United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

Information and Communication Technologies (ICT) and Related New and Emerging Technologies

A. Introduction

1. **Information and communication technologies (ICT)** – to include the Internet, social media platforms and related online spaces such as video games and virtual reality platforms – and related new and emerging technologies – including platforms and systems supported by artificial intelligence (AI) and other cyber-based tools – are mostly used for beneficial ends such as social communications, digital commerce, and informational purposes by the general population. Unfortunately, such technologies are also increasingly exploited by terrorist groups, such as the Islamic State in Iraq and the Levant (ISIL)/Da'esh, Al-Qaida, their affiliated groups and supporters, and other terrorist and violent extremist actors.

2. These groups and supporters are known to **exploit ICT and other emerging technologies to engage in a wide range of activities for terrorist purposes**, including incitement to terrorism, recruitment, training, planning, networking, securing logistical support, acquiring weapons and their components, fundraising, and conducting terrorist operations. Consequently, there is a pressing need to pay a heightened degree of attention to what is both a present-day and emerging threat to ensure that Member States, the United Nations Counter-Terrorism entities, and other relevant stakeholders fully grasp the nature of the risks flowing from these advancements in technology and are aligned to take effective steps to mitigate those risks.

B. United Nations Security Council Engagement on ICT and Emerging Technologies

3. The Security Council has focused attention on countering the exploitation of ICT for terrorist purposes for over 20 years and adopted **fifteen counter-terrorism related resolutions**,[1] as well as **four policy documents**, on the matter.[2] In its resolution 2129 (2013), the Council noted the evolving nexus between terrorism and ICT, in particular the Internet, and the use of such technologies to commit and facilitate terrorist

[1] These include resolutions 1373 (2001), 1624 (2005), 1963 (2010), 2129 (2013), 2178 (2014), 2199 (2015), 2322 (2016), 2331 (2016), 2341 (2017), 2354 (2017), 2370 (2017), 2395 (2017), 2396 (2017), 2462 (2019), and 2617 (2021).

[2] These consist of the Madrid Guiding Principles (S/2015/939), the Statement by the President of the Security Council (S/PRST/2016/6), the Comprehensive International Framework to Counter Terrorist Narratives (S/2017/375), and the Addendum to the Guiding Principles on foreign terrorist fighters (2018) (S/2018/1177).

acts. In resolution 2617 (2021) pertaining to terrorism, the Council referred for the first time to "**other emerging technologies**".[3]

4. The Security Council has repeatedly called on States to ensure that any measures taken to combat terrorism **comply with all their obligations under international law, including international human rights law, international humanitarian law, and refugee law,** as applicable. This is particularly relevant to the use of new technology in terrorism prevention and law enforcement efforts for which unintended consequences and potential human rights implications are evolving in tandem with technological adaptations.

5. The Council has further stressed that the **gendered impacts of new and emerging technologies**, including ICT, in the fight against terrorism be recognized and taken into consideration in order to avoid bias and ensure gender-responsiveness. The involvement of a broad range of stakeholders (including civil society, academia, and the private sector) can help to ensure that measures and policies developed to prevent and counter terrorist and violent extremist abuse of the cyber domain are crafted in a comprehensive and holistic manner reflecting whole-of-government and whole-of-society approaches.

C. Recent Counter-Terrorism Committee Engagement on ICT

6. On 28-29 October 2022, the Counter-Terrorism Committee held a **Special Meeting on countering the use of new and emerging technologies for terrorist purposes** in Mumbai and New Delhi, India. In advance of the Special Meeting, CTED organized a series of technical meetings in September and October 2022 on issues relating to ICT, CFT, and UAS to gather a broad range of views and good practice to inform the proceedings of the Special Meeting.[4] As the primary output from the Special Meeting, the members of the Committee formally adopted the "Delhi Declaration" outcome document.

16. In the **Delhi Declaration**, the Committee noted "with concern the increased use, in a globalized society, by terrorists and their supporters of the Internet and other information and communication technologies, including social media platforms, for terrorist purposes" and acknowledged "the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes".[5] The Delhi Declaration also provides guidance to Member States and stakeholders in countering the use of new and emerging technologies, including ICT, for terrorist purposes. It notably sets forth areas of future work for the Counter-Terrorism Committee and its Executive Directorate, to include the "intention to develop,

[3] Previous resolutions had addressed financial technologies (2462 (2019)), unmanned aircraft systems (2370 (2017)), and cybersecurity (2341 (2017)).

[4] The ICT sessions were held 30 September and 3 October 2022, a summary of which can be read here.

[5] In both Security Council resolution and the Delhi Declaration, "the need to preserve global connectivity and the free and secure flow of information facilitating economic development, communication, participation and access to information" was emphasized.

with the support of CTED, set of non-binding guiding principles (NBGPs) with a view to assisting Member States to counter the threat posed by the use of new and emerging technologies for terrorist purposes, including by compiling good practices on the opportunities offered by the same set of technologies to counter the threat, consistent with international human rights and international humanitarian law."[6]

D. CTED's Mandate and Role

7. As a special political mission supporting the Security Council's Counter-Terrorism Committee (CTC), the Counter-Terrorism Committee Executive Directorate (CTED) implements the Committee's policy decisions and conducts expert CTC assessments of Member States, facilitates technical assistance, and identifies emerging issues trends and developments in relation to Security Council resolutions on counter-terrorism.

8. Within its mandate on ICT, **CTED assists Member States to develop ways to prevent and counter the use of the Internet and related technologies for terrorist purposes, prevent and counter terrorist narratives, and develop innovative technological solutions, while respecting human rights and fundamental freedoms and in compliance with their other obligations under international law.** Through this, CTED emphasizes the need for States to work together to identify durable solutions for ICT-related challenges, despite differences in opinion regarding methodology and desired end-results. CTED strongly promotes a holistic, all-of society, and comprehensive approach, including civil society organizations (CSOs) and public-private partnerships (PPPs), to address the many challenges that arise around countering violent extremism and terrorism online.

6. CTED's work on ICT currently focuses on **six main pillars**: (i) mainstreaming ICT into the assessment visits conducted on behalf of the Committee to assess Member States' implementation of the relevant Security Council resolutions; (ii) promoting industry self-regulation and public-private partnerships; (iii) strengthening international cooperation for legal access to digital content; (iv) promoting counter-messaging techniques, including online; (v) advocating for compliance with human rights and fundamental freedoms in ICT; and (vi) the identification of emerging trends, evolving threats and other developments in terrorist use of ICTs.

9. The thematic scope of CTED's mandate for ICT has expanded, with additional activities becoming part of the Council's jurisprudence. These include:

- Gathering **digital data and evidence** (including battlefield evidence).
- **Cybersecurity** in relation to the protection of critical infrastructure.
- Use of ICT to facilitate the trafficking of persons and the illicit trade of cultural property.
- Countering **terrorist narratives online** and offline.

[6] The text of the Delhi Declaration can be seen here.

- Gathering and sharing of **biometric and biographic information**.
- Countering the financing of terrorism via new **financial technologies**, products and services.

10. CTED is additionally looking at new trends and evolving threats in terrorist use ICT and other emerging technologies to include:

- Threats and risks relating to **advances in AI** and data-driven **machine learning systems** and other **cyber-based tools**, to include recent developments in generative AI and large language models, diffusion models, and deepfake video and audio capabilities.
- The role of **algorithmic amplification** in promoting harmful and violent content; Use of new payment methods such as merchandise sales and crowdfunding to raise funds for terrorist purposes.
- Use of **gaming platforms** and related online spaces, including **augmented reality and virtual reality (AR/VR)** platforms and applications, to spread terrorist and violent extremist messaging, incite violence, recruit the next generation of extremists and terrorists, and support terrorist training and activities.
- Risks associated with terrorist exploitation of **dual-use technologies** to include drones and other unmanned aircraft systems, 3-D printing, self-driving cars, and advanced robotics.

11. As part of its work on human rights and fundamental freedoms and States' compliance with obligations under international law and their domestic legal frameworks, CTED is working in areas relating to:

- The **programming and use of artificial intelligence and algorithmic systems**, particularly those used in content moderation, law enforcement and border control (i.e. CCTV/surveillance and facial recognition technology).
- **Privacy, data protection** and lawful collection, handling and sharing of data.
- **Transparency**, including through support for initiatives to increase transparency through the provision and publishing of data on basic elements of government data request-processing and wider content removal compliance.

12. The breadth of CTED's mandate has expanded via new relationships and partnerships as cited in resolutions from the past ten years. These include cooperation with outside partners such as **civil society organizations** (CSOs), religious actors, CTED's **Global Research Network** (GRN) of respected think-tank and academic experts, and **private sector** entities. CTED has engaged in a number of initiatives to strengthen **public-private partnerships**, to include launching **Tech Against Terrorism**, advising and participating in the **Global Internet Forum to Counter-Terrorism** (GIFCT), and participating in the work of the **Christchurch Call**.

E. CTC Assessments on ICT

13. The use of ICT for terrorist purposes is one of the key thematic areas of the **assessment visits to Member States** conducted by CTED on behalf of the Counter-Terrorism Committee. ICT-related issues are outlined in the technical guide to the implementation of Council resolution 1373 (2001) and other relevant resolutions (S/2017/716) and in the updated "Framework document for Counter-Terrorism Committee visits to Member States aimed at monitoring, promoting and facilitating the implementation of Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017), 2462 (2019) and 2482 and other relevant Council resolutions" (S/2020/731). ICT issues (digital evidence, protection of critical infrastructure, online incitement, online moderation, etc.) have also been included in the Overview of Implementation Assessment (OIA) and the electronic Detailed Implementation Survey (e-DIS), the recently updated survey tools of the Committee and its Executive Directorate, which are hosted in a new cloud-based assessment and analysis portal.

14. Specific issues relating to the misuse of ICT for terrorist purposes regularly discussed with Member States during assessments visits, include:

- **Strategies** including ICT and Cyber issues.
- **Legal, regulatory and policy frameworks** to counter the misuse of ICT for terrorist purposes,
- Capacity to use **special investigative techniques** to lawfully monitor the use of ICT for terrorist purposes.
- Methods of **identifying terrorist content and activities online** and operational practices to lawfully block, filter, and take down terrorism-related online content, in compliance with international human rights obligations.
- **Cooperation with the private sector and civil society** (public-private partnerships) to counter the use of ICT for terrorist purposes, including through technological solutions.
- Use of **digital evidence** to bring terrorists to justice, including access to digital evidence stored in another jurisdiction (legislation, national structure, intra- and international cooperation).
- Policies and practices for **critical infrastructure security and resilience** against malicious activities by terrorists through cyber-based means and attacks against critical cyber-related targets.
- **Human rights** aspects of Member States' counter-terrorism measures, including safeguards for freedom of expression relating to ICT and the right to privacy.

MORE INFORMATION

More info about CTC and CTED, including the CTC Chair and CTED's Executive Director, can be found here: https://www.un.org/securitycouncil/ctc/content/about-us-0.

Information on the 2022 CTC Special Meeting on countering the use of new and emerging technologies for terrorist purposes can be found here:

https://www.un.org/securitycouncil/ctc/content/countering-use-new-and-emerging-technologies-terrorist-purposes

A list of FAQs is available here: https://www.un.org/securitycouncil/ctc/content/frequently-asked-questions-faqs.

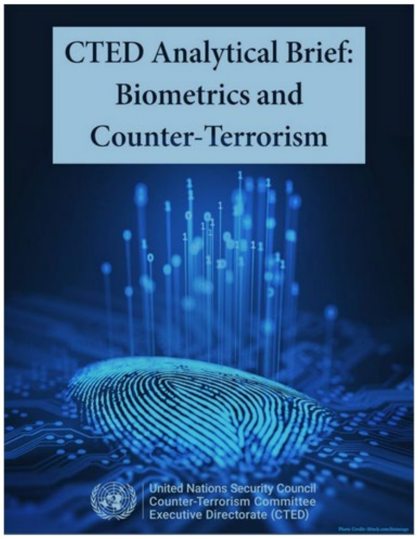
F. Recent CTED Publications on ICT-Related Issues

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

THE STATE OF INTERNATIONAL COOPERATION FOR LAWFUL ACCESS TO DIGITAL EVIDENCE:

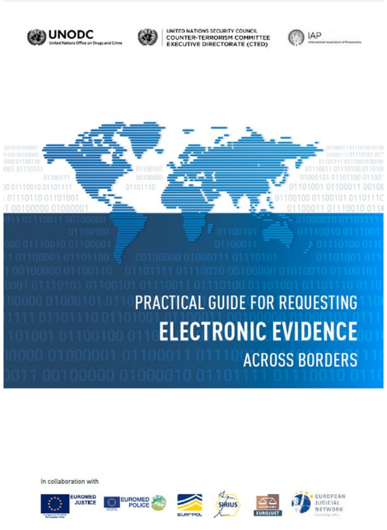
RESEARCH PERSPECTIVES

CTED TRENDS REPORT
JANUARY 2022



CTED Analytical Brief:
Biometrics and
Counter-Terrorism

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)



UNODC
United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)
IAP

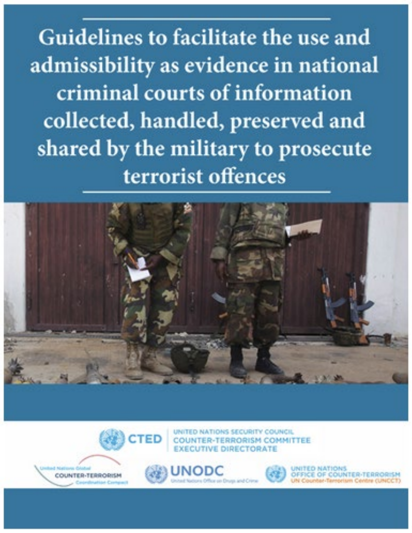
PRACTICAL GUIDE FOR REQUESTING
ELECTRONIC EVIDENCE
ACROSS BORDERS

In collaboration with

- CTED Trends Report – The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives
- CTED Analytical Brief: Biometrics and Counter-Terrorism
- Practical Guide for Requesting Electronic Evidence Across Borders

CTED Analytical Brief:
Countering terrorist
narratives online and offline

CTED
UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

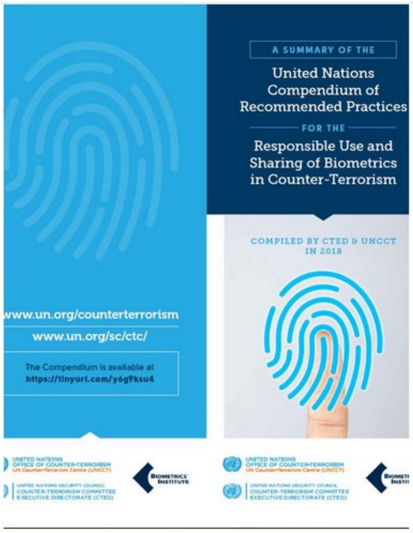


Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences

CTED
UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

UNODC

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)



www.un.org/counterterrorism
www.un.org/sc/ctc/

The Compendium is available at
https://tinyurl.com/y6g9ksu4

A SUMMARY OF THE
United Nations
Compendium of
Recommended Practices
FOR THE
Responsible Use and
Sharing of Biometrics
in Counter-Terrorism

COMPILED BY CTED & UNCCT
IN 2018

- CTED Analytical Brief – Countering Terrorist Narratives Online and Offline
- Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences
- United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism and its Summary

G. Overview of Security Council resolutions relating to ICT

Security Council resolutions	Mandate on countering the use of ICT for terrorist purposes
SCR 1373 (2001)	Calls on all Member States to find ways to intensify and accelerate the exchange of operational information concerning the use of information and communication technologies (ICT) by terrorist groups and to suppress terrorist recruitment.
SCR 1624 (2005)	Recognizes the importance of cooperative action by Member States aimed at preventing terrorists from exploiting sophisticated technology, communications, and resources to incite support for criminal acts.
SCR 1963 (2010)	Notes the increased use by terrorists of new ICT, particularly the Internet, for the purposes of recruitment, incitement, financing, planning and preparation of their activities. Also recognizes the importance of local communities, private sector, civil society and media in tackling terrorism threats.
SCR 2129 (2013)	Notes the evolving nexus between terrorism and ICT, in particular the Internet, and the use of such technologies to commit terrorist acts, and to facilitate such acts through their use to incite, recruit, fund, or plan terrorist acts, and directs CTED to identify emerging issues, trends and developments related to resolutions 1373 (2001) and 1624 (2005) and to continue to address the use of ICT in terrorist activities.
SCR 2178 (2014)	Calls on Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications, and resources, including audio and video, to radicalize and recruit to terrorism and incite support for terrorist acts, while respecting human rights and fundamental freedoms and ensuring compliance with their obligations under international law. Specifically mentions social media.
SCR 2199 (2015)	Expressing concern at the increased use, in a globalized society, by terrorists and their supporters, of new ICT, in particular the Internet, to facilitate terrorist acts.
SCR 2331 (2016)	Notes with concern the criminal misuse of ICT, particularly the Internet, to facilitate the trafficking in persons by certain terrorist groups.
SCRs 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017)	Call upon Member States to collect and preserve evidence, i.e., digital data and electronic evidence, so that investigations and prosecutions may occur to hold those responsible for terrorist attacks accountable.
SCR 2341 (2017)	Recognizes that the protection of critical infrastructure efforts entails multiple streams of efforts including cybersecurity.
SCRs 2341 (2017), 2354 (2017), 2370 (2017), 2395 (2017), 2396 (2017), and 2617 (2021)	Stress the importance of cooperation with civil society and the private sector. Acknowledge the need to develop/strengthen public-private partnerships, through voluntary cooperation, to address the exploitation of ICT by terrorists, including in developing counter-narratives and technological solutions, while respecting human rights and fundamental freedom, and ensuring compliance with domestic and international law.
SCR 2354 (2017)	Notes that terrorists craft distorted narratives to justify violence, recruit, mobilize resources, and garner support, in particular by ICT, including the Internet and social media. Sets out guidelines for implementing a "comprehensive international framework" on counter-narratives and amplifying positive and credible alternatives to audiences vulnerable to extremist messages, both online and offline.
SCR 2370 (2017)	Urges Member States to prevent terrorists from acquiring weapons, including through ICT.
SCR 2462 (2019)	Notes the use of crowdsourcing and the use of emerging payment methods, such as prepaid cards and mobile-payments or virtual-assets.
SCR 2617 (2021)	Adds reference to the use of "other emerging technologies" for terrorist purposes and encourages CTED to deepen its engagement and cooperation with the private sector. Calls on Member States to counter the use of social media, cyber trade and e-commerce as platforms that may aid the illicit trade of cultural property by terrorist groups or with terrorist intent. Also specifically references the GIFCT, Tech Against Terrorism and the Christchurch Call to Action and notes the need to preserve global connectivity, the free and secure flow of information, and access to information.