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

CTED-led technical meetings informing the
Special Meeting of the Counter-Terrorism Committee (CTC) on
"Countering the Use of New and Emerging Technologies for Terrorist Purposes"

Countering terrorist exploitation of information and communication technologies (ICT) and emerging technologies

30 September 2022 from 9.00 – 12.30 EDT / 13.00 – 16.30 UTC
3 October 2022 from 9.00 – 13.00 EDT / 13.00 – 17.00 UTC
virtual format via Microsoft Teams

Agenda

Technical Session 1 – Friday, 30 September 2022

09.00 – 09.20 Opening session

- **Opening statement**: *Dr. David Scharia, Chief of Branch, CTED*
  - Introduction of the main objectives and modalities for the technical sessions
  - The current and evolving work on ICT and emerging technologies
- **Update from the Global Internet Forum to Counter Terrorism (GIFCT) on operations and lessons-learned to date and new directions:** *Dr. Erin Saltman, Director of Programming, GIFCT*
- **Update from the Christchurch Call to Action – results from the Leadership Conference and future work:** *Mr. David Reid, Chief Advisor, Department of Prime Minister and Cabinet, Government of New Zealand*
- **Reflections on terrorism in the cyber domain and global security through digital cooperation:** *Dr. Ajai Sahni, Executive Director of the Institute for Conflict Management and Executive Director of the South Asia Terrorism Portal*

09.20 – 10.20 Session I: Threats and trends in terrorist exploitation of ICTs, including the Internet, social media platforms, and other online spaces

- **Observations on new and emerging methods used by terrorists to conduct online activities and "terrorist OPSEC" for circumventing regulatory and enforcement mechanisms**: *Ms. Maygane Janin, Policy Manager, Tech Against Terrorism*
- **Cyberproxies – Proliferation of threat actors and dual-use concerns at the convergence of emerging technologies:** *Ms. Eleonore Pauwels, Senior Fellow, Global Center on Cooperative Security*

- **Beyond the game – new developments in how video games, related spaces, and virtual reality are being misused for terrorist purposes**: *Mr. Galen Englund, Co-Founder of Extremism and Gaming Research Network (EGRN)*
- **Malicious use of Artificial Intelligence and the misuse of related technologies**: *Mr. Irakli Beridze, Head of the Centre for AI at the United Nations Interregional Crime and Justice Research Institute (UNICRI)*
- **Content curated to radicalize and recruit – the breadth, reach, and limitations of violent extremist and terrorist propaganda online:** *Ms. Sian Hutchinson, Head of UNCCT's Global Programme on Preventing and Countering Violent Extremism*
- **Tracking and mapping threats online:** *Ms. Samantha Kutner, Proud Boys Research Lead, Khalifa Ihler Institute*
- **The Use of Internet, Cyber and Digital Platforms as well as Digital Devices to Support and Commit Acts of Terrorism in Eastern Africa:** *Ms. Claudia Jematia, Cybercrime and OSINT Consultant*
- **How terrorist use of the Internet is evolving – focus on Asia:** *Dr. Mohamed El-Guindy, Digital Expert at the Egyptian Public Prosecution Office and President of the Information Systems Security Association, Egypt*

<u>Guiding Questions Session I</u>

1. What would you cite as the **top-three existing threats** relating to terrorist exploitation of online spaces and emerging technologies? Does the answer change as you look out five years and consider new and emerging technologies?
2. What under- or unmoderated spaces can be expected to remain or become even more problematic vis-à-vis terrorist propaganda, fundraising, and/or incitement?
3. Are challenges like fragmentation of online spaces and diversification of users more of a threat than new technologies?
4. How great of a threat is terrorist use of cloud archiving, self-owned websites, use of the Darkweb and other "circumvention" techniques?
5. How likely are artificial intelligence, virtual reality, the metaverse, and other emerging technologies likely to be taken up and utilized by terrorist actors?
6. How likely is it that terrorist use of these new and emerging technologies will lead to offline, "real world" harm?

10.20 – 10.45 Q&A / Statements from the Floor / Interactive discussion

10.45 – 10.55 Ten-minute break

10.55 - 11.55 <u>Session II</u>: Legal and policy responses by Member States, the technology private sector and civil society organizations

- **Terrorist designations and banned content – how the lack of a universal definition of terrorism increases challenges for moderating terrorist content online:** *Dr. Erin Saltman, Director of Programming, GIFCT*

- **The evolution of public-private cooperation in policing the online space -- A new (geo)-political order**: *Ms. Giulia Dino Giacomelli, GDG Inspire*
- **Policy and regulatory measures to combat the abuse of new and emerging technologies:** *Dr. Christina Schori Liang, Head of Terrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy (GCSP) and Member of the Global Initiative Network*
- **Establishing and enforcing user and community guidelines and measures to sanction and/or remove rule breakers:** *Mr. Albert Calamug, US Public Policy, TikTok*
- **Pro-active practices – steps taken by Meta to address emerging technologies and the evolving online terrorism threat landscape:** *Ms. Dina Hussein, Global Head, Policy Development and Expert Partnerships, Counterterrorism & Dangerous Orgs Policy, Meta*
- **The geographic scope of content restrictions:** *Ms. Julija Kalpokienė, Consultant, Content & Jurisdiction Contact Group, Internet & Jurisdiction Policy Network*
- **How United Nations sanctions tools under the 1267 regime could be better used to combat the terrorism online:** *Ms. Wuhong Shi, Expert, Al-Qaida/ISIL/Taliban Monitoring Team, United Nations Security Council 1267/1988 Sanctions Committee*
- **Legislating now for the online crimes of the future:** *Dr. Pavan Duggal, Founder & Chairman of International Commission on Cyber Security Law*

<u>Guiding Questions Session II</u>

1. What would you cite as the **top-three legal and policy-based methods** to effectively address the threats discussed in the first panel? Does the answer change as you look out five years and consider new and emerging platforms and technologies?
2. Legislation, community guidelines and platform policies are already imperfect. Are Member States and tech companies positioned to deal with anticipated threats?
3. How will content moderation policies and 'rules' have to grow, change, and adapt?
4. How can smaller tech platforms be further assisted in developing legal and policy responses and better protected from terrorist exploitation.
5. What are some of the good practices in regulating grey area content? What can be done to cultivate policy/frameworks for regulating such content?

11.55-12.25 Q&A / Statements from the Floor / Interactive discussion

12:25-12:30 Wrap-up and closing

Moderators: Session I – Ms. Jennifer Bramlette (CTED); Session II – Mr. Mattias Sundholm (CTED)

Technical Session 2 – Monday, 3 October 2022

09.00 - 09.10 Opening session

- Opening statement: *Ms. Jennifer Bramlette, ICT Coordinator, CTED*
  - Recap of discussions of 30 September
  - Day 2 layout and explanation of the main objectives and modalities for the technical sessions

09.10 – 10.10 Session III: Operational responses by Member states, the technology private sector, Civil Society, and other key stakeholders

- **Trawling for terrorist content – the success of and next steps in development and operations for the Terrorist Content Analytics Platform:** *Ms. Anne Craanen, Research Manager, Tech Against Terrorism*
- **Using AI, tech-based operational solutions and digital literacy to prevent and halt radicalization and recruitment to violent extremism and terrorism online:** *Mr. Priyank Mathur, CEO, Mythos Lab*
- **Preventing online hate in a decentralized web:** *Ms. Clara Tsao, Cofounder and Board Member, Trust and Safety Professional Association / Senior Nonresident Fellow at the Atlantic Council*
- **The future of counter-narratives in the digital space – Lessons learned and possible pathways:** *Mr. Munir Zamir, Freelance Academic and Communications Consultant*
- **Online law enforcement and security measures – developments in technology and applications for identifying and removing terrorist content:** *Mr. Hadelin Feront, Public Policy Manager, Dangerous Organizations, Meta*
- **The future functionality of crisis response protocols and the hash-sharing database**: *Mr. Tom Thorley, Director of Technology, Global Internet Forum to Counter Terrorism (GIFCT)*
- **The today and tomorrow of OSINT and online investigations:** *Ms. Akvile Giniotiene, Head of Cyber and New Technologies Unit, United Nations Counter-Terrorism Centre / United Nations Office on Counter-Terrorism (UNCCT/UNOCT)*

Guiding Questions Session III

1. What would you cite as the **top-three operational measures** used to effectively address the terrorist exploitation of ICT? Does the answer change as you look out five years and consider new and emerging platforms and technologies? Are Member States, tech companies, CSOs, and other stakeholders positioned to deal with anticipated future threats from an operational context?
2. How will counter-narratives, content takedown, de-platforming, and other operational content moderation activities have to grow, change, and adapt in light of changing

threats and technologies? What operational steps are tech platforms taking and how do they differ between large and small platforms?

3. Are content moderation solutions based on algorithms the best way forward? How are tech platforms working together to standardize or at least share information on algorithms to identify and address terrorist-related content?
4. How are algorithms and other AI/machine learning tools being adapted for different languages, different national priorities, and differing understandings of what constitutes terrorist activity and prohibited behavior and content?
5. How can we measure success in terms of countering terrorist narratives, measures to redirect users from certain spaces, and actions to de-platform/deactivate terrorist use of online spaces?
6. How should States balance their online CT activities in terms of focus for content moderation, OSINT, online investigations, and the gathering of digital evidence?

10.10 - 10:35 Q&A / Statements from the Floor / Interactive discussion

10.35-10.45 Ten-minute break

10.45 – 11.45 <u>Session IV</u>: Human rights, privacy and gender-related concerns and considerations related to countering terrorist activities online

- **Raising awareness of human rights and gender dimensions of countering violent extremism and terrorism in online spaces:** *Mr. Masood Karimipour, Chief, Terrorism Prevention Branch, UNODC*
- **Internet governance: Shaping global cyberspace to protect women and children** – *Major Vineet Kumar, Founder and Global President, CyberPeace Foundation*
- **Human rights considerations in countering terrorists' activities online:** *Ms. Ifeyinwa Nsude, Professsor, Department of Mass Communication, Ebonyi State University, Nigeria*
- **How human rights are violated under the guise of counterterrorism and the role of technology (social media, spyware, etc.) in these violations:** *Ms. Noura Aljizawi, Senior Researcher at the Citizen Lab at Munk School of Global Affairs and Public Policy, University of Toronto*
- **When content moderation becomes a breach of human rights and fundamental freedoms – the privacy implications of social media monitoring:** *Mr. Tomaso Falchetta, Global Advocacy Coordinator, Privacy International*
- **Jurisdictional challenges regarding access to electronic evidence:** *Mr. Ajith Francis, Director, Data & Jurisdiction Program, Internet & Jurisdiction Policy Network*
- **When content moderation becomes a breach of human rights and fundamental freedoms – the (un)intended consequences of content removal:** *Ms. Anna Oosterlinck, Head of United Nations Team, Article 19*
- **Fighting Internet shutdowns – an increasing and increasingly dangerous tactic:** *Mr. Peter Micek, General Counsel, Access Now*

Guiding Questions Session IV

1. It seems there has been an increase in human rights abuses by States across the globe under the banner of counter-terrorism measures and shrinking space for freedom of expression and opinion. What pragmatic and effective steps could be taken to change this trend with regard to countering terrorism online?
2. What are the long-term negative effects of de-platforming, Internet filtering, and Internet shutdowns? What efforts can be made with Member States to convince that Internet filtering and shutdowns are counter-productive?
3. How can gender dimensions relating to access to the Internet and the effects of countering terrorist exploitation of ICT be better incorporated into the measures being taken by tech platforms and States? What can be done to modify algorithms and other AI/machine learning tools to better address gender considerations?
4. How can transparency be improved/enhanced – with regard to algorithms, reporting on content moderation, etc. – to ensure greater integration between government and tech sector policies/operations and societies? How can enhanced transparency also positively affect compliance with human rights?
5. How do you view the intersection of content moderation practices, compliance with human rights, privacy and data protection, and the need to collect and share digital evidence? Does one have priority over the other, and why? What about privacy/data protection versus security? How can competing needs be balanced and met?
6. What effect are data localization laws having on tech platforms and their policies and operations? How are such laws affecting the privacy and data protection for users?

11.45 – 12.00 Q&A / Statements from the Floor / Interactive discussion

12.00-12.05 Five-minute break

12.05 – 12.55 Session V: Moderated conversation on practices worth keeping, new ways of working, and recommended ways forward

- **UNOCT capacity building and global programming for the future:** *Dr. Jehangir Khan, Director of UN Counter-Terrorism Centre (UNCCT)*
- **Building Member State capacity today to address tomorrow's threats:** *Mr. Masood Karimipour, Chief, Terrorism Prevention Branch, UNODC*
- **Coordinating the United Nation's digital technology-related efforts to address over-the-horizon concerns:** *Ms. Yu Ping Chan, Senior Programme Officer, Office of the Secretary-General's Envoy on Technology*
- **Ongoing process of the elaboration of an international convention – the new UN convention on countering the use of information and communications technologies for criminal purposes:** *Ms. Xiaohong Li, Chief of Section, UNODC*
- **Good practice and future role of UNDP in countering the exploitation of ICT for terrorist purpose:** *Ms. Nika Saeedi, Team Leader, Prevention of Violent Extremism,*

Conflict Prevention, Peacebuilding and Responsible Institutions (CPPRI), Crisis Bureau, UNDP

- **EU actions to counter violent and extremist content online:** *Ms. Yolanda Gallego-Casilda Grau, Head of Unit, European Commission, Directorate-General for Migration and Home Affairs*
- **Crafting a regional strategy to combat terrorism, including in the cyber domain – Good practice and lessons learning in preventing and countering terrorist activities online:** *Dr. Maryem Ammi, Assistant Professor, Head of Partnerships and International Cooperation, Naif Arab University for Security Sciences, Arab Interior Ministers' Council (AIMC)*
- **Reading of a statement on behalf of the African Centre for the Study and Research on Terrorism (ASCRT/CAERT)**: *Mr. Ameur Dahmani*, *Senior Officer, Cybercrime & Cyberterrorism, CAERT*

<u>Guiding Questions Session V</u>

1. What good practices should tech platforms retain and expand on? What about Member States?
2. What could or should the role of the United Nations be? What about IROs?
3. How could CSOs be positioned and supported to facilitate the work of Member States and the technical sector in countering the exploitation of ICT for terrorist purposes?
4. What technical assistance would need to be created to ensure online CT operational tactics are in step with the latest technologies and Member States, in particular, have the talent and capacity to deploy them?
5. Would having an agreed definition of terrorism – even if only between large and small platforms, or if only relating to terrorist abuse of online spaces – solve content moderation challenges? How could one be crafted and agreed?
6. If the Security Council (or other United Nations body) were to develop guiding principles or even a new resolution on terrorist use of ICTs, what should be contained therein?

12.55 – 13.00 Wrap-up and closing

Moderators: Session III – Ms. Jennifer Bramlette (CTED); Session IV – Mr. Mattias Sundholm (CTED); Session V – Dr. David Scharia (CTED)