1 December 2020.

[34] State military use of UAS also requires regulation. The disastrous August 2021 drone strike in Kabul during the Afghanistan withdrawal that killed ten civilians led to a review of drone practices by the US Department of Defense and to the establishment of the Civilian Harm Mitigation and Response Plan.

[35] For more on the public impact of submitting strikes to the UN for approval, see P. Lushenko et al., "Multilateralism and Public Support for Drone Strikes", *Research and Politics*, Vol.9(2), 2022. Also see C. Kennedy-Pipe et al., *Drone Chic: The Precision Myth*, London, Oxford Research Group, 2016.

[36] European Commission, European Drone Strategy 2.0: Creating a Large-scale European Drone Market, Press Release, 29 November 2022.

components in specific circumstances and contexts, and identify relevant legislation such as criminal statutes that sets clear standards for the legal and illegal uses of UAS;

3. put civil aviation legislation and regulations in place that are fit for purpose and cover the lawful use – including by civilians – of specific and defined categories of UAS and their components in defined airspace zones;

4. establish clear rules in national aviation legislation or regulations on the state's use of UAS (e.g. military and law enforcement use, use in defined airspace zones, etc.);

5. establish oversight mechanism to support critical infrastructure owners and operators in purchasing C-UAS equipment;

6. establish a system for licensing the commercial use of UAS that sets out specific areas where defined categories of UAVs are not to be operated. Such a system should provide for electronic remote identification and geo-fencing configurations as part of licensing criteria for emergency services' use of commercially produced UAV in restricted airspace and urban environments;

7. initiate information gathering and research on technological mitigation platforms that can be used to identify vulnerabilities in national airspace. Technological mitigation platforms should include a drone detection and monitoring system, a mass communication notification system, and physical airspace observation posts and communication systems;

8. work with all relevant stakeholders to design a roadmap that identifies the safety, security and economic objectives of the future national UAS industry;

9. establish a national C-UAS training centre to increase knowledge and promote public/private and interagency cooperation;

10. design, short-, medium- and long-term objectives to align the needs of the national UAS industry with government resources;

11. coordinate activities to enhance industry stakeholders' access to funding to explore new technologies to support industry, the military and national security actors; and

12. enhance international cooperation on C-UAS technologies.

Guidelines on the protection of civilians from the use of UAS

The UNSC can also work towards ensuring the protection of civilians from UAS by encouraging each UN member state to design a more robust legal framework that would underscore the following operational and legal principles, while improving transparency and accountability.

Operational principles

Each state should:

1. update and publish its policy on the use of drone technologies for military purposes, with explicit reference to the use of drones (a) for lethal strikes, and (b) in complex environments where allied partners are, or may be, involved;
2. clarify the processes in place to ensure that national rules of engagement and adherence to international law are upheld at all times; and
3. explain to the national legislative body the steps the state has taken and intends to take in response to the UN Secretary-General's call to action in May 2018 that states should lead the creation of common protocols among allies on the legal and effective use of drone technologies in complex environments.

Legal principles

Each state should:

1. set out the national position on the geographical scope of armed conflicts with non-state armed groups. In particular, national governments should clarify their position with specific regard to two criteria under the law of armed conflict: (a) whether it considers that lethal force may be used against members of a non-state armed group with which the country is involved in an armed conflict, when those persons are located in a different state from that in which the conflict is taking place; and (b) whether non-state actors operating across different states may be targeted in light of their affiliations with other groups;
2. focus attention on how to apply international human rights law in situations of armed conflict. In the EU, this would include state obligations under the European Convention on Human Rights rather than continuing to debate whether human rights law applies; and
3. publish national policy on the targeted killings of individuals in line with the precedents set by the United States and Israel. This policy should include (a) its legal basis; (b) criteria to be used and precautions applied in the selection of targets; and (c) the decision-making processes controlling the targeted killing of individuals.

Conclusion

The ubiquity of UAS will likely lead to a "third drone age" with "uncrewed aerial, ground and underwater vehicles".[37] Swarm attacks will increase in the future.[38] Notional swarming concepts range from large formations of low-cost UAS that could overwhelm adversary defensive systems to smaller, more tailored formations that could execute electronic attack or intelligence, surveillance and reconnaissance missions. Some analysts argue that swarms could have several advantages over individually deployed UAS, such as the ability to easily disperse combat power. This ability could in turn complicate an adversary's ability to target and neutralise the swarm, thus creating an unfavourable cost-exchange ratio for the defender.[39]

AI is on the horizon and will further benefit UAS operability. While terrorists might not be able to fully harness AI technology, they can still benefit from its dissemination. Self-piloted drones are in development, such as the EU's project to use AI drone swarms to protect borders. Some countries are already experimenting with drones with integrated AI algorithms capable of independently selecting objectives to be neutralised. These could include launching intelligent swarms of autonomous vehicles to deliver explosives in rapid, coordinated attacks while allowing attackers to be further removed from their targets in both time and location.

Rapid advances in drone technology (including in speed, payload, fuel cells and resistance-to-radio interdiction) will make countering the threat costlier and even more difficult. These new UAS technological innovations will require multilateral and rules-based approaches to build greater safeguards in the interest of national and international security. The prevention of the illicit transfer of drone technologies to non-state groups, in particular, requires international leadership. States must pledge to uphold international law and human rights; to take collective action against those who breach these rules; and to limit the global proliferation of the next generation of weaponised drones through licensing, tariffs, tracking, legal action, and/or the imposition of quotas on specific dual-use systems.[40]

---

[37] J. Rogers, "The Third Drone Age: Visions Out to 2040", Centre for International Governance Innovation, 28 November 2022.

[38] Swarming refers to cooperative behaviour – generally enabled by AI and networked communications – in which a group of UAS autonomously coordinate to accomplish a mission. A "swarming tactic" was evidenced by the Houthi attacks on the capital city of the UAE, Abu Dhabi, on 17 January 2022.

[39] An unfavourable cost-exchange ratio would occur if, in an attempt to neutralise the swarm, the defender uses a countermeasure (e.g. missile interceptors) with an aggregate cost that is higher than the aggregate cost of the swarm (P. Scharre, *Robotics on the Battlefield Part II: The Coming Swarm*, Center for a New American Security, October 2014, pp.20-21). An unfavourable cost-exchange ratio can also occur in countering a single UAS. For example, a US ally reportedly used a US$3 million Patriot surface-to-air missile to shoot down a US$200 UAS (C. Baraniuk, "Small Drone 'Shot with Patriot Missile'", BBC, 15 March 2017).

[40] Lushenko et al., 2022; Kennedy-Pipe et al., 2016.

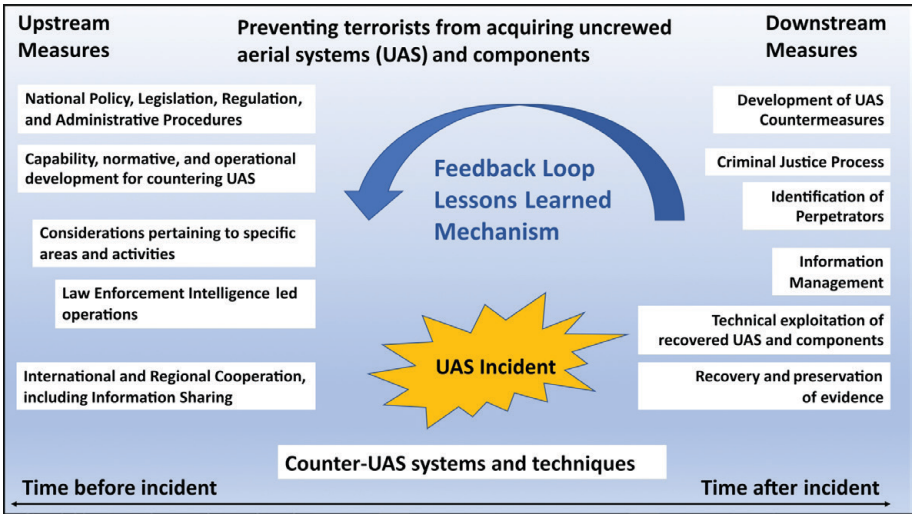
Annex

Table 1: Drone categories

Category	Weight (kg)	Type	Range (km)	Model(s)
High-altitude long-endurance (HALE)	600-14,000	Strategic	Unlimited*	Global Hawk
Weaponised drones	600-6,000	Strategic/ operational	Unlimited*	Reaper; Gray Eagle; Wing Loon; TB2 Bayraktar; Samad-3; Orion
Medium-altitude long-endurance (MALE)	600-1,200	Strategic/ operational	Unlimited*	Heron; Hermes 900
Tactical drones	150-600	Tactical (brigade/battery	200	Hermes 450; Orlan-10; Sky-Eye; Harop**
Small drones	15-150	Tactical (battalion	50	Scan Eagle; Puma; Switchblade 600**; Phoenix Ghost**; KUB BLA**; Lacet-3**; RAM-II**
Mini drones	2-15	Tactical (company	25	Switchblade 300**; Warmate**; DJI Mavic
Micro drones	0-2 kg	Tactical (troop/ group/individual)	5	Black Widow; Black Hornet

* With satellite guidance, range is only limited by the drone's fuel capacity.
** Loitering munition/"kamikaze" drones

Figure 1: Developing multidimensional responses to threats posed by UAS



Source: authors figure based on UNCTED module (2022)

People make peace and security possible

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-408-0

GCSP
Geneva Centre for Security Policy