Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems

Introduction

Unmanned Aerial Systems (UAS)[1] are a rapidly developing technology. UAS are and will increasingly be used in important, positive and legitimate ways by governments (e.g., emergency responses, firefighting) and the private sector (e.g., agriculture, pipeline monitoring, consumer goods delivery). But informed observers are concerned that also terrorists will continue to utilize UAS for their own illicit and unlawful aims. Possible misuses of UAS by terrorists extend beyond physical attacks and include conducting intelligence collection, surveillance, and reconnaissance; monitoring targets, security protocols, and patterns of behavior; using UAS to make indirect fire more accurate; collecting footage for use in terrorist propaganda; disrupting law enforcement operations; disrupting, interfering with or paralyzing key infrastructure, air traffic and economic assets; smuggling illicit goods across borders or into sensitive areas; intimidation and harassment; and inciting panic in mass gatherings. Terrorist attacks by UAS could be directed against a variety of targets, governmental, economic, and other critical infrastructure as well as other public targets (sometimes referred to as "soft targets")[2]. There is also a growing concern that UAS might be used during cyberattacks or as a delivery vehicle for explosives or chemical, biological, and radiological agents. UN Security Council Resolution 1540 (2004) (UNSCR 1540) 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. UNSCR 1540 also requires states to enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery. To the extent that UAS constitute such a means of delivery, this Memorandum may assist states in the implementation of these UNSCR 1540 obligations.

To date, terrorist use of UAS outside of the context of armed conflicts has been relatively rare. Terrorists have favored other kinds of weapons that are easier to acquire and operate (e.g., vehicles used for ramming attacks) or may have a more lethal impact (e.g., ground-based use of improvised explosive devices and firearms). Yet, UAS have improved significantly in recent years in terms of flight duration, ease of use, potential to be repurposed to drop a payload on targets, ability to be networked with civilian communication and with other UAS, and these technological capabilities are expected to accelerate. Both current and anticipated developments could overcome many limitations that, to date, might have limited terrorists UAS use. As UAS become more advanced, and more readily available at lower cost, they may have increasing appeal for terrorist uses. Growing commercial availability also means advancements in homemade or hobbyist UAS. Advanced autopilot components

[1] The International Civil Aviation Organization (ICAO) Circular 328 AN/190 *Unmanned Aircraft Systems (UAS)* proposes to define "Unmanned Aircraft Systems" as an "aircraft and its associated elements which are operated with no pilot on board". Therefore, in this Memorandum, the term "Unmanned Aerial Systems (UAS)" refers to aerial vehicles and associated elements that are operated without a pilot on board. UAS can be operated either remotely by a human pilot or autonomously without human intervention and can assume various forms, such as fixed-wing planes or multi- or single-rotor copters in various sizes. Sometimes these systems are referred to as "Unmanned Aircraft Systems". For the purpose of this Memorandum, there is no difference between the two terms.

[2] "Public", or "soft targets", as defined in the GCTF *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context*, are places which support community and economic prosperity, where people congregate to study, shop, dine, conduct business, be entertained, worship, or travel.

and an active online hobbyist UAS community make construction and operation of these aircrafts cheap and within the capacity of even low skilled individuals. This way, terrorists might increasingly attempt to manipulate off-the-shelf UAS or invest in self-made UAS to circumvent government restrictions. At the same time, UAS could become more difficult to counter with existing or anticipated counter-UAS technologies. Ultimately, terrorists could even employ UAS that have technological capabilities similar to current military-use platforms.

It should be noted that ISIL/Da'esh has repeatedly utilized UAS for attacks, surveillance, and battlefield propaganda in Iraq and Syria. Such knowledge and experience might be brought back from there by returning foreign terrorist fighters (FTFs),[3] or may serve as a blueprint for homegrown terrorists, including lone actors.[4] ISIL/Da'esh has produced propaganda calling for the use of UAS to attack targets in other regions across the globe. Other terrorist groups in the Middle East and West Africa have utilized weaponized UAS to attack targets.

The non-binding good practices contained in the *Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems* are intended to inform and guide governments in identifying, developing, and refining policies, practices, guidelines, regulations, programs, and approaches for countering the terrorist use of UAS. The Memorandum synthesizes the takeaways and knowledge 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 2018-19. It also draws important lessons from the GCTF *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context*.[5]

The *Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems* identifies 26 good practices in four areas for states' consideration:

1. 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.
2. 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.
3. Implement Policies and Regulations, Establish 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

[3] For guidance regarding effective responses to the FTF phenomenon, see GCTF *The Hague – Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon*.

[4] For guidance regarding homegrown terrorism, see GCTF *Rabat – Washington Good Practices on the Prevention, Detection, Intervention and Response to Homegrown Terrorism*.

[5] The GCTF *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context* identified understanding and countering malicious use of new technologies like UAS as a priority area of attention for governments and industry.

incidents. Governments should also develop crisis management and mitigation strategies to react adequately to UAS incidents.

4. 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.

The following good practices are intended to address the use of UAS by terrorists outside of the context of armed conflicts. While the use of UAS by violent non-state actors during instances of armed conflict might require states to take measures similar to the good practices contained in this Memorandum, they are not intended to be applied in that context, nor in response to the use of UAS by national defense forces during armed conflicts.[6] While the good practices contained in this Memorandum are solely and specifically compiled to address the terrorist use of UAS, they may also prove useful to respond to other malicious (e.g., by criminal enterprises) or negligent, unwitting or careless misuses in a domestic setting.[7] The Memorandum is not intended to be exhaustive. States should consult other past or future regional and international documents and initiatives to ensure that effective counter-UAS efforts are in place.[8]

When countering the terrorist use of UAS, states should at all stages comply with their obligations under domestic and international law. Further, states should not impede beneficial and legitimate UAS uses.

Good Practices

I. Assessing the Risk, Assessing Vulnerabilities, and Raising Awareness

Good Practice 1: Integrate the potential use of UAS by terrorists into routine risk assessments.

While UAS are and will be used mostly for legitimate and beneficial purposes, they can also be misused by terrorists. Terrorist uses of UAS outside of the context of armed conflicts have been relatively rare to date. Even so, the sophistication of certain terrorist groups and lone actors, as well as continued advances in readily available UAS and the growing commercial use of UAS, makes an increase in terrorist experimentation and uses of UAS more likely. Risk assessment should take account of relevant developments and lessons learned and should enable states to incorporate available information and intelligence into a risk-based approach to the threat. States should assess the probability of, vulnerability to, and possible consequences of terrorist uses of UAS while also comparing the risk of terrorist use of UAS to other threats. This will enable states to ultimately rank and prioritize the terrorist UAS threat in relation to other threats.

---

[6] Therefore, if not indicated otherwise, in this Memorandum the phrase "terrorist use of UAS" and similar phrases refer solely to the use of UAS by terrorists outside of the context of armed conflicts.

[7] As this Memorandum addressees practical means to counter the terrorist use of UAS outside of armed conflicts, the phrase "terrorist use of UAS" and similar phrases are used throughout the document. Whether certain good practices may be applicable for uses of UAS by other malicious actors or negligent unwitting or careless users depends on the particularities of the situation.

[8] The UN Security Council has already recognized the threat of UAS in the hands of terrorists, for example in Resolution 2370 (2017). INTERPOL will issue its *Drone Response and Forensic Guidelines* in 2019. For the initiatives of the United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), see footnotes 15 and 16.

Certain developments related to transnational terrorism might not obviously be connected to the specific threat of terrorist use of UAS, but might nonetheless have an impact on it. For example, returning FTFs may seem at first blush to be a problem set distinct from terrorist misuse of UAS. Nonetheless, their return may result in a growing threat of terrorist use of UAS in their countries of origin, or even third countries, if they bring back with them knowledge about the manufacture, use, and weaponization of UAS. Because the activities of terrorists can be transnational, states should enhance their cooperation in sharing lessons learned, information about prosecutions, and evidence about UAS uses and plots as well as relevant transfer and proliferation of equipment, weaponry and knowledge.[9]

States should also stay current with general and UAS-specific technological developments and commercial innovations, as well as innovative, often legitimate, ways UAS are and may in future be used (e.g., the spraying of crops that may serve as inspiration for terrorists to use UAS to disperse biological agents), and assess their impact on the broader threat environment. Technological innovations (e.g., the enhancement of UAS using artificial intelligence, automatic image recognition, jet propulsion, 5G networks, collision avoidance technologies) could alter the scale, scope, magnitude, lethality, and trajectory of the threat posed by terrorist use of UAS. States should constantly monitor such developments, and their potential implications for the UAS risk. In addition, states should constantly and actively research and monitor recent technological developments and potential innovative uses and emerging capabilities of both commercial off-the-shelf and hobbyist UAS and gain insight from experts and academia as well as through innovative activities, such as "hack-a-thons", events that bring together (non-professional) experts in a particular field to experiment with or advance hard- and software. A fundamental understanding of current and anticipated UAS technologies will better prepare states to develop effective countermeasures.

A commonly articulated concern regarding the development of UAS technology is "drone swarms," a large number of UAS communicating and operating with each other, forming a massive, coordinated stream. "Drone swarms" pose a significant threat for a variety of reasons, especially their real-time information sharing and their ability to act and coordinate with one another that create resilience to saturate defense. This threat serves as one example of why states should constantly take into consideration technological innovations in routine threat assessments.

Good Practice 2: Recognize there are multiple ways terrorists may use UAS.

States should consider all possible, innovative ways terrorists might use UAS. While terrorist attacks with or enabled by UAS might have the highest impact from a national security perspective, states should recognize the diversity of potential malicious uses of UAS by terrorists. Recorded uses, predominantly in the context of armed conflicts, range from physical attacks[10] (e.g., by equipping a UAS with improvised explosive devices to conduct munition drop or direct (kamikaze) strikes in support of main attacks or to target first responders) to conducting intelligence collection, surveillance, and reconnaissance; monitoring targets, security protocols, and patterns of behavior; using UAS to make indirect fire more accurate; collecting footage for use in terrorist propaganda; disrupting or paralyzing key infrastructure, air traffic and economic assets; smuggling of illicit goods across borders or into sensitive areas. UAS could also be used as a diversion to distract or disrupt law enforcement, or to intimidate or incite panic in mass gatherings.

---

[9] For guidance regarding sharing of evidence related to terrorism prosecutions, see GCTF *Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects*.

[10] As recognized in the *International Convention for the Suppression of Terrorist Bombings* (New York, 15 December 1997).

As is the case with the myriad manners of use, the targets of terrorist uses of UAS can vary widely. UAS could be used against governmental, economic, and other critical infrastructure[11], or public targets[12]; against high-profile or randomly selected individuals, or during major public gatherings (e.g., sport events, concerts, parades). UAS-based attacks can also be designed to interfere with critical or economic infrastructure. Finally, terrorists might also attempt to hack or misuse UAS that are intended for beneficial or recreational purposes by governments or the private sector to create disruption or chaos, to avoid or mislead countermeasure systems, or during cyberattacks.

Given the variety of ways and targets, states should conduct a comprehensive threat assessment, and consider, test, discuss, and implement a variety of measures to counter the threat. States will always have to prioritize certain threat scenarios over others, but it is imperative that a range of possible *modi operandi* are taken into consideration in the overall threat assessment.

Good Practice 3: Engage in a comprehensive vulnerability assessment to identify security and protection gaps.

Due to the potential of UAS to overcome traditional barrier defenses (e.g., fences), otherwise well-protected sites, such as nuclear power plants or diplomatic facilities, may be vulnerable to UAS attacks. To identify existing vulnerabilities and security gaps, states should, building upon their general threat assessment as described in Good Practice 1, engage in a comprehensive vulnerability assessment. The vulnerability assessment should review existing physical and procedural security measures and their potential effectiveness against UAS attacks taking into account key features of the threat, including speed and altitude; the limited reaction time for security forces; and the ability of malicious actors to remotely operate UAS. The vulnerability assessment should also take into consideration locations of suitable launching sites for UAS in proximity to a possible target.

Thus far, most (attempted) terrorist or criminal UAS uses outside of the context of armed conflicts have targeted governmental facilities. Consequently, attention should be paid to these places and to government officials. This, however, does not imply that other critical infrastructure[13] or public targets,[14] such as public events, hotels, and airports, are less attractive to terrorists. Rather than a change in tactics, the limited number of UAS attacks on non-governmental targets appears to be the result of the limitations of current UAS. With the forecast developments of UAS, the risk of attacks against non-governmental targets will increase and should be taken seriously when assessing the vulnerability of public targets and non-governmental critical infrastructure. States should prioritize the protection of certain possible targets based on their risk and vulnerability assessment.

---

[11] As explained in *CTED Trends Report: Physical Protection of Critical Infrastructure against Terrorist Attacks*, despite slightly different national definitions, "critical infrastructure" can be defined as assets, systems or organizations that are responsible and essential for providing and maintaining vital functions of society. This might include, but is not limited to, communication systems, such as radio and television; information technology, such as Internet exchange points; emergency services; energy and industrial facilities, such as nuclear or chemical facilities; financial infrastructure; public services, such as health facilities; transportation systems; and water facilities.

[12] For a definition of "public targets", see footnote 2.

[13] For general guidance regarding the protection of critical infrastructure against terrorist attacks, see *CTED Trends Report: Physical Protection of Critical Infrastructure against Terrorist Attacks* and CTED, INTERPOL, United Nations Office of Counter-Terrorism (UNOCT) *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*.

[14] For general guidance regarding the protection of public targets against terrorist attacks, see GCTF *Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context*.

Good Practice 4: Share risk assessments across different sectors.

With the expanding commercial and public use of UAS across multiple sectors (e.g., emergency response, agriculture, public safety, aviation, telecommunications, public health services), different stakeholders will encounter variations of risk and vulnerability pertaining to potential interference, disruptions or attacks by UAS.

Given the intersection of UAS' growing ubiquity across multiple sectors, an effort should be made to analyze, discuss, and compare commonly shared and distinctly experienced threats across different sectors, governmental and non-governmental alike. This will improve the collective understanding of the risk across different spheres. Information sharing with relevant stakeholders as described in Section II is critical to achieve this goal.

Good Practice 5: Avoid UAS fatigue.

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. Governments should take steps to avoid this syndrome, referred to here as "UAS fatigue".

To help avoid UAS fatigue, governments (across all levels) should be transparent about the threat (underpinned by well-informed threat assessments), and provide regular updates to its civil servants and engage and partner with the general public as described in Good Practice 15. This may also include methods for reporting suspicious or observed UAS activity to assist governments and organizations in developing intelligence and understanding, which may inform future updates and threat assessment. While this approach may seem counterintuitive, it is critical. The antidote to complacency is consistent engagement and information sharing. Governments should maintain open lines of communication within their national security caveats to inform officials and, if appropriate the general public about the threat of terrorist use of UAS and necessary preventive and response measures.

Good Practice 6: Raise awareness of the threat while avoiding unnecessary public alarm.

States should feel a sense of urgency to raise awareness and create a common understanding about the threat of terrorist use of UAS and the safety hazard from negligent misuse of UAS at a political and public level, without unnecessarily alarming domestic populations and without compromising the beneficial and legitimate uses of UAS. Achieving both objectives requires a delicate balancing act. Efforts to raise awareness should not trivialize the threat, but it is equally important not to unnecessarily alarm the public to fear UAS, which continue to be used for a variety of peaceful and productive purposes. States should therefore engage with the public in a constructive manner that clarifies the potential threat posed by the illicit use of UAS, while noting the common benefits of UAS. Messages should highlight regulatory requirements and responsibilities. Additional messages could note, in unclassified, broad terms, the various countermeasures that are taken to keep the public safe, as well the practical advice on appropriate responses to UAS incidents. Transparency of data, statistics, and figures related to the use of UAS, will be critical in ensuring citizens' trust in authorities tasked with keeping the public safe.

The efforts should address various issues, including privacy, regulatory requirements for ownership and operations responsibilities under a future unmanned aircraft system traffic management (UTM), both within and across borders. Transparency of data, statistics, and figures related to the terrorist

use of UAS, as well as the potential threat, will be critical in building and maintaining public trust. Engaging with the general public is further and in more detailed described in Good Practice 15.

II. Enhancing Information Sharing, Engaging with Relevant Stakeholders, and Educating the Public

Good Practice 7: Identify and establish knowledge exchange and information sharing with relevant stakeholders.

The terrorist UAS threat is multifaceted and spans across borders. It thus demands a response by a broad coalition of stakeholders. States should identify the relevant actors, as put forward in Good Practices 9-15, with whom to exchange knowledge and, where appropriate, information and intelligence. Information sharing should take place during all stages of implementing a counter-UAS strategy. It should include sharing information about the threat as described in Good Practice 4; about regulations in various jurisdictions to prevent exploitable loopholes (e.g., different requirements for UAS manufacturers to equip UAS with precautionary technological solutions) and to share best practices; about perpetrators of terrorist-related UAS incidents, and criminal prosecutions; about responses adopted by law enforcement and other actors; and about the effectiveness of various countermeasures in different operational conditions.

Information sharing calls for states to establish an active dialogue with key stakeholders. States should ensure, where this has not yet happened, that they establish points of contact that are competent for receiving relevant information.

Good Practice 8: Develop a common lexicon and tools that enable information sharing.

To share information effectively, stakeholders should understand one another. Divergent lexicons and definitions can undermine an effective mutual understanding. States and regional and international organizations should work towards a common lexicon and standardized definitions for discussing UAS to ensure that cooperation is effective. A common lexicon can be developed through intergovernmental exchange as described in Good Practice 9, or within and in cooperation with regional and international organizations as described in Good Practice 12. Several states and regional and international organizations, such as the European Union (EU) and the North Atlantic Treaty Organization (NATO), have already initiated efforts designed to develop common lexica. States should build awareness of existing efforts, and consider joining and supporting these efforts.

A common lexicon should, at a minimum, include shared classifications of different categories of UAS (e.g., based on size or capabilities) and of incidents (e.g., negligent incidents and terrorist misuses). While desirable, there is no need to perfectly align every definition or classification, as some states will have slightly different understandings or practices. However, states should have as much in common as is needed to enable them to conduct a common risk and vulnerability assessment, and to cooperate with one another when setting up and establishing regulations, policies, and countermeasures. If a common lexicon is agreed upon, states should, where possible, use shared definitions in their own UAS legislation. This will facilitate knowledge exchange, intergovernmental cooperation, and comparison of the rates of success of regulations, policies and countermeasures.

When developing a common lexicon, states should also work towards common standards for the testing of UAS and UAS countermeasures. When comparing test results of countermeasures, it is crucial that states adhere to the same standards and protocols.

When states cooperate with non-state actors (e.g., private industry or academia), they should similarly ensure that a shared language is used. Depending on the frequency of cooperation, such efforts can be undertaken on an *ad hoc* or permanent basis.

There is a need for a common database to share information about terrorism-related UAS incidents, developments and countermeasures. Such a database could be maintained at either an international, regional, national, or sub-state (e.g., academia or private sector) level and would enable states to realistically assess the threat of terrorist UAS use, countermeasures, and other relevant information. States should therefore develop such database in a common effort, or, to avoid fragmentation, join existing efforts by other actors, such as INTERPOL. However, care should be taken to ensure the collection and repository of such data does not disclose vulnerabilities or sensitive security information.

Good Practice 9: Enhance intergovernmental knowledge exchange and information sharing.

In combating the transnational threat of terrorist use of UAS, states should enhance their efficacy by exchanging best practices and lessons learned with other countries and governments. It is crucial to regularly convene major national and, where appropriate, regional and international stakeholders to discuss, among other matters, the technological evolution of UAS, the most effective methods of countering the threat posed by terrorist use of UAS, and potential gaps in practices and policies, both within and across states. To enhance international cooperation on the issue, an intergovernmental knowledge exchange should be established or enhanced. It may also be beneficial to make use of regional coordination centers that allow the sharing of information that is regionally relevant. Regional counterterrorism centers, where they exist, may serve as a platform for these regional exchanges. If such centers do not exist, states should consider establishing them to share information about regional terrorist activities in general and the threat of terrorist use of UAS in particular.

International knowledge exchange can also compare various governmental approaches and the variance in constitutional and other legal limitations on government regulations. Such awareness will be important to understanding, and countering, terrorists' ability to exploit the differences in regulations, authorities, and policies across jurisdictions. Information shared may also include lessons learned from prosecutions and law enforcement activities.

Information about terrorist activities might be classified intelligence that cannot easily be shared with other governments. Therefore, states should make an effort to identify and declassify key information, or portions thereof, where it is possible, to enable effective information sharing.

Good Practice 10: Establish and enhance coordination between national and local authorities.

While a strategy to counter terrorist use of UAS might be developed at a national, regional or international level, local authorities will most likely be tasked with actually putting these strategies into practice and countering UAS. Therefore, it is imperative to ensure information- and intelligence-sharing through enhanced coordination between national and local authorities within a country, and to raise awareness of the threat on the local level.

This coordination calls for a variety of measures. Local authorities should be educated in differentiating legitimate from terrorist use of UAS; in how to respond to suspicious activity; in the use of countermeasures; and, where they exist, in national capacities to support local authorities. Similarly, local authorities should be encouraged to actively share their experiences, best practices and lessons learned with the national level. Coordination between the local and national level can also be improved by a standardized reporting scheme of UAS incidents.

To ensure a well-functioning coordination between national and local authorities, states should establish a national coordination point for counter-UAS efforts and respective counterparts on the local level. The national coordination point can be tasked with developing a national action plan that outlines relevant policies, procedures, countermeasures and strategies, and with disseminating this information among the local focal points. Alternatively, the local authorities may be asked to develop local action plans that are subsequently reviewed and coordinated by the national coordination authority.

Where competencies to counter UAS are divided among different national and local authorities, states should hold regular joint exercises with relevant units.

Good Practice 11: Establish and enhance coordination with national defense forces.

While the good practices contained in this Memorandum are limited to the terrorist use of UAS outside of the context of armed conflicts, states should take into consideration the experiences and lessons learned from national defense forces. Many military branches have already gained experience in countering the use of UAS by violent non-state actors during instances of armed conflict.

In order to protect against all malicious and dangerous uses of UAS, states should actively learn from defense forces on national, regional and international levels. In doing so, states should take into consideration the particularities of military engagement. It is important to note 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.

Good Practice 12: Establish and enhance coordination with regional and international organizations.

States should also enable and conduct information sharing with regional and international governmental organizations. Such organizations are a proven platform for hosting or assisting interstate cooperation, delivering valuable knowledge and carrying out analyses of states' resources (e.g., regarding the implications of technological UAS developments in the fight against terrorism). States should therefore make an effort to identify relevant regional and international organizations.

For example, the United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) established a variety of initiatives that may be of relevance for countering the terrorist use of UAS and interconnected issues.[15] Consequently, CTED is a crucial stakeholder when assessing gaps in the protection against the terrorist use of UAS and developing counter-strategies. It further constitutes a valuable platform for the sharing of good practices and successful responses for countering terrorist use of UAS, and an accelerator for cooperation and partnerships with other

[15] During the course of the initiative, CTED published its *CTED Trends Alert* on the risks posed by the terrorist use of UAS that is designed to raise awareness of the threat within the UN and among states and other relevant actors. The Trends Alert also collects and systematizes different national, regional and international approaches, challenges and initiatives. For CTED's efforts with respect to the protection of critical infrastructure against terrorist attacks, see footnote 11. Further guidance for states, including for preventing the proliferation of weapons by terrorists, see CTED *Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions*. Regarding the issue of the flow of foreign terrorist fighters, see CTED *Madrid Guiding Principles*.

relevant actors (e.g., academia[16], the private sector and other regional and international organizations).

Good Practice 13: Establish and enhance coordination with Civil Aviation Authorities, Air Navigation Services Providers and relevant agencies governing aviation safety and communications.

Civil Aviation Authorities (CAAs), Air Navigation Services Providers (ANSPs) and relevant national, regional and international agencies governing aviation safety and communications are important stakeholders for efforts to counter the terrorist use of UAS, and some have already made comprehensive efforts.[17] In particular, states should partner with CAAs, ANSPs and relevant agencies governing aviation safety and communication in two regards.

CAAs, ANSPs and relevant government authorities governing aviation safety and communications are indispensable when setting up UAS operational safety and air traffic regulations and a future UTM. In most countries, CAAs are responsible for aviation safety regulations, while either CAAs or ANSPs monitor airspace; therefore, these entities might be able to identify non-compliant in-flight UAS. States should work together with CAAs, ANSPs and relevant agencies governing aviation safety and communication, and learn from their experiences, when enacting rules and establishing measures to regulate UAS operations. States should also be in constant communication with them to ensure that information about suspicious UAS are exchanged in real-time.

CAAs, ANSPs and relevant government authorities governing aviation safety and communications should also be regarded as crucial stakeholders when engaging in countermeasures against UAS. As countermeasures are likely to cause unintended consequences, particularly in relation to the safety of civil aviation and radiofrequency-based (communication) systems, states should coordinate their counter-UAS activities with the relevant governmental agencies so that they can assist in mitigating consequences to the greatest extent. States should also cooperate with these entities when developing and testing countermeasures, as these entities can provide valuable early input on the consequences of countermeasures on aviation safety and operations.

Good Practice 14: Establish and enhance coordination with private industry and other non-traditional stakeholders.

Cooperation with private industry and other non-traditional stakeholders in countering the misuse of UAS by terrorists is also indispensable. These actors share many of the same interests as states in countering the misuse of UAS by terrorists. Public Private Partnerships (PPPs) have been relatively effective in other areas of counterterrorism, including countering the financing of terrorism and protecting public targets from attack. PPPs should be considered an integral aspect of successful counter-UAS strategies and can involve one or various industry sectors and stakeholders.

The active involvement of industry representatives during the regional workshops demonstrated that private industry is equally concerned about terrorist use of UAS, and is able and willing to share their unique expertise to contribute to a comprehensive counter-UAS strategy.

---

[16] CTED launched its *Global Research Network (GRN)* in 2015. It is aimed at leveraging the expertise in terrorism-related topics of research institutes and think tanks from across the globe.

[17] ICAO has produced its extensive *The ICAO UAS Toolkit* containing best practices and recommendations for developing UAS regulations and training and education programs, as well as an overview of current UAS regulations in different states, an awareness campaign, and educational materials for hobby pilots. The International Air Transport Association (IATA) has issued its *IATA Information Bulletin: Key Considerations when protecting manned aviation from drones*. The US Federal Aviation Administration (FAA) has built an extensive library of guidance for UAS pilots, authorities and governments, including a mobile application for hobby pilots.

UAS manufacturers can integrate early detection measures (e.g., remote identification capabilities) and precautionary tools (e.g., geo-awareness and geo-fencing functions that are activated in proximity to sensitive sites) to prevent the misuse of UAS. The counter-UAS industry can further provide insights on countermeasures. Other industries can also be valuable stakeholders, such as the telecommunications industry, which could provide real-time data about active flights in particular areas. Private industry may also be able and willing to share information about UAS operators engaged in suspected wrongdoing or other relevant forensic data (e.g., location data) in the aftermath of an incident.

As is further described in Good Practice 17, UAS vendors can play a vital role in preventing the illicit proliferation of UAS and UAS equipment. States should make an effort to educate UAS vendors to identify and report suspicious purchases.

States should, in constant exchange with the sector and without impairing their justified economic interests, explore and mandate specific security-enhancing information and measures that can reasonably be expected to be provided and taken by private industry. This might include early information about technological developments; the integration of early detection or precautionary tools (e.g., remote identification capabilities and geo-fencing) as described above, and technological solutions that enable non-kinetic countermeasures *(*e.g., specific receivers for certain frequencies used by law enforcement agencies); the installment of robust systems that prevent the illicit hacking of UAS, including regular security updates; the provision of (real-time) flight data, possibly anonymized; assistance in the registration of UAS (e.g., by disabling motor capabilities until a successful registration); informing the public about relevant regulations and precautionary measures (e.g., through leaflets or online information) and offering training to pilots.

States should also work with and learn from organizers of major public events. Such events are usually preceded by the development of comprehensive security assessments and planning that may be useful when developing a broader counter-UAS strategy.

Finally, academia should play a role in countering the threat of terrorist use of UAS. Academia is a vital stakeholder for assessing the terrorist threat and connected key developments as well as technological developments of UAS and countermeasures.

Good Practice 15: Engage and partner with the general public on the safe use of UAS and appropriate responses to terrorist use of UAS.

With the increasing accessibility of UAS for hobby pilots and commercial enterprises, the number of UAS flown for recreational and commercial purposes will increase significantly. While states should refrain from generally prohibiting and hampering such legitimate and beneficial use, it is critical to ensure that the public is aware of and adheres to UAS regulations and policies as further and in more detail described in Good Practice 17. Ultimately, this will make it easier, for the general public and relevant authorities alike, to distinguish legitimate from terrorist uses of UAS and reduce the risk of false alarms and UAS fatigue.

Therefore, states should engage with the public to educate on the safe and compliant use of UAS. Such safe use of UAS should entail all necessary operational limitations on UAS operators as described in Good Practice 17. Preventive communication offers the possibility to make known and accessible to the public relevant domestic rules and regulations and precautionary measures and policies. This can be done through online information, leaflets that UAS manufacturers deliver along with their products, and obligatory or voluntary courses for UAS pilots. States should also ensure that the public

is aware of no-fly zones through public information and clear signage, and, where possible, through enabling the incorporation of these zones into UAS software as described in Good Practice 14.

States should also inform the general public on how to respond appropriately to terrorist use of UAS. Firstly, the public may be involved with identifying suspicious UAS. Besides raising general awareness of the threat as described in Good Practice 6, states should establish, and, when it comes to national security concerns, make known to the public, the signs of possible unauthorized UAS activity, as well as how and where to report such activity. Secondly, the public should be educated to adequately respond to UAS incidents. This should be done in a way that does not trigger unnecessary public alarm as advised in Good Practice 6 and that does not lead to UAS fatigue as outlined in Good Practice 5.

III. Implement Policies and Regulations, Establish Crisis Planning

Good Practice 16: Respect domestic and international obligations and beneficial uses of UAS and justified economic interests.

States need to ensure that all measures taken fully comply with their obligations under applicable domestic and international law. Equally, states should not unduly impede beneficial uses of UAS and justified economic interests of the UAS industry.

Good Practice 17: Explore and implement regulations and policies that minimize the potential for misuse of UAS by terrorists.

States should not focus solely on regulations and policies that mitigate the impact of terrorist use of UAS. Instead, states should implement regulations and policies that minimize already the potential for misuse of UAS by any actor. When doing so, states should ensure that they do not unduly impair beneficial uses of UAS. A regulatory and policy framework to minimize the potential for misuse of UAS should rest on three components.

Firstly, states should enact regulations and policies to provide airspace awareness. The most effective method is establishing electronic remote identification and early detection measures that enable the monitoring of all UAS in a particular airspace, both described in Good Practice 18.

Secondly, states should enact regulations and policies that provide appropriate limitations on the operation of UAS, including limitations on their illegal proliferation. This might include regulations allowing states to monitor and track suspicious purchases of UAS, such as through import and export controls of UAS and other UAS equipment, or through restrictions on purchasing UAS of a certain size or capability. To prevent the circumvention of such non-proliferation regulations and policies that often take place across borders, states should enhance their transnational coordination, including by reinforcing mechanisms of export control, possibly through regional or international organizations, to exchange critical information and to enforce rules against transnational illicit proliferation of UAS technology.[18]

Regulations and policies that provide appropriate limitations on the operation of UAS should entail operator licensing and UAS registration requirements as further described in Good Practice 23. The former may include obligatory or voluntary courses and an examination before receiving permission to fly UAS and could also enable a background check of UAS pilots. In the event of a UAS incident,

[18] For guidance regarding border management in the context of counterterrorism, see GCTF *Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters"*.

licensing and registration requirements may enable states to identify the operator and facilitate the investigation of the incident.

To provide appropriate limitations on the operation of UAS, states should also consider creating reasonable performance and capability limitations designed to reduce the potential for misuse. Among other measures, states should consider restrictions on airspeed and altitude in certain classes of airspace, as well as appropriate restrictions for the purposes of permitted UAS flights in certain airspace, such as state critical infrastructure and national security sites. Regulations along these lines help to create norms of behavior that assist security personnel in more effectively identifying non-compliant operations that may require the use of technical countermeasures or enforcement action. However, these limitations should not overly constrain the legitimate use of UAS.

Thirdly, states should further enact air restrictions around people, emergency, national security and law enforcement activity, or infrastructure, such as airports, mass gatherings, sport stadiums, etc. Such flight restrictions could be enforced by geo-awareness and geo-fencing as described in Good Practice 23, or, in extreme situations, kinetic or non-kinetic UAS countermeasures as described in Good Practice 24.

Good Practice 18: Explore and implement regulations and policies that enable the detection of UAS and effective countermeasures.

Many countries lack the regulations and policies necessary to enable the effective detection of UAS and effective responses to UAS misuse, including law enforcement or regulator action against operators. While most governments recognize the necessity for such regulations and policies, the complexity of the topic, the technical particularities, and the involvement and shared responsibilities of various national, international and regional agencies and bodies complicate the process. However, to avoid legal uncertainty and to allow all relevant stakeholders, such as law enforcement agencies, to effectively counter terrorist UAS threats, it is indispensable that regulations and policies are in force before incidents occur. Such regulations and policies are most needed in regard to operational limitations on UAS as described in Good Practice 17.

States should carefully consider which stakeholders have the greatest need to exercise capabilities to detect and counter suspicious UAS, and whether those stakeholders have the technical ability and training to use their capabilities in a manner that does not threaten the safety and efficiency of the airspace system, communications networks, or privacy interests. Use of a risk-based approach to countering terrorist UAS threats is vital as the use of some countermeasures may result in safety hazards equal to or even greater than the potential hazard posed by the terrorist UAS operation.

Good Practice 19: Establish crisis management and mitigation strategies for UAS incidents.

No strategy can guarantee complete security from terrorist use of UAS. States should therefore develop adequate and specific crisis management strategies that mitigate the impact of UAS incidents. Emergency protocols for all relevant stakeholders, including an early assessment of the situation, are key to ensuring the most effective response to terrorist use of UAS. It is critical that all relevant stakeholders on the national and local level that might be required to respond to a UAS incident are sufficiently trained in dealing with the particularities of such incident. In particular, states should explore ways to secure the airspace above crowded areas as fast as possible after a UAS incident has occurred. A crisis management strategy is especially important to protect airports and high-profile public events, which may be particularly vulnerable to UAS attacks.

When establishing these protocols, states should review existing crisis and mitigation strategies that were developed in order to address other public security and safety threats. These strategies can serve as a blueprint for the development of a UAS emergency protocols and strategies. Nonetheless, states should ensure to adapt existing crisis management strategies to the distinctiveness of the UAS threat.

Good Practice 20: Explore and implement regulations and policies that facilitate prompt and comprehensive investigations and allow effective prosecutions, and appropriate sanctions for terrorist uses of UAS.

While prevention of terrorist use of UAS is key, it is also important that states put in place regulations and policies that enable effective investigations of UAS incidents and enforcement action as necessary. It is crucial to conduct investigations immediately following incidents to determine whether there is proof of a terrorist intent, whether incidents were of other criminal nature or occurred solely because of negligence or non-terrorist related criminal activity. Investigations should, where criminal or disorderly behavior is proven, lead to effective and swift prosecutions and, if a person is found guilty, to appropriate sanctioning or punishment of identified offenders. While this might require the modification of national legislation, a systematic prosecution could have a deterrent effect for certain terrorist actors or individuals who violate export control regulations. Civil investigations are also necessary to ensure negligent or uninformed operators receive education or are subject to civil enforcement as necessary to deter future non-compliant behavior. Sanctions should also be enforced against UAS producers, vendors and exporters if they do not comply with binding domestic regulations such as those outlined in Good Practice 14.

Operator licensing, UAS registration requirements, and export control regulations, as described in Good Practices 17 and 23, could facilitate the search for perpetrators, while electronic remote identification systems might enable law enforcement agencies to analyze flight patterns, even though homemade or manipulated off-the-shelf UAS might enable terrorists to escape such requirements in certain cases. Investigations should further be conducted by investigators that are trained and familiar with UAS technology and promptly, adequately and effective as the use of UAS might be a part of a wider-scale attack strategy. The earlier the facts are established, the more time remains for states to develop an appropriate response.

Investigations should also be set up in a way that enables law enforcement agencies to identify the broader network behind a UAS attack. In many or even most cases, 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 21: Set up a process to periodically review regulations and policies and revise them where necessary.

UAS regulations and policies may prove ineffective or become outdated as technological developments run the risk of rendering existing frameworks inapplicable. For example, it may become necessary to extend regulations and policies to previously not regulated, small-size UAS, because of their enhanced capabilities, or to unmanned surface or sub-surface systems as this technology evolves. Therefore, states should set up a process to periodically review UAS regulations, and to renew or revise them where necessary.

Such review processes should be based on an ongoing exchange of the experiences of all relevant stakeholders, domestically and potentially internationally and regionally, as well as technological

developments. Regulations that are found to be ineffective, inapplicable, impractical or disproportionate should be revised or removed. If regulations become ineffective because of technological developments, states should equally revise them.

IV. Developing Tactical Countermeasures and Technical Solutions

Good Practice 22: Implement protection measures to mitigate vulnerabilities.

The vulnerability to UAS attacks is high when protection measures are lacking. Therefore, states should implement protection measures against UAS attacks by, in the first place, granting necessary authorization to the competent authorities. When implementing protection measures, states can build on their risk and vulnerability assessments as described in Good Practices 1 and 3. Places that, under these assessments, are found to be at high risk should be prioritized but states should also focus on protecting other (public) targets, including many forms of public events and mass gatherings.

When implementing protection measures, states should take into account the nature, location, purpose, and use of a site, and the safety impacts of the use of a particular counter-UAS system. A measure that is appropriate and effective in countering terrorist UAS threats in remote places might be highly hazardous in the airspace of an airport or in a densely populated urban area. There is no "one-size-fits-all" solution. Countermeasures may also consist of preventive systems, such as physical barriers (e.g., resistant glass or protective netting) and preventive security concepts and emergency protocols as described in Good Practice 19.

Throughout the various stages of countering terrorist use of UAS, states should employ a layered approach, using a range of appropriate countermeasures. States should begin by conducting a comprehensive assessment of the most effective types of technical countermeasures in specific scenarios (e.g., in proximity to airports, above mass gatherings).

Good Practice 23: Establish methods of detecting and differentiating between legitimate and terrorist use of UAS.

Analysts expect the use of UAS by the public and private sectors to increase exponentially. States should prioritize the development of technical solutions and protocols that make it possible for the relevant authorities and agencies to detect and promptly differentiate between legitimate, criminal and terrorist use of UAS in a timely manner. This is critical because an early detection of suspicious UAS will give the relevant authorities more time to develop an appropriate response.

States might therefore employ a broad range of UAS detection tools. At the moment, a combination of radar systems, radio frequency scanners, electro-optical and infrared camera systems, acoustic sensors, and human observation of airspace, possibly supported by artificial intelligence, may, depending on individual system capabilities and conditions, provide a comprehensive surveillance of the airspace enabling early UAS detection. Due to environmental factors, UAS capabilities, and deficiencies of various types of detection systems, a single-sensor approach is unlikely to provide sufficient coverage.

States should also establish methods to identify suspicious UAS. A promising technical solution is to equip UAS, comparable to other aerial systems, with individual digital IDs that would enable law enforcement and other relevant agencies to determine the origin and registered ownership of UAS. Regulations may prescribe that all UAS of a certain size have to be registered with the national authorities and broadcast their registration number, speed and position while in-flight. This approach

gives the authorities awareness of all UAS in the airspace while enabling them to focus resources on UAS that fail to comply with remote identification protocols or that are otherwise flagged due to the information that they are emitting. Nonetheless, not all detection technology that is suitable for UTM might be equally effective for security purposes. Therefore, states should assess, and where necessary enhance, the efficiency of detection technology for the purpose of detecting UAS flown with a terrorist intent.

The establishment and monitoring of no-fly zones and geo-awareness and geo-fencing in proximity to critical infrastructure and clear operational limitations as described in Good Practice 17, could equally enable an early identification of non-compliant UAS that may be operated by terrorists. Such no-fly zones could even be programmed into UAS systems before they are sold. In this regard, states should actively work together with private UAS manufacturers as advised in Good Practice 14 and provide them with the necessary data.

Good Practice 24: Develop and implement kinetic and non-kinetic countermeasures against UAS misuse.

Currently, the development of effective countermeasures against terrorist use of UAS is in its early stages and far from complete. Some of the countermeasures were designed for the military context and have not been evaluated for safe use in a civil context. The lack of developed and evaluated countermeasures exposes even otherwise well-protected places to attacks from the air. Therefore, states should develop, test, and implement effective countermeasures.

Private industry has developed a wide variety of countermeasures using a multitude of technological methods to detect and counter terrorist use of UAS. Therefore, when evaluating countermeasures, states should avoid "reinventing the wheel" and work closely with private industry to determine which solutions are best suited for their cases. This, however, should not imply that states should count on industry alone. States should also enhance, and standardize as advised in Good Practice 8, their own research and development capabilities to test and verify private industry technology, and, where necessary, enhance this technology or develop their own countermeasures. To avoid duplicating efforts, states should also share information with other states on the most effective measures, possibly through international and regional organizations as mentioned in Good Practices 9 and 12.

As a general matter, kinetic and non-kinetic countermeasures should not be regarded as substitute for prevention and mitigation strategies (e.g., engagement with the general public as described in Good Practice 15; preventive regulation and policies as described in Good Practice 17; effective emergency protocols and investigation capabilities as described in Good Practices 19 and 20). Detection technology and mitigation strategies entail a lower level of risk to the operational environment, such as airspace safety and communications networks, than countermeasures technology, and should therefore be preferably used. Nonetheless, when necessary, states should also be prepared to use effective countermeasures.

Countermeasures are generally divided into kinetic and non-kinetic countermeasures. Kinetic countermeasures include the use of net-guns; tactical projectiles; and anti-aircraft weaponry or other UAS to destroy, capture or interfere with suspicious UAS. Non-kinetic countermeasures entail spoofing; jamming of UAS' radio frequencies or global navigation satellite systems; destruction by high-energy weapons (e.g., lasers, high-energy microwaves, electromagnetic waves); and ultrasonic weapons. For the most effective protection, these measures should, as much as possible, be combined in one systems or employed as part of an integrated capability. The selection of a countermeasure for use in a particular environment should be informed by both its efficacy against the threat of terrorist use of UAS as well as the ability to mitigate any negative impacts use of such a system. Mitigation

should consider the collateral effect the countermeasure may have on people, radio-communications spectrum, infrastructure and reputation as further described in Good Practice 26.

Where this has not happened yet, states should set up speedy procedures to comprehensively evaluate the effectiveness of countermeasures and their suitability in various environments. This also includes assessing the effectiveness against "drone swarm" scenarios mentioned in Good Practice 1.

To ensure an effective and safe use of kinetic and non-kinetic countermeasures, states should sufficiently instruct and provide regular trainings in theory and practice, under realistic conditions, to all authorities that are tasked with deploying them. This includes trainings and joint exercises with local authorities as described in Good Practice 10.

Finally, states should also support efforts or oblige private industry to effectively prevent the hacking of UAS used for beneficial or recreational purposes by developing robust systems that protect against the illicit takeover of UAS.

Good Practice 25: Set up a procedure to periodically review countermeasures and adapt them to technological developments and terrorist tactics.

As this Memorandum has repeatedly noted, UAS technology is evolving rapidly. Just as states should continually update their risk assessment in light of these developments, states should also ensure that countermeasures keep up with developments and system upgrades in UAS technology.

This review process should be an ongoing process and involve reviewers, governmental or from other entities (e.g., academia or private industry), who possess the requisite technological knowledge and experience. It should identify, categorize and analyze relevant developments in UAS technology, as well as inter-connected industries that can have an impact on terrorists' potential exploitation of UAS. This process should also review observable and potential changes in the *modi operandi* of terrorists and whether established countermeasures are still robust enough to counter emerging and anticipated terrorist uses of UAS. If current countermeasures are found to be potentially ineffective, states should adapt them accordingly or develop new effective countermeasures employing the framework described in Good Practice 24.

To identify, analyze, and react to technological developments, states should collaborate with a broad array of stakeholders. These include leading technologists, scholars, practitioners in the field, and scientific institutions. Private industry can be a valuable stakeholder in assisting the review process and developing up-to-date and effective countermeasures. Comparison to and engagement with the policies of other countries can be highly effective in identifying new countermeasures and strategies.

Good Practice 26: Evaluate and take steps to mitigate the potential negative impacts of countermeasures on infrastructure and on individuals' personal property, privacy, and safety.

In all stages of countering terrorist use of UAS, states should consider and attempt to mitigate any negative consequences on infrastructure, civil society, and individuals' personal property, privacy, and safety. In particular, jamming can significantly impact information technology systems, emergency networks, communications networks, manned and unmanned aviation operations, air navigation services infrastructure, global positioning systems (GPS), and transportation networks. States should assess these possible side-effects and refrain from the use of countermeasures with disproportionate effects. To understand possible side effects, states should work together with all relevant stakeholders as identified in Section II. Some agencies and countries responsible for security at high-profile public events, as well as safety of aviation and other critical services, such as emergency response and

transportation, have already spent time and resources thinking through scenarios and should be included as stakeholders in future discussions.

CAAs, ANSPs and other relevant agencies governing aviation safety have made clear that states should be particularly cautious when countering UAS in proximity to airports or flight corridors. Measures that interfere with aircraft safety systems or ground-based air navigation services infrastructure can create safety hazards exceeding the potential threat posed by errant UAS.

It is indispensable that states evaluate potential impacts and, to the extent possible, mitigate side effects and negative operational repercussions such as, in the case of airports, closure or traffic diversion, before taking countermeasures. For example, if countermeasures interfere with particular frequencies, these frequencies should not be used for critical and emergency transmissions or these countermeasures should not be used in that environment; states should conduct risk assessments to weigh these concerns. When engaging in countermeasures that may cause unintended consequences on parts of civil society, states should ensure to coordinate their response with a responsible agency (e.g., CAAs, ANSPs and relevant agencies governing aviation safety and communication) to mitigate consequences to the greatest extent.

Conclusion

Terrorists have repeatedly exploited the capabilities of UAS to conduct attacks and other operations in armed conflicts. There is little doubt that they will attempt to utilize UAS also outside of the context of armed conflicts. To defend against this growing threat, states should create robust national legal and policy frameworks and implement effective detection and mitigation measures. The *Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems* is intended to guide governments in putting in place the necessary measures to prevent and respond to the use of UAS technology by terrorists. The Memorandum can also guide governments in developing and implementing necessary regulations and protocols to facilitate effective crisis management and investigations after UAS incidents occurred.

This GCTF Initiative and the resulting good practices should only mark the beginning of states' efforts to counter the threat posed by terrorist use of UAS. It is crucial that states continuously cooperate with each other and third-party stakeholders. With continued vigilance, states can minimize the risk posed by terrorist uses of UAS while maximizing the benefits of UAS technology to improve our economies and societies.