CTED Trends Alert | May 2019

GREATER EFFORTS NEEDED TO ADDRESS THE POTENTIAL RISKS POSED BY TERRORIST USE OF UNMANNED AIRCRAFT SYSTEMS

CTED
UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

OVERVIEW

The present *Trends Alert* was prepared by CTED in accordance with Security Council resolution 2395 (2017). This reaffirms the essential role of CTED within the United Nations to identify and assess issues, trends and developments relating to the implementation of Council resolutions 1373 (2001), 1624 (2005) and 2178 (2014) and other relevant resolutions.

CTED *Trends Alerts* are designed to increase awareness, within the Security Council Counter-Terrorism Committee, and among United Nations agencies and policymakers, of emerging trends identified through CTED's engagement with Member States on their implementation of the relevant Council resolutions. The Alerts also include relevant evidence-based research conducted by members of the CTED Global Research Network (GRN)[1] and other researchers.

INTRODUCTION

Unmanned aircraft systems (UAS) - colloquially known as "drones" - consist of an unmanned aircraft and its associated elements, including a remote pilot (typically ground-based) and the system of communication between the two.[2] Initially developed in a military context, UAS technology has advanced over the past decade, making it increasingly affordable and accessible for a growing range of uses in the public, private, and non-profit sector.

This increased accessibility has led to renewed attempts[3] by malicious actors, including organized crime[4] and terrorist groups, to exploit UAS for nefarious purposes. There have been several examples of terrorist groups' use of weaponized UAS to conduct attacks, and use of UAS in support of surveillance, reconnaissance and propaganda activities. Member States are also concerned at the potential nexus between terrorism and transnational organized crime.

TRENDS ALERT

CTED has been alerted by Member States to their increasing concern at the potential risks posed by terrorist use of UAS. This concern, combined with inconsistent national, regional and international regulatory and policy responses, suggests that **greater efforts are needed to address the potential risks posed by terrorist use of UAS**.

[1] See March 2019 GRN newsletter for further information.

[2] *Unmanned Aircraft Systems (UAS)* International Civil Aviation Organization (2011). However, if the aircraft is on a programmed path, it may not require a system of communication in real-time with the remote pilot.

[3] For older instances of terrorist attempts to use UAS or unmanned aerial vehicles (UAV) to conduct attacks, see for example Miasnikov, Eugene *Unmanned Aerial Vehicles: Technical Aspects* (2005).

[4] 5 ways Commercial Drones are Pushing the Boundaries of Crime – Cellebrite (January 2019)

The use, or potential use, of UAS by terrorists encompasses four interlinked and often overlapping areas:

1. **Attacks** — Terrorists and non-State armed groups have successfully acquired and weaponized commercial UAS with small improvised explosive devices (IEDs) to conduct lethal attacks in conflict zones.[5] The Islamic State in Iraq and the Levant (ISIL, also known as Da'esh) played a leading role in this innovation, and has disseminated guidance material to its supporters on executing attacks using UAS[6] and released propaganda depicting UAS attacks in the United States[7] and France. However, there has been limited evidence of the attempted use of UAS in terrorist attacks in non-conflict, urban environments. Research suggests that, owing to the challenges involved in building an IED, the limited payload held by most UAS, and the relative complexity in comparison to other attack methods, **the use of weaponized UAS is currently a difficult terrorist attack methodology to pursue outside conflict zones**.[8]

2. **Disruption** — Despite these challenges, an attack or attempted attack using UAS could have a significant psychological or economic impact (rather than a physical one).[9] Although this methodology has not yet been exploited by terrorist groups, a series of incidents in which UAS have disrupted operations at airports in the United Kingdom and United States are illustrative of the **potential for terrorist groups to use UAS in a disruptive, rather than destructive manner**.

3. **Surveillance** — ISIL and other terrorist or non-State armed groups have used commercially available UAS to conduct surveillance and reconnaissance in conflict zones, allowing them to gather intelligence through aerial photography and videography and to survey potential targets.[10]

4. **Propaganda** — ISIL and other terrorist or non-State armed groups operating in Iraq, Libya, Nigeria, the Philippines, Syrian Arab Republic and Yemen have also used commercially available UAS to produce high-quality propaganda videos that capture the impact of their operations, particularly those within conflict zones.[11]

AVAILABLE GUIDANCE

Security Council resolution 2370 (2017) condemns the flow of weapons, including UAS, to and between ISIL, Al-Qaida, their affiliates and associated groups, illegal armed groups and criminals. It also encourages Member States to prevent and disrupt procurement networks

[5] Harper, Alexander *Drones level the battlefield for extremists* (2018).
[6] Rossiter, Ash *Drone usage by militant groups: exploring variation in adoption* (2018).
[7] Rassler, Don *The Islamic State and Drones: Supply, Scale, and Future Threats (*2018).
[8] Stewart, Scott *When Drones Attack: The Threat Remains Limited* (2018).
[9] Greenwood, Faine *Consumer Drones are Propaganda tools, not Killing Machines* (2018)
[10] Almohammed, Assad & Speckhard, Anne *ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics* (2017).
[11] Rassler, Don *The Islamic State and Drones: Supply, Scale, and Future Threats (*2018).

for such weapons, systems and components between ISIL, Al-Qaida, and associated individuals, groups, undertakings and entities.[12]

The Security Council Counter-Terrorism Committee's *Addendum to the guiding principles on foreign terrorist fighters* (2018)[13] provides further guidance relating to the protection of critical infrastructure and vulnerable or "soft" targets and recommends approaches to preventing the illicit trafficking of small arms and light weapons (SALW).

In 2015, the International Civil Aviation Organization (ICAO) established a UAS Advisory Group to develop guidance material and provisions to be used by States to regulate UAS. In December 2016, ICAO launched its *Unmanned Aircraft Systems Toolkit,*[14] developed in cooperation with industry and international expert partners. The Toolkit collates best practices and lessons learned and can assist Member States to develop effective operational guidance on the use of UAS. ICAO's Remotely Piloted Aircraft Systems Panel and Aviation Security Panel (AVSECP) are also working to address and review the threat posed by UAS.

The International Criminal Police Organization (INTERPOL) has developed a global unmanned aerial vehicle (UAV) initiative, which considers UAVs as threats, as law enforcement tools, and as evidence. To improve its understanding of the UAS threat in its member countries, INTERPOL will hold a series of regional working groups, whose findings will be used to help develop comprehensive UAS countermeasures. Later in 2019, INTERPOL will release *Drone Response and Forensic Guidelines,* providing police and other first responders with procedures to follow where drones are part of a criminal investigation.[15]

The Global Counterterrorism Forum (GCTF) has developed a counter-UAS (C-UAS) initiative, co-chaired by Germany and the United States. The initiative will conclude its fourth and final regional workshop in the Netherlands in late-May 2019, with the workshops feeding into a non-binding Good Practices document, which will be adopted in September 2019.

CURRENT APPROACHES

Although Member States take varied approaches to countering UAS, through a combination of regulation and security frameworks, common elements of these approaches include (i) pilot's licensing; (ii) aircraft registration; (iii) insurance; and (iv) restricted zones.

In many States, licensing, registration, and insurance requirements are mandatory for commercial UAS usage, but not typically required for small UAS used for recreational purposes.[16] However, some States have recently introduced compulsory registration schemes for both recreational and commercial UAS. The imposition of flight restrictions in

[12] S/RES/2370 (2017).
[13] S/2018/1177.
[14] ICAO UAS Toolkit.
[15] INTERPOL to issue drone guidelines for first responders (2018).
[16] Jones, Therese *International Commercial Drone Regulation and Drone Delivery Services* (2017).

the proximity of critical infrastructure and heavily-populated areas is a well-established counter-measure used by many Member States.

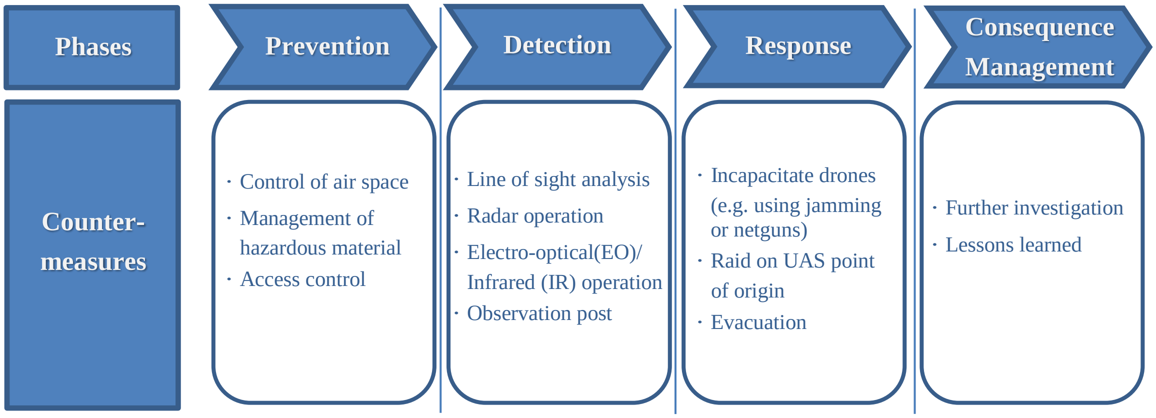
In addition to these regulatory approaches, many Member States utilize C-UAS technologies to detect and/or intercept UAS in flight. C-UAS technology has been widely used to protect airspace around airports or major events.[17] C-UAS systems use a variety of techniques to detect and intercept UAS. CTED's engagement with Member States suggests that jamming and netguns are currently among the more effective and reliable technologies:

Table 1: Counter-UAS technology[18]

Methods	Products
Detection and tracking systems	radar, radio-frequency (RF), electro-optical, infrared, acoustic, combined sensors
Interdiction	RF jamming, Global Navigation Satellite System (GNSS) jamming, spoofing, laser, nets, projectile, combined interdiction-elements
Platform types	Ground-based, hand-held, UAC-based

These technologies have also been used as part of a comprehensive response to protect major sporting or political events. CTED's engagement with Member States has identified four phases of UAS counter-measures:

Table 2: Flow chart of counter-UAS measures



Phases	Prevention	Detection	Response	Consequence Management
Counter-measures	· Control of air space · Management of hazardous material · Access control	· Line of sight analysis · Radar operation · Electro-optical(EO)/ Infrared (IR) operation · Observation post	· Incapacitate drones (e.g. using jamming or netguns) · Raid on UAS point of origin · Evacuation	· Further investigation · Lessons learned

CHALLENGES

Despite the evolution in Member States' practices and the development of guidance on the protection of soft targets and critical infrastructure (notably civil aviation), there remains

[17] Holland Michel, Arthur Counter-Drone Systems (2018).
[18] *Ibid*.

limited guidance on measures that Member States can take to prevent terrorists from purchasing, enhancing or manufacturing UAS for malicious purposes.

It is likely that UAS technology will continue to develop rapidly, and concurrently with other technological advancements (including Artificial Intelligence and the spread of 5G networks). While further technological UAS countermeasures will be required, and an improvement in the effectiveness of existing UAS counter-measures, it will be difficult for countermeasures in many Member States to keep pace with UAS technology. It is important therefore that **Member States' responses become less technology-reliant and more holistic**. Member States are encouraged to pursue a multi-stakeholder approach that includes:

- Training for those responding to incidents involving the malicious use of UAS
- Measures to strengthen community and business resilience in the event of incidents involving UAS
- Greater coordination between different parts of Government to help ensure a more joined-up response
- Greater cooperation with the private sector — for example, UAS companies can geo-fence locations (including aviation, critical infrastructure, or other sensitive locations such as prisons) within mapping software used by UAS.[19]

Regional and international initiatives — including the existing ICAO, INTERPOL and GCTF initiatives — will be central to developing more harmonized Member State responses and improving the sharing of information and lessons learned, including through technical assistance and capacity-building initiatives.

The need for a transnational response is emphasized by research indicating that ISIL's UAS programme in Iraq and the Syrian Arab Republic used a network of individuals based in at least seven different States to make purchases from 16 different countries.[20] In a first step towards greater regional harmonization, the European Union (EU) introduced the first EU-wide rules for unmanned aircraft in July 2018, identifying essential requirements for their design, production, maintenance and operation.[21]

In addressing the potential risks posed by UAS, **States should also consider the potential impact that their responses could have on internationally protected human rights (notably the right to privacy), particularly when using UAS themselves**. Engagement with civil society is encouraged to help ensure that States' UAS responses do not subject individuals to arbitrary or unlawful interference with their privacy, family, or home.

CTED will continue to engage with these initiatives and develop and share its expertise on the issue of terrorist use of UAS, in partnership with Member States; other United Nations entities; international, regional and subregional organizations; civil society; the private sector; and the research community (through the GRN).

[19] Software Update aims to keep Drones away from Airports – Bloomberg (February 2019).

[20] Rassler, Don The Islamic State and Drones: Supply, Scale, and Future Threats (2018).

[21] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018.

CTED

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

✉ cted@un.org

https://www.un.org/sc/ctc/

@UN_CTED

@UnitedNationsCTED

@un_cted