DIGITAL CONFERENCE ON COUNTERING TERRORIST COMMUNICATIONS:

Terrorist Propaganda, Public Provocation, Recruitment and Radicalisation

PROGRAMME

31 January – 1 February 2023

Council of Europe, Strasbourg

Palais de l'Europe Room 6

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Introduction

The Council of Europe Counter-Terrorism Strategy (2018 – 2022) foresees the development of guidance for member States on programmes and other national measures to prevent the spread of terrorist communications public provocation, propaganda, recruitment, training and radicalisation leading to terrorism and to ensure that member States remain ahead of the evolving threat.

For this Digital Conference, the Council of Europe Committee on Counter-Terrorism (CDCT) took the decision to merge two Strategy items for the purposes of countering and preventing these phenomenon in both online and offline spheres, and to bridge the gap between research and practice in these complex and interrelated areas.

Background and context

Due to the ubiquity of modern internet technology, practically all terrorist actors use online platforms and technologies for recruitment, training, radicalisation, public provocation, propaganda or in order to plan, prepare and execute attacks. This phenomenon continues to evolve as new platforms and services emerge, enabling terrorist actors to find new and innovative ways of harnessing the capabilities these technologies provide.

These technologies can be used by terrorist actors in many ways, though two key trends stand out: closed channels and groups which are primarily intended to facilitate communication sharing information, as well as for coordinating and planning attacks, and public forums and message boards where terrorist actors can reach a wider audience in order to promote their terrorist ideologies, or recruit new adherents.

As these technologies facilitate decentralised communication networks, small cell terrorist groups and lone actors can communicate and exchange with relative ease. These networks and actors can then amplify ideologies and sentiments which normalise violent extremist viewpoints and may inspire or encourage others to carry out terrorist attacks.

The widespread use of encryption technologies often puts law enforcement and intelligence officials at a significant disadvantage when it comes to the interception of these communications, often requiring careful cooperation with private sector companies and other groups in order to establish effective means of sharing e-evidence and information in a manner that is compatible with privacy rights and data protection.

Consequently, the Council of Europe is working to help improve co-operation between law enforcement and the private sector to prevent terrorists abusing vital online platforms, including social media, while ensuring adequate safeguards are in place for key human rights protections such as freedom of expression.

Day One - 31 January 2023	
10:00 – 10:15	**Opening Remarks** **Ambassador Päivi Kairamo**, Ambassador for Counterterrorism Cooperation, Ministry for Foreign Affairs of Finland, Legal Service, and Chair of the Council of Europe Committee on Counter-Terrorism (CDCT)
10:15 – 11:15	**Session I: Radicalisation conducive to terrorism: Online and Offline Dimensions** **Moderator:** **Ambassador Päivi Kairamo -** Ambassador for Counter-terrorism Cooperation, Finland **Dr Sharri R. Clark –** Senior Advisor for Cyber & CVE, Bureau of Counterterrorism (CT), U.S. Department of State **Mr Umar Abubakar –** Counter Terrorism Centre, Office of the National Security Adviser, The Presidency, Nigeria, GCTF CJ-ROL WG Co-Chair **Prof. Noemie Bouhana –** Professor of Crime Science and Counter Extremism, University College London **Ms Annukka Kurki –** PVE Advisor, Save the Children (Finland)
Break	
11:30 – 12:30	**Session II: Preventing and responding to terrorism narratives and public incitement to commit terrorist attacks** **Moderator:** **Ambassador Christian Meuwly –** Ambassador Extraordinary and Plenipotentiary and Permanent Representative of Switzerland to the Council of Europe **Dr Charlie Winter** – ExTrac and Associate Fellow International Centre for Counter-Terrorism (ICCT) **CDR Salvatore Murolo -** Global Coalition against Daesh Communication Cell **Ms Charlotte Mariën –** Policy Officer, European Commission **Ms Thawab Glynn & Ms Cindy Schaefer** - Product Policy-Issue-Violence and Aggression, and Law Enforcement Outreach Manager, TikTok
Lunch	
14:30 – 15:45	**Session III: Preventing and disrupting recruitment to terrorism** **Moderator:** **Ms Ileana Visoiu -** Ministry of Justice, Romania and former Chair of the CDCT **Ambassador Roger Noble –** Ambassador for Counter-terrorism, Australia, GCTF CVE WG Co-Chair **Ms Julia Ebner –** Senior Research Fellow, Institute for Strategic Dialogue (ISD) **Ms Sian Hutchinson –** Head of Global PCVE Programme, United Nations Office of Counter-terrorism (UNOCT) **Ms Carolina Rocha da Silva –** Moonshot CVE
Break	
16:00 – 17:00	**Session IV: Preventing the proliferation of terrorist training material** **Moderator:** **Mr Nicola Piacente** – Vice-Chair of the CDCT, Chief Prosecutor, Prosecutor's Office, Genoa **Ms Elizaveta Busygina –** Digital Forensic Investigation Officer, UNITAD **Mr Jakob Guhl –** Senior Manager, Policy & Research, Institute for Strategic Dialogue (ISD) **Ms Gülden Neslihan Kesici –** Counter Terrorism Department, Turkish National Police

Day Two - 1 February 2023	
14:30 – 15:30	**Session V: Digital forensics and e-evidence when tackling terrorism content online** **Moderator:** **Mr Pedro Verdelho –** Chair, Council of Europe Committee on Cybercrime (T-CY) and Public Prosecutor, General Prosecutor's Office of Lisbon, Portugal **Mr Larry Schneider –** Deputy Chief, Counterterrorism Section, U.S. Department of Justice **Mr Manuel Eising –** Senior legal advisor, Action against Terrorism Unit, OSCE **Ms Natalie Mand –** Office of the Federal Public Prosecutor General, Germany **Mr Alberto Ferraresso –** EUROPOL Internet Referral Unit (IRU)
Break	
15:45 – 16:45	**Session VI: Reinforcing human rights and rule of law mechanisms when countering terrorist content online** **Moderator:** **Ambassador Petr Válek –** Ambassador Extraordinary and Plenipotentiary and Permanent Representative of the Czech Republic to the Council of Europe and the Focal Point on the Fight against Terrorism **Dr Nagham El-Karhili –** Programs and Partnerships Lead, Global Internet Forum to Counter Terrorism (GIFCT) **Ms Maygane Janin –** Policy manager, Tech Against Terrorism **Dr Krisztina Huszti-Orban –** Human Rights Officer, United Nations Office of Counter-terrorism (UNOCT) **Dr Katy Vaughan –** Christchurch Call Advisory Network Co-Chair, University of Swansea
16:45 – 17:00	**Closing Remarks**

Conference Overview

The Digital Conference will cover a range of terrorist activity on- and offline, focusing primarily on communication acts and efforts by terrorist groups to recruit and gain support among their targeted constituencies, as well as those aimed at providing the means and the know-how to carry out terrorist attacks.

Speakers will include public and private sector practitioners as well as experts in counter-terrorism issues. The Conference will also benefit from academic experts in order to promote cross-sectoral discourse and the exchange of good practices to address these challenges.

In planning this Conference, the Council of Europe will rely on the previous and current work developed in this area by the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), United Nations Office on Counter-Terrorism (UNOCT), the Global Internet Forum to Counter Terrorism (GIFCT), the Global Counterterrorism Forum (GCTF), and the Organization for Security and Co-operation in Europe (OSCE).

Conference Themes

Session I: Radicalisation conducive to terrorism: Online and Offline Dimensions

The first session will provide participants with an overview of the main issues and challenges relating to terrorist communications. As such, it will look at both online and offline means of engagement, as well as the emerging means by which terrorist actors seek to spread their ideology, distribute propaganda material and recruit people to their cause.

Session II: Preventing and responding to public incitement to commit terrorist attacks

This session explores the ways that different states approach the issue of persons seeking to inspire, encourage or incite others into carrying out acts of terrorism. Specifically, the session will consider legal thresholds in different jurisdictions enabling investigation and/or prosecution of persons who may be seeking to incite terrorist activities, as well as potential warning systems and rapid response mechanisms prior to terrorist attacks.

Session III: Preventing and disrupting recruitment to terrorism

This session deals with how terrorists seek to recruit and indoctrinate new members into their organisation and examine viable approaches to prevent a range of terrorist actors from expanding membership of their groups. A special emphasis will be placed on different recruitment strategies depending on various factors, such as their organisational structure and financial capacity, local or international demographics, as well as the growing trend

of targeting specific groups (e.g. children), or working in specific settings (e.g. prisons).

Session IV: Preventing the proliferation of terrorist training material

This session looks at the risks presented by material primarily intended to train or provide key operational information to would-be terrorist actors in order to enable them to carry out terrorist acts. Furthermore, the session will look at the potential risks posed by new technology, such as virtual reality or gaming platforms, and how these may be abused by terrorist actors to prepare, coordinate or plan terrorist activities.

Session V: Digital forensics and e-evidence when tackling terrorism content online

Law enforcement and technology companies perform a range of digital forensics to gather and share evidence related to online or social media content. The session will look at ways to overcome the main challenges in this field and the forensic techniques available to both private and public sector actors to facilitate the identification, collection and preservation of digital evidence for use in criminal proceedings.

Session VI: Reinforcing human rights and rule of law mechanisms when countering terrorist content online

The overarching issue of the need to observe human rights within the context of application of counter-terrorism measures, such as content takedowns and suppression of dangerous material. It will consider some of the available guidance and good practice in this field and explore potential means and measures available to states to facilitate effective cooperation with technology companies and to encourage a human-rights compliant approach to countering and suppressing online material.