UNITED NATIONS SECURITY COUNCIL

Counter-Terrorism Committee (CTC)

CONCEPT NOTE

Agenda Item

"Addressing the Expansion of Extremist Networks through Encrypted Platforms and Emerging Technologies, amid Rising Proxy Warfare and Regional Conflicts"

I. Introduction to the Committee

The Counter-Terrorism Committee (CTC) was established by Security Council resolution 1373 (2001), adopted in the immediate aftermath of the 11 September 2001 attacks. The Committee monitors Member States' implementation of the Council's counter-terrorism resolutions and works to strengthen their capacity to fight terrorism. Its expert body, the Counter-Terrorism Committee Executive Directorate (CTED), was created by resolution 1535 (2004) to support the Committee's monitoring, facilitation, and technical-assistance functions; CTED's mandate was most recently renewed by resolution 2810 (2025) until 5 January 2029.

The Committee oversees the implementation of a body of resolutions built over two decades, including resolution 1624 (2005) on incitement, resolution 2178 (2014) on foreign terrorist fighters, resolution 2354 (2017) on countering terrorist narratives, resolution 2396 (2017) on returning and relocating fighters and border security, and resolution 2482 (2019) on the links between terrorism and transnational organized crime. This session convenes the CTC to examine how that framework holds up against a rapidly changing threat: one shaped simultaneously by digital tradecraft and by the proxy dynamics of contemporary armed conflict.

II. Background and Overview of the Agenda

Two trends are converging to reshape the terrorism landscape the Council must confront, and both have visibly accelerated over the past two to three years. The first is technological: violent extremist and terrorist organizations have systematically adopted end-to-end encrypted messaging platforms, decentralized and dark-web infrastructure, cryptocurrency, unmanned aerial systems, and generative artificial intelligence, with a reach and operational secrecy that earlier generations of terrorist groups did not have. What began, in the mid-2010s, largely as the use of encrypted apps for one-to-one operational secrecy has evolved into an integrated digital ecosystem: propaganda produced with generative AI and deepfake tools for audience-specific targeting, recruitment funnels that begin on open platforms and migrate to closed encrypted channels, and financing increasingly routed through virtual assets rather than traditional banking or hawala networks alone.

Investigations into the 2024 Crocus City Hall attack in Moscow, claimed by Islamic State Khorasan Province (ISKP), found that the entire plot was coordinated remotely across borders through encrypted channels, with no in-person contact between the group's leadership and the attackers involved. Independent analysis of ISKP's more recent operations describes a structurally reorganized digital enterprise spanning four interlocking domains: unrestricted propaganda propagation, encrypted recruitment and vetting, cryptocurrency-based financing, and remote coordination of external attacks planned in Afghanistan and executed abroad. Similar migration patterns are visible outside South and Central Asia: in Jammu and Kashmir, successive generations of encrypted applications, from BlackBerry Messenger to Threema, have surfaced in the communications of cross-border terrorist modules as each platform is compromised or banned and networks shift to the next.

The second trend is geopolitical and regional: the proliferation of proxy warfare and protracted regional conflicts is creating permissive environments in which extremist networks entrench themselves, diversify financing, and access weapons and technology. The Secretary-General has told the Council that the Sahel now accounts for roughly half of all terrorism-related deaths worldwide, with over 450 attacks and more than 1,900 fatalities recorded across West Africa between January and November 2025 alone. The Secretary-General's most recent report on West Africa and the Sahel (S/2026/537) describes a regional security landscape defined by interstate tensions, terrorist and insurgent attacks, and transnational organized crime, with armed groups such as JNIM and Islamic State-affiliated factions increasingly relying on drones, sophisticated communications, and cryptocurrency to coordinate cross-border operations. In Niger, JNIM's June 2026 attack on Niamey's international airport, and a January 2026 assault on the same airport claimed by the Islamic State Sahel Province, illustrate how drone-enabled tactics are now being turned directly against national infrastructure. Compounding this, the withdrawal of Burkina Faso, Mali and Niger from the Economic Community of West African States (ECOWAS) has widened the coordination gap that these networks exploit, while armed groups increasingly wage what regional officials describe as “economic warfare” by restricting fuel supplies and disrupting trade.

Comparable dynamics recur across other theatres examined in this agenda. In the Lake Chad Basin, the Secretary-General's most recent biannual report on the ISIL/Da'esh threat (S/2026/57) notes that Islamic State West Africa Province continues to strengthen its presence even as the parent organization loses ground elsewhere. In Sudan, Libya and the wider Horn of Africa, regional security analysis increasingly treats these theatres not as isolated conflicts but as a single interconnected war economy, linked by arms supply chains, militia financing, gold and resource extraction, logistics corridors, and external power projection — an environment in which the line between proxy-force sponsorship and terrorist financing becomes difficult to draw. Taken together, these regional patterns show that technology is not simply making existing terrorist networks marginally more efficient; it is enabling a qualitatively different model in which planning, financing, propaganda and attack execution can be distributed across multiple jurisdictions and conducted almost entirely outside the reach of traditional law-enforcement and intelligence tools.

III. International and UN Responses to Date: Normative and Institutional Framework

A layered but largely non-binding framework has developed around this agenda, combining Security Council resolutions, General Assembly strategy documents, sanctions machinery, technical guidance, and voluntary industry-led initiatives. Delegates should treat the framework below as the baseline their resolution must build upon, not duplicate.

A. Security Council Resolutions and Sanctions Architecture

The core legal architecture rests on resolution 1373 (2001) establishing the CTC; resolution 1535 (2004) establishing CTED; resolution 1624 (2005) on incitement; resolution 2178 (2014) on foreign terrorist fighters; resolution 2354 (2017) endorsing a comprehensive international framework to counter terrorist narratives; resolution 2396 (2017) on information-sharing, biometrics and returning fighters; and resolution 2482 (2019) on the nexus between terrorism and transnational organized crime. The 1267/1989/2253 sanctions regime targeting ISIL (Da'esh), Al-Qaida and associated individuals and entities was further consolidated by resolution 2734 (2024), and is supported by the Analytical Support and Sanctions Monitoring Team, whose periodic reports (most recently S/2026/44) track the financial and technological adaptation of listed entities. Resolution 2686 (2023) specifically addressed the use of new communications and information technologies for terrorist purposes. CTED's own mandate was renewed until January 2029 by resolution 2810 (2025).

B. The UN Global Counter-Terrorism Strategy

Adopted by the General Assembly in 2006 (resolution 60/288) as the single universally agreed framework for national and international counter-terrorism action, the Global Counter-Terrorism Strategy is reviewed biennially. Its eighth review, in 2023, formally expressed concern over the use of the internet and other information and communications technologies, including social media, for terrorist purposes, and encouraged cooperation between Member States, academia, the private sector and civil society to deny terrorists safe haven online while preserving an open, secure internet consistent with international human rights law. The ninth review, taking place in 2025–2026 to mark the Strategy's twentieth anniversary, is specifically examining emerging and evolving threats, including virtual assets, cybertools, unmanned aircraft systems and artificial intelligence, and offers this Committee's session a live opportunity to feed recommendations into an ongoing intergovernmental process rather than a closed one.

C. CTC Non-Binding Guiding Principles

Recognizing the absence of binding treaty law tailored to these specific technologies, the CTC has developed a growing toolkit of non-binding guiding principles. The 2022 Delhi Declaration addressed the use of new and emerging technologies for terrorist purposes broadly, including calling on the Financial Action Task Force (FATF) to strengthen counter-terrorist-financing standards for virtual assets. The 2023 Abu Dhabi Guiding Principles provided the first comprehensive guidance specifically on countering the malicious use of unmanned aircraft systems by terrorists. The 2025 Algiers Guiding Principles addressed the use of new payment technologies and fundraising methods, including virtual assets, for terrorist purposes. Collectively, these instruments give Member States a substantive, if voluntary, reference point — but they remain guidance rather than obligation, and implementation varies widely.

D. Financial and Industry-Led Frameworks

On terrorist financing specifically, FATF has issued global standards and identified red-flag indicators for the misuse of virtual assets and virtual asset service providers (VASPs), and continues to publish targeted updates assessing gaps in global implementation. On content and platform governance, the 2019 Christchurch Call to Action — launched after the livestreamed Christchurch mosque attacks — produced a nine-point action plan adopted by major technology companies, institutionalized through the independently governed Global Internet Forum to Counter Terrorism (GIFCT). GIFCT maintains a cross-platform hash-sharing database and a Content Incident Protocol for coordinated takedowns during active attacks, and has expanded from an ISIL/Al-Qaida focus to a broader remit covering violent extremist exploitation of digital platforms generally. These mechanisms are voluntary, industry-governed, and sit outside the UN system proper, which is itself a gap this Committee may wish to address.

E. UNOCT Technical Assistance and Regional Engagement

The UN Office of Counter-Terrorism's Global Counter-Terrorism Programme on Cybersecurity and New Technologies, running since 2020, provides capacity-building to Member States, regional organizations and UN entities to prevent, mitigate and respond to terrorist misuse of the internet and AI, and to build digital forensic capacity. In 2025, CTED conducted assessment visits to Austria, Cameroon, Chad, Hungary, Malta, Norway and Somalia, with a further visit to Tajikistan, and convened a gathering of States in Kenya specifically on countering sophisticated new payment and fundraising methods. At the regional level, ECOWAS, the African Union, and the (now-strained) G5 Sahel architecture provide the operational counterparts to UN-level frameworks in West Africa, while UNOWAS channels UN political engagement into the region; the withdrawal of several Sahelian States from ECOWAS illustrates how quickly regional institutional coverage can erode even as the underlying threat intensifies.

F. Assessment of the Framework

Three structural gaps stand out. First, there is no binding international instrument addressing encrypted-platform cooperation, AI-generated terrorist content, or virtual-asset-based terrorist financing specifically — only guiding principles, strategy resolutions, and industry commitments that Member States and companies may or may not adopt. Second, the framework is heavily weighted toward technical guidance and reporting, with comparatively limited attention to predictable financing for the regional and sub-regional bodies expected to implement it. Third, coordination between the UN counter-terrorism architecture, industry-led bodies such as GIFCT, and financial-standard-setters such as FATF remains largely informal, creating seams that adaptive terrorist networks can exploit. These gaps define much of the space available to this Committee's draft resolutions.

IV. Key Thematic Sub-Areas for Delegate Consideration

Delegations are encouraged to treat the following as overlapping thematic clusters rather than a rigid checklist. Regional examples are integrated into each cluster below because, as the trends above show, the technological and geopolitical dimensions of this agenda are rarely separable in practice.

A. Encrypted Communications and Digital Radicalization

The operational core of this sub-area is the shift from open-platform radicalization to closed-channel operational planning. Groups including Al-Qaida, Da'esh and their affiliates have adopted encrypted applications offering end-to-end encryption and self-deleting messages, resisting both real-time interception and after-the-fact forensic recovery, as seen in the Crocus City Hall investigation. The Jammu and Kashmir experience, where terrorist modules have cycled through successive encrypted applications as each is compromised, shows that platform-specific countermeasures have a short shelf life and that any resolution focused narrowly on naming particular applications risks obsolescence within the life of the mandate it creates.

B. Emerging and Dual-Use Technologies

Weaponized commercial drones now feature directly in regional attack planning, including the twin 2026 assaults on Niamey's international airport in Niger attributed to JNIM and Islamic State Sahel Province respectively. The CTC's 2023 Abu Dhabi Guiding Principles represent the first dedicated UN-level response to this specific threat, but implementation capacity varies sharply between Member States with advanced counter-drone systems and those, including several Sahelian States, without them. In parallel, generative AI and deepfake tools are being used to produce tailored, audience-specific propaganda, a trend flagged by the UN Counter-Terrorism Office as a defining feature of the ninth Global Counter-Terrorism Strategy review.

C. Terrorist Financing in the Digital Age

Cryptocurrency and other virtual assets increasingly supplement, rather than replace, traditional terrorist financing channels. ISKP's own crowdfunding operations, conducted through publicized virtual-asset wallets, were disrupted after law-enforcement action compromised a wallet the group had relied on — illustrating both the vulnerability and the adaptability of this financing model. The 2025 Algiers Guiding Principles and ongoing FATF standard-setting on virtual asset service providers form the current normative response, but delegates should note that FATF standards bind only States that adopt and enforce them domestically, leaving significant variation in practice, particularly in conflict-affected States with limited regulatory capacity.

D. Proxy Warfare and State-Linked Sponsorship

In Sudan, Libya and the wider Sahel, arms trafficking, militia financing, gold and resource extraction and logistics corridors increasingly connect proxy warfare to the financing and freedom of movement enjoyed by adjacent terrorist networks. This convergence complicates a sanctions and monitoring architecture built primarily around designated terrorist entities, since the same supply chains and territory may simultaneously sustain State-linked proxy forces that fall outside existing terrorism listings. Delegates should consider how reporting mechanisms such as the Analytical Support and Sanctions Monitoring Team could be adapted, without overstepping the Council's mandate on non-terrorism-designated actors, to flag these overlaps for Member State and regional-body attention.

E. Legal, Human Rights and Privacy Considerations

Every technical measure considered above carries a human rights dimension. The Global Counter-Terrorism Strategy's eighth review explicitly called for denying terrorists safe haven online while preserving an open, secure internet consistent with international human rights law, including freedom of expression. Any lawful-access, content-removal, or financial-monitoring mechanism proposed in this Committee should specify safeguards against misuse against journalists, human rights defenders, humanitarian actors and political opposition, particularly in States where counter-terrorism law has previously been applied more broadly than its stated purpose.

F. Public-Private Partnership and Industry Accountability

The Christchurch Call and GIFCT demonstrate that industry-led, voluntary frameworks can achieve meaningful cross-platform coordination — GIFCT's hash-sharing database and Content Incident Protocol are functioning examples — but they remain outside formal UN oversight and depend on continued voluntary participation by a limited set of member companies. Delegates should consider whether and how this Committee can formalize channels between GIFCT-type mechanisms, FATF, and the UN counter-terrorism architecture without displacing the operational flexibility that has made these voluntary models effective.

G. International and Regional Cooperation

CTED's 2025 assessment visits and its Kenya gathering on new payment and fundraising methods show the Directorate translating guiding principles into direct Member State engagement, but this capacity is concentrated in relatively few countries per year. In West Africa, the erosion of ECOWAS coverage following the withdrawal of Burkina Faso, Mali and Niger illustrates how quickly regional cooperation infrastructure can weaken precisely where the threat is most acute, underscoring the need for cooperation mechanisms that do not depend entirely on any single regional body's continued membership.

V. Challenges

1. Jurisdictional fragmentation: encrypted platforms and virtual-asset transactions cross borders far faster than mutual legal assistance and extradition mechanisms can respond, and self-deleting messaging can eliminate evidence before it is ever requested.
2. Private-sector variability: technology companies differ widely in their capacity, business model, and willingness to respond to lawful requests or to proactively moderate content, and GIFCT-type frameworks currently cover only a subset of relevant platforms.
3. Human rights safeguards: expanded monitoring, content-removal, or financial-tracking authority risks being applied against legitimate dissent, journalism, and humanitarian actors if not tightly bounded and independently overseen.

4. Financing gaps: regional counter-terrorism architecture, including proposed Sahel standby arrangements, faces chronic underfunding, with 2026 humanitarian appeals for the region reported to be funded only in small part.
5. Institutional coordination and erosion: the withdrawal of States from established regional bodies such as ECOWAS has created coverage gaps that ad hoc arrangements have not fully closed, even as CTED's own technical capacity to conduct country visits remains limited relative to the number of States facing this threat.
6. Rapid technological obsolescence: guidance and countermeasures built around specific platforms or tools risk being outpaced by the next generation of applications, as demonstrated by the repeated platform migration seen in cross-border terrorist networks.
7. Sanctions-proxy overlap: existing sanctions and monitoring architecture is built around designated terrorist entities and struggles to address financing and logistics networks that simultaneously serve State-linked proxy forces not subject to terrorism listings.

VI. Observations and Recommendations

Building on the framework and challenges identified above, delegates may wish to consider draft resolutions that:

- Strengthen CTED's technical capacity to assess national frameworks for AI-generated propaganda, virtual-asset financing, and drone-enabled attacks, integrating this into its existing thematic clusters and country-visit programme rather than creating a parallel mechanism.
- Establish clearer, rights-respecting channels of cooperation between Member States, GIFCT-type industry bodies, and FATF, so that voluntary technical progress in each forum is not lost to the others.
- Provide predictable, multi-year financing mechanisms for regional counter-terrorism forces and institutions, particularly in the Sahel and Lake Chad Basin, rather than relying on ad hoc or annually renegotiated support.
- Support regional coordination mechanisms capable of functioning despite the withdrawal of individual States from existing organizations such as ECOWAS.
- Build independent human rights oversight into any new monitoring, surveillance, or financial-tracking mandate arising from this agenda, drawing on CTED's existing senior human rights officer function as a model.
- Enhance information-sharing between the Analytical Support and Sanctions Monitoring Team, CTED, and regional bodies specifically on the convergence between proxy-warfare financing and terrorist financing.
- Where appropriate, convert selected non-binding guiding principles (such as the Abu Dhabi or Algiers principles) into more structured, monitorable commitments, without prematurely seeking binding treaty status that may be unachievable within the Council's current consensus.

VII. QARMA — Questions a Resolution Must Answer

Delegates should be prepared to answer the following in caucus, in working papers, and in the operative clauses of their draft resolutions:

1. How should the Council balance lawful-access requirements for encrypted platforms against the right to privacy and the security benefits of strong encryption for civil society and ordinary users?

2. What obligations, if any, should be placed on technology companies operating across jurisdictions to detect, report, and remove terrorist content without infringing on legitimate expression, and how should this interact with existing voluntary frameworks such as GIFCT?
3. How can CTED's existing monitoring mandate be adapted to assess Member States' capacity to counter AI-generated propaganda, deepfakes, and drone-enabled attacks, building on the Abu Dhabi Guiding Principles?
4. What mechanisms can distinguish and address the financing of terrorism through virtual assets separately from broader efforts to regulate digital assets, and how should FATF standards be reinforced at the UN level?
5. How should the Council address situations in which external state or non-state sponsorship of proxy forces in a conflict indirectly strengthens designated terrorist entities, without expanding sanctions authority beyond its current scope?
6. What regional cooperation frameworks can substitute for or reinforce architecture such as ECOWAS in areas where Member States have withdrawn from existing structures?
7. How can counter-terrorism financing for the Sahel and comparable regions be made more predictable given current humanitarian and peacekeeping budget constraints?
8. What safeguards should accompany expanded counter-terrorism surveillance or content-removal powers to prevent misuse against journalists, human rights defenders, and political opposition?
9. How should returning and relocating foreign terrorist fighters who were radicalized primarily online be handled differently, if at all, from those radicalized through in-person networks?
10. Should any of the existing non-binding guiding principles (Delhi, Abu Dhabi, Algiers) be strengthened into more formally monitored commitments, and if so, through what CTED or CTC mechanism?

VIII. Guidance for Preparation

In preparing for this Committee, delegates are encouraged to go beyond general knowledge of terrorism as a subject and build a country-specific research base:

- Research your country's domestic legal framework on encryption, data privacy, and lawful access, and whether it has taken a public position in FATF, GIFCT, or Global Counter-Terrorism Strategy review discussions.
- Identify whether your country has been the subject of a CTED assessment visit or is named in recent Secretary-General or Sanctions Monitoring Team reports, and understand the recommendations made.
- Determine your country's relationship to the relevant regional architecture discussed in this note — ECOWAS, the African Union, UNOWAS, or equivalent bodies relevant to Sudan, Libya, Afghanistan, or the Middle East — including whether it is a member, contributor, or subject to related peacekeeping or political missions.
- Establish your country's stance on the balance between privacy/human rights and security-driven surveillance or content-removal measures, as this will shape your negotiating position on several QARMA above.
- Prepare a position paper that addresses your country's national policy, its regional context, and at least two concrete, implementable proposals responsive to the Challenges and Recommendations sections of this note.

- Identify likely allies and opponents by bloc position — e.g., States prioritizing digital sovereignty and content regulation versus those prioritizing platform-neutral privacy protections — ahead of caucusing.

IX. Suggested Sources for Further Research

- UN Security Council Counter-Terrorism Committee and CTED official pages (un.org/securitycouncil/ctc), including factsheets and guiding principles (Delhi, Abu Dhabi, Algiers).
- UN Office of Counter-Terrorism, Global Counter-Terrorism Programme on Cybersecurity and New Technologies.
- UN Global Counter-Terrorism Strategy review resolutions and ninth-review documentation (General Assembly, 80th session).
- Reports of the Analytical Support and Sanctions Monitoring Team (1267/1989/2253 Committee).
- Secretary-General's biannual reports on the threat posed by ISIL (Da'esh), and periodic reports on West Africa and the Sahel (UNOWAS).
- Financial Action Task Force (FATF) publications on virtual assets and virtual asset service providers.
- Global Internet Forum to Counter Terrorism (GIFCT) transparency reports and Christchurch Call to Action documentation.
- Security Council Report (securitycouncilreport.org), including its Counter-Terrorism publications and West Africa/Sahel monthly forecasts.
- Regional and policy-institute analysis from organizations such as the International Peace Institute, International Crisis Group, and RAND Corporation on the Sahel, Lake Chad Basin, and Afghanistan/ISKP.
- The Concept Note's accompanying Annotated Bibliography, prepared for this Committee session.

Annotated Bibliography

Counter-Terrorism Committee (CTC) — Addressing the Expansion of Extremist Networks through Encrypted Platforms and Emerging Technologies, amid Rising Proxy Warfare and Regional Conflicts

1. Official Resources from Organizations of the UN System

Security Council Resolutions (Counter-Terrorism Committee page)

UN Security Council / Counter-Terrorism Committee

https://www.un.org/securitycouncil/ctc/content/security-council-resolutions

The CTC's official repository of the resolutions underpinning this agenda, including resolution 2810 (2025) renewing CTED's mandate to January 2029. Establishes the binding legal baseline — 1373, 1624, 2178, 2354, 2396, 2482 — that any draft resolution builds upon.

Security Council/CTC Policy Guidance

UN Security Council / Counter-Terrorism Committee

https://www.un.org/securitycouncil/ctc/content/security-councilctc-policy-guidance

Hosts the CTC's non-binding guiding principles, including S/2025/22 (the Algeria Guiding Principles on new and emerging financial technologies) and S/2023/1035 (the Abu Dhabi Guiding Principles on unmanned aircraft systems). The primary normative reference for the financing and drone sub-areas of this agenda.

Information and Communications Technologies

UN Security Council / Counter-Terrorism Committee Executive Directorate (CTED)

https://www.un.org/securitycouncil/ctc/content/information-and-communications-technologies

CTED's thematic page on terrorist exploitation of ICTs, covering encrypted communications, dark-web investigations, electronic evidence, and AI, and describing initiatives such as Tech Against Terrorism and the Global Initiative on Handling Electronic Evidence.

Cybersecurity and New Technologies Programme

UN Office of Counter-Terrorism (UNOCT)

https://www.un.org/counterterrorism/en/cct/programme-projects/cybersecurity

Describes UNOCT's Global Counter-Terrorism Programme on Cybersecurity and New Technologies (since 2020) and the eighth Global Counter-Terrorism Strategy review's concern over AI, 3D printing, virtual assets and unmanned aircraft systems being used for terrorist purposes.

Countering the Financing of Terrorism

UN Office of Counter-Terrorism (UNOCT)

https://www.un.org/counterterrorism/en/cct/countering-the-financing-of-terrorism

Sets out UNOCT's capacity-building work on terrorist financing, including the goFintel financial-intelligence software, and situates virtual-asset-based financing within the Council's broader resolution 2462 (2019) framework.

The United Nations Global Counter-Terrorism Strategy: A Living Framework for Global Action

UN Office of Counter-Terrorism (UNOCT)

https://www.un.org/counterterrorism/en/united-nations-global-counter-terrorism-strategy-living-framework-global-action

Official overview of the biennially reviewed Global Counter-Terrorism Strategy (GA resolution 60/288) and its ninth review in 2026, marking the Strategy's twentieth anniversary and examining virtual assets, AI and unmanned aircraft systems as emerging threats.

2026 Counter-Terrorism Week

UN Office of Counter-Terrorism (UNOCT)

https://www.un.org/counterterrorism/en/2026-counter-terrorism-week

Programme page for the Fourth UN Counter-Terrorism Week (26 June–2 July 2026), including the ninth Global Counter-Terrorism Strategy review plenary — the live intergovernmental process this Committee's recommendations could feed into.

UNODC and Prevention of Terrorism: Cybercrime and Terrorism

UN Office on Drugs and Crime (UNODC)

https://www.unodc.org/copak/en/Stories/SP4/countering-the-use-of-internet-for-terrorist-purposes-3-5-august-2022.html

UNODC field-level capacity-building report on countering internet-based terrorism, detailing how UNODC trains investigators on encrypted VOIP applications, cloud storage, and small-scale privacy-focused platforms exploited by terrorist actors.

United Nations Office of Counter-Terrorism (UNOCT) — AI Actions

UN Interregional Crime and Justice Research Institute (UNICRI), via ITU AI for Good

https://aiforgood.itu.int/about-us/un-ai-actions/unoct/

Documents the joint UNOCT–UNICRI research initiative on the dual-use nature of AI for counter-terrorism, including the reports "Algorithms and Terrorism" and "Countering Terrorism Online with Artificial Intelligence," directly supporting the emerging-technology sub-area.

General Assembly Adopts Text Affirming UN Global Counter-Terrorism Strategy amid Calls for International Convention, Agreed Definition to Surmount Legal Vagary

UN Meetings Coverage and Press Releases (GA/12767)

https://press.un.org/en/2026/ga12767.doc.htm

Official UN record of the General Assembly's adoption of the ninth GCTS review resolution (A/80/L.82) by a recorded vote of 140-3-1, with Member State interventions on AI-enabled propaganda, virtual-asset financing and unmanned aircraft systems.

Terrorists' Use of Emerging Technologies Poses Evolving Threat to International Peace, Stability, Acting UN Counter-Terrorism Chief Warns Security Council

UN Meetings Coverage and Press Releases (SC/16288)

https://press.un.org/en/2026/sc16288.doc.htm

Official record of the Security Council briefing presenting the Secretary-General's twenty-second report on the ISIL (Da'esh) threat (S/2026/57), documenting the group's continued expansion in the Lake Chad Basin and adaptive use of technology.

Renewed Diplomacy Beginning to Yield Results in West Africa, Sahel Despite Growing Terrorist Threat, Top Official for Region Tells Security Council

UN Meetings Coverage and Press Releases (SC/16413)

https://press.un.org/en/2026/sc16413.doc.htm

Official record of the UNOWAS briefing on the Secretary-General's report on West Africa and the Sahel (S/2026/537), documenting armed groups' growing use of drones, encrypted communications and cryptocurrency, and Member State reactions.

2. Official Statements/Documents by UN Member States and Observer States

A. Permanent Members of the Security Council

Remarks at the Security Council's Open Debate on Artificial Intelligence and International Peace and Security

United States Mission to the United Nations

https://usun.usmission.gov/remarks-at-the-security-councils-open-debate-on-artificial-intelligence-and-international-peace-and-security/

The official US national statement at the Security Council's high-level open debate on AI, setting out its position on frontier AI development and national-security risk — relevant to QARMA on global AI-governance frameworks for counter-terrorism.

We remain concerned by the deteriorating security and humanitarian situation across West Africa and the Sahel

UK Government (GOV.UK) — statement at the UN Security Council

https://www.gov.uk/government/speeches/we-remain-concerned-by-the-deteriorating-security-and-humanitarian-situation-across-west-africa-and-the-sahel-uk-statement-at-the-un-security-council

Official UK statement citing JNIM's fuel blockade in Mali as evidence of growing terrorist sophistication, and welcoming ECOWAS–Alliance of Sahel States cooperation — a useful national-position reference for the regional cooperation sub-area.

The fight against ISIS, Al-Qaeda, and their affiliates must remain a collective priority

France ONU — Permanent Mission of France to the United Nations

https://onu.delegfrance.org/the-fight-against-isis-al-qaeda-and-their-affiliates-must-remain-a-collective

France's national statement welcoming the ninth GCTS review, reaffirming its commitment to the 1267 sanctions regime and the fight against terrorist misuse of new technologies, and referencing the Christchurch Call, which France co-founded.

Statement by Ambassador Fu Cong at the General Assembly Debate on the Ninth Review of the United Nations Global Counter-Terrorism Strategy

Permanent Mission of the People's Republic of China to the UN

https://un.china-mission.gov.cn/eng/hyyfy/202607/t20260707_11976483.htm

China's official 2026 statement calling for accelerated application of emerging technologies to strengthen counter-terrorism and for greater funding, technology and intelligence support to developing countries facing higher terrorism risk.

Statement by the Delegation of the Russian Federation, Sixth Committee, Agenda Item: Measures to Eliminate International Terrorism

Permanent Mission of the Russian Federation to the United Nations

https://www.un.org/en/ga/sixth/78/pdfs/statements/int_terrorism/02mtg_russia_e.pdf

Russia's official statement following the eighth GCTS review, expressing support for the Strategy's four pillars and highlighting Russia's role as a donor to UNOCT capacity-building projects for developing countries.

B. Other Current Security Council Members (2026)

Pakistan Assumes Chair of SCO-RATS (2025-26)

Ministry of Foreign Affairs, Government of Pakistan

https://mofa.gov.pk/press-releases/pakistan-assumes-chair-of-sco-rats-2025-26

Official Pakistani statement on assuming the chair of the Shanghai Cooperation Organization's Regional Anti-Terrorist Structure, committing to host events on cyber counter-terrorism, information operations and terrorist financing — notable given Pakistan also chairs the CTC for 2025–26.

Counterterrorism and Extremism

Ministry of Foreign Affairs, Kingdom of Bahrain

https://www.mofa.gov.bh/en/combating-terrorism-and-extremism

Bahrain's official policy statement on its counter-terrorism-financing framework, FATF alignment, and commitment to the UN Global Counter-Terrorism Strategy, relevant given Bahrain's current non-permanent Security Council seat (2026–2027).

Consejo de Seguridad de la ONU

Ministerio de Relaciones Exteriores de Colombia (Cancilleria)

https://www.cancilleria.gov.co/consejo-seguridad-onu

Colombia's official page on its 2026–2027 Security Council term, highlighting its extensive experience in counter-terrorism, disarmament, demobilization and reintegration as a contribution it intends to offer the Council.

C. Additional Named Delegations (Per Committee Matrix)

Review of the United Nations Global Counter-Terrorism Strategy — Statement

Permanent Mission of Argentina to the United Nations

https://enaun.cancilleria.gob.ar/en/node/6726

Argentina's official statement detailing its terrorist-financing legislation, asset-freezing mechanisms recognized by FATF, and support for international human-rights safeguards in counter-terrorism — relevant given Argentina's vote against the ninth GCTS review resolution in 2026 to protest insufficient ambition.

Brazil Statement — Measures to Eliminate International Terrorism, Sixth Committee

Permanent Mission of Brazil to the United Nations

https://www.un.org/en/ga/sixth/74/pdfs/statements/int_terrorism/brazil.pdf

Brazil's official statement describing its domestic sanctions-implementation legislation aligning with FATF standards, and its proposal for a high-level UN conference to help finalize a comprehensive convention on international terrorism.

With Terrorism at 'Tipping Point' in Africa, Security Council Speakers Call for Development-Driven Solutions

UN Meetings Coverage and Press Releases (SC/15971), featuring Egypt's statement on behalf of the Arab Group

https://press.un.org/en/2025/sc15971.doc.htm

Official UN record of Egypt's statement on behalf of the Arab Group, warning against growing cooperation between terrorist and transnational organized-crime networks in Africa and calling for technology transfer to strengthen border control and information exchange.

General Assembly Adopts Resolution Urging Unity to Tackle New, Emerging Threats, as Speakers Assess Progress in Advancing Global Counter-Terrorism Strategy

UN Meetings Coverage and Press Releases (GA/12511), featuring Indonesia's national statement

https://press.un.org/en/2023/ga12511.doc.htm

Official UN record of Indonesia's statement highlighting its national action plan on preventing violent extremism and the ASEAN Plan of Action to Prevent and Counter Radicalization and Violent Extremism as its regional implementing framework.

General Assembly Adopts Text Affirming UN Global Counter-Terrorism Strategy amid Calls for International Convention, Agreed Definition to Surmount Legal Vagary

UN Meetings Coverage and Press Releases (GA/12767), featuring Morocco's statement as GCTS ninth-review co-facilitator

https://press.un.org/en/2026/ga12767.doc.htm

Official UN record of Morocco's statement as ninth-review co-facilitator, describing counter-terrorism as a national, continental and international priority for Morocco and flagging non-State actors' military-grade drone use in at least nine African countries.

Nigeria Seeks Crack Down on Illicit Financial Flows

Voice of Nigeria (Federal Government of Nigeria official broadcaster)

https://von.gov.ng/nigeria-seeks-crack-down-on-illicit-financial-flows/

Official Nigerian government media report quoting Nigeria's Foreign Minister at the AU Peace and Security Council on illicit financial flows enabling terrorist groups to recruit youth and deploy drones — directly linking financing and technology sub-areas from an affected State's perspective.

General Assembly Adopts Resolution Urging Unity to Tackle New, Emerging Threats, as Speakers Assess Progress in Advancing Global Counter-Terrorism Strategy

UN Meetings Coverage and Press Releases (GA/12511), featuring Qatar's national statement

https://press.un.org/en/2023/ga12511.doc.htm

Official UN record noting Qatar's 2022 national counter-terrorism strategy and its status as UNOCT's largest donor Member State, with an annual $15 million contribution renewed through 2026, including funding for technology-related capacity-building.

Saudi Arabia — Measures to Eliminate International Terrorism, Sixth Committee (80th session)

Permanent Mission of the Kingdom of Saudi Arabia to the United Nations

https://www.un.org/en/ga/sixth/80/int_terrorism/saudi_arabia_e.pdf

Saudi Arabia's 2025 official statement, describing its chairmanship of the Counter-ISIL Finance Group and its hosting of an international roundtable specifically on "the impact of new technologies on countering the financing of terrorism" in Riyadh in April 2025.

Statement by Turkiye at the 78th Session of the Sixth Committee, Agenda Item 109

Permanent Mission of the Republic of Turkiye to the United Nations

https://www.un.org/en/ga/sixth/78/pdfs/statements/int_terrorism/03mtg_turkey.pdf

Turkiye's official national statement on measures to eliminate international terrorism, addressing terrorism as a grave violation of human rights and outlining its extensive first-hand counter-terrorism experience.

Statements

Permanent Observer Mission of the Holy See to the United Nations

https://holyseemission.org/contents/statements/

Repository of the Holy See's statements as a UN Observer State, including its intervention at the General Assembly's interactive dialogue with the Independent International Scientific Panel on AI, reflecting an Observer State perspective on emerging-technology governance.

UNSC Briefing on Global counter-terrorism approach – principles and the way forward

Permanent Mission of India to the United Nations, New York

https://pminewyork.gov.in/IndiaatUNSC?id=NDg4OA

Statement by India's External Affairs Minister proposing an eight-point action plan on counter-terrorism during India's Council term, reflecting one Member State's formal national position on Committee priorities.

Statement on terrorist use of ICT and emerging technologies

Permanent Mission of India to the United Nations, New York

https://audit.pminewyork.gov.in/IndiaatUNGA?id=NDQ4OA

India's official statement flagging terrorist use of social media, new payment methods, encrypted messaging, cryptocurrencies and drones as an emerging threat most Member States lack adequate capacity to address, and calling for strengthened FATF standards.

3. Official Statements/Documents by UN Regional and Political Groups

A. The Five UN Regional Groups

Summaries of Meetings — Eightieth Session, Sixth Committee (Legal)

UN General Assembly, featuring Cameroon's statement on behalf of the African Group

https://www.un.org/en/ga/sixth/80/summaries.shtml

Official 2025–26 record of the African Group's collective statement (delivered by Cameroon) on measures to eliminate international terrorism, alongside statements by the Arab Group, CELAC/GRULAC, ASEAN and the Non-Aligned Movement in the same session.

Summaries of Meetings — Eightieth Session, Sixth Committee (Legal)

UN General Assembly, featuring Colombia's statement on behalf of CELAC/GRULAC

https://www.un.org/en/ga/sixth/80/summaries.shtml

Official 2025–26 record of the Community of Latin American and Caribbean States' (CELAC, the political counterpart to the UN's GRULAC regional group) collective statement, delivered by Colombia, on counter-terrorism measures.

B. European Union

EU Statement — 9th Review of the UN Global Counter-Terrorism Strategy: Briefing to Member States

European Union External Action Service (EEAS)

https://eeas.europa.eu/delegations/un-new-york/eu-statement-9th-review-un-global-counter-terrorism-strategy-briefing-member-states_en

The European Union's consolidated statement, delivered on behalf of the EU and aligned candidate and partner countries, affirming the Global Counter-Terrorism Strategy as the cornerstone of multilateral cooperation amid fast-evolving, technology-enabled threats.

C. Association of Southeast Asian Nations (ASEAN)

Summaries of Meetings — Eightieth Session, Sixth Committee (Legal)

UN General Assembly, featuring the Philippines' and Singapore's statements on behalf of ASEAN

https://www.un.org/en/ga/sixth/80/summaries.shtml

Official 2025–26 record of ASEAN's collective statements on counter-terrorism, delivered on rotation by member States; ASEAN's substantive contribution in this field is its Plan of Action to Prevent and Counter the Rise of Radicalization and Violent Extremism (2018–2025) and the Bali Work Plan, referenced by Indonesia's national statement in Section 2.

D. African Union

Communique of the 1237th Meeting of the Peace and Security Council (23 October 2024) on Combating Terrorism in the Continent

African Union Peace and Security Council

https://www.peaceau.org/en/article/communique-of-the-1237th-meeting-of-the-peace-and-security-council-held-on-23-october-2024-on-consideration-of-the-au-commission-report-on-combating-terrorism-in-the-continent

The AU's principal recent communique on terrorism, explicitly condemning the increasing use of new technologies by terrorist groups and directing AU institutions to build resilient counter-terrorism institutions across the continent.

Remarks by H.E. Ambassador Bankole Adeoye at the UN Security Council Open Debate on African-Led and Development-Focused Counter-Terrorism

African Union Peace and Security Department

https://www.peaceau.org/en/article/united-nations-security-council-open-debate-remarks-by-h-e-ambassador-bankole-adeoye-commissioner-political-affairs-peace-and-security-on-african-led-and-development-focused-counter-terrorism-strengthening-african-leadership-and-implementation-of-counte

The AU Commissioner's official remarks describing AU initiatives on new technologies and terrorist financing methods, the Nouakchott and Djibouti Processes, and the Continental Strategic Plan of Action — the clearest statement of Africa's regional institutional response.

ECOWAS Counter-Terrorism Strategy

Economic Community of West African States (ECOWAS)

https://edup.ecowas.int/allevents/categories/key-resources/ecowas-counter-terrorism-strategy/

ECOWAS's own regional counter-terrorism strategy document, calling for national legislation, coordinating mechanisms and intelligence-sharing across the bloc — the operative sub-regional counterpart to the AU-level frameworks above, directly relevant to the Sahel dynamics discussed throughout the concept note.

4. Official Statements/Documents by Other International Intergovernmental Organizations

Virtual Assets

Financial Action Task Force (FATF)

https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html

FATF's official standards and red-flag indicators for virtual assets and virtual asset service providers, the principal global reference underpinning this agenda's terrorist-financing sub-area and the source most frequently cited by Member States on this issue.

Project CT-Tech

INTERPOL

https://www.interpol.int/en/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech

INTERPOL's official page on its joint initiative with UNOCT to build member countries' capacity against terrorist exploitation of new and emerging technologies, including facial recognition, OSINT, and dark-web/virtual-asset investigation.

Resolution on Artificial Intelligence and the Fight Against Terrorism

OSCE Parliamentary Assembly (31st Annual Session, Bucharest, 2024)

https://www.oscepa.org/en/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/resolutions-and-publications/5040-resolution-on-artificial-intelligence-and-the-fight-against-terrorism-adopted-at-the-31st-annual-session-bucharest-29-june-to-3-july-2024/file

A formally adopted parliamentary resolution urging participating States to regulate AI to prevent terrorist misuse while protecting human rights — a rare example of a binding-on-its-members regional legislative text addressing this agenda's AI sub-area directly.

Countering the Use of the Internet for Terrorist Purposes

OSCE Transnational Threats Department

https://tntd.osce.org/secretariat/107810

The OSCE's official statement of its programme on terrorist use of the internet and emerging technologies, explicitly framing its work as building on the UN Global Counter-Terrorism Strategy while safeguarding freedom of expression and privacy.

5. Non-Official Resources

A. Think Tank and Policy Institute Reports

CTED's Mandate Renewal: A Chance to Assess the Future of Security Council Counterterrorism Efforts

International Peace Institute, Global Observatory (November 2025)

https://theglobalobservatory.org/2025/11/cteds-mandate-renewal-a-chance-to-assess-the-future-of-security-council-counterterrorism-efforts/

Analyzes CTED's periodic mandate renewal process and its evolving relationships with GCTF, ICAO, the Biometrics Institute and FATF, offering useful background on the institutional politics behind the normative framework in Section III of the concept note.

The UN Security Council in the AI Era

Stimson Center (2026)

https://www.stimson.org/2026/the-un-security-council-in-the-ai-era/

Traces the Council's growing engagement with AI and security since 2024, including the December 2025 joint statement by four elected members, and assesses what the Council can and cannot yet do to govern AI-related threats, including terrorism.

How ECOWAS Can Make Its New Counter-Terrorism Force Effective

Institute for Security Studies (ISS Africa, March 2026)

https://issafrica.org/iss-today/how-ecowas-can-make-its-new-counter-terrorism-force-effective

Assesses the financing and credibility challenges facing ECOWAS's newly endorsed counter-terrorism brigade, directly informing the concept note's discussion of regional financing gaps and institutional erosion.

Counter-Terrorism in Africa: Open Debate

Security Council Report, What's In Blue (January 2025)

https://www.securitycouncilreport.org/whatsinblue/2025/01/counter-terrorism-in-africa-open-debate.php

Independent analysis previewing a Security Council open debate on African-led counter-terrorism, summarizing AU initiatives and the political dynamics among Council members on sustainable financing for African counter-terrorism efforts.

Cyber Threats and the Security Council

Security Council Report, Research Report (2026)

https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Cyber_report_2026_v10.pdf

A detailed independent research report tracking the Council's evolving engagement with cyber and technology threats, including their intersection with counter-terrorism, sanctions and peace operations mandates.

9th Global Counter-Terrorism Strategy Review Falls Short of Potential

Charity & Security Network (July 2026)

https://charityandsecurity.org/news/9th-global-counter-terrorism-strategy-review-falls-short-of-potential/

Civil-society analysis of the ninth GCTS review — the first in the Strategy's 20-year history not adopted by consensus — explaining the human-rights and civic-space concerns that led the CSO Coalition to call the outcome a missed opportunity.

B. Academic and Scholarly Sources

Unveiling the Shadows: Exploring the Roles of the Dark Web and Encrypted Messaging Apps in Facilitating Online Terrorist Networks

Ogele, E.P., Journal of Strategic and Global Studies, Vol. 8, No. 2 (2025)

https://scholarhub.ui.ac.id/jsgs/vol8/iss2/3/

A peer-reviewed study examining how the dark web and encrypted messaging applications enable terrorist communication, recruitment and financing, providing an academic framework for the encrypted-communications sub-area of this agenda.

Exploring the Role of Encryption and the Dark Web in Cyber Terrorism: Legal Challenges and Countermeasures in India

Cogent Social Sciences, Vol. 11, No. 1 (2025)

https://www.tandfonline.com/doi/full/10.1080/23311886.2025.2479654

A peer-reviewed legal analysis of how encryption and the dark web are exploited for terrorist purposes and the regulatory countermeasures available, offering a comparative legal perspective relevant to the QARMA on lawful-access frameworks.

C. News and Regional Media Analysis

Islamic State-Khorasan Province's Virtual Planning

Lawfare (May 2024)

https://www.lawfaremedia.org/article/islamic-state-khorasan-province-s-virtual-planning

Analyzes how ISKP recruited and guided the Crocus City Hall attackers via the Telegram messaging app, and situates this within the group's broader pattern of virtual planning and its operational limits — a key case study for the encrypted-platforms sub-area.

Nigeria: Terrorists Deploying Drones, Crypto to Deepen Attacks in Nigeria — UN

allAfrica (July 2026)

https://allafrica.com/stories/202607200020.html

Pan-African outlet reporting on the UNOWAS briefing to the Security Council, with additional regional detail on ECOWAS's standby-force funding constraints not covered in the UN's own press release.

'A terrorist is a terrorist': India urges global unity against terrorism

Business Standard (July 2026)

https://www.business-standard.com/external-affairs-defence-security/news/a-terrorist-is-a-terrorist-india-urges-global-unity-against-terrorism-126070200198_1.html

Indian outlet coverage of India's statement during the ninth Global Counter-Terrorism Strategy review, including its criticism that the review failed to reach agreement on denying terrorists access to emerging technologies.

Terrorists Misusing Tech, Ethos of Open Societies: Jaishankar

Deccan Herald (2022)

https://www.deccanherald.com/amp/national/terrorists-misusing-tech-ethos-of-open-societies-jaishankar-1157668.html

Regional Indian coverage of the special CTC meeting in New Delhi that produced the 2022 Delhi Declaration, capturing the national context and voluntary financial pledge behind that guiding-principles instrument.

Terrorists Increasingly Using Drones, Cryptocurrencies in Nigeria, Sahel to Boost Operational Capabilities — UN Warns

PRNigeria (July 2026)

https://prnigeria.com/2026/07/20/terrorists-increasingly-using/

Nigerian outlet reporting on the UNOWAS Security Council briefing with local detail on displacement figures and ECOWAS standby-force funding constraints, offering a West African vantage point on the regional conflict sub-area.