SUMMARY OF THE DIGITAL CONFERENCE ON COUNTERING TERRORIST COMMUNICATIONS:

Terrorist Propaganda, Public Provocation, Recruitment and Radicalisation

31 January – 1 February 2023

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Welcoming Remarks by the Chair of the Council of Europe Counter-Terrorism Committee (CDCT)

Amb Päivi Kairamo, Ambassador for Counter-Terrorism Cooperation, Finland, and Chair of the CDCT

As Chair of the Council of Europe Committee on Counter-Terrorism (CDCT) for 2022-2023, I am honoured to present this summary from the Digital Conference on Countering Terrorist Communications.

Modern terrorists are highly reliant on media and the internet. Propaganda has long been a key part of terrorist strategies as they seek to spread their message of fear to their targeted audience, while inciting individuals to commit further acts of terrorism.

Terrorists and violent extremists have been known to use all communications available to them. This adds to the challenge of identifying and monitoring a wide range of media and sources. Indeed, one of the more notable shifts in the terrorist landscape in the recent years has been the fact that online groups and networks have become the primary means by which certain violent extremist movements engage with other, recruit new members and inspire further attacks.

Thus, building effective mechanisms to counter-terrorist communications is a vital part of our counter-terrorist strategies. International cooperation is, and will remain, an essential aspect of our work. We must have effective mechanisms to improve engagement not only between national authorities and law-enforcement, but also with counterparts at technology platforms and online service providers. We all play an essential role in preventing the proliferation of terrorist communications, as well as support efforts to gather and share essential data and information on terrorist activity online.

This Digital Conference arrived at a timely moment to have a comprehensive discussion on these topics and bridge some of the gaps in coordination between States and international organisations, the private sector and academia.

In our efforts to combat this phenomenon we must not lose sight of the need to uphold the rule of law and human rights. Promoting these values and living up to them in our policy and action - that is, in itself, a powerful counter-narrative to terrorism.

We should also remind ourselves that countering terrorist communications is not just about stopping attacks now, but also about disrupting terrorists in the long-term. The threat of terrorists using the opaque nature of the internet to foster the next wave of attacks is real. We must take coordinated action to disrupt these plans from coming to fruition.

As we look to our new Strategy for 2023-2027, the CDCT looks forward to working on these challenges together with our partners worldwide.

Executive Summary

Disclaimer: The positions presented in this event summary do not represent the official position of the Council of Europe.

The Council of Europe Committee on Counter-Terrorism (CDCT) organised a Digital Conference on "Countering Terrorist Communications: Terrorist Propaganda, Public Provocation, Recruitment and Radicalisation", at the Council of Europe premises on 31 January to 1 February 2023.

Modern terrorism is often a form of media terrorism and many terrorists are propagandists as much as they are violent criminals. The current wave of terrorists have unfortunately thrived on message crimes in a media-rich environment, committing horrendous acts of violence, broadcast widely, to coerce and intimidate Governments and citizens. Terrorists and violent extremists have abused a variety of 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.

Given these challenges, the Digital Conference focused on ways to monitor and counter activity by terrorist groups online and offline, particularly 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. Authorities, internet companies and others are in a constant struggle against terrorist content online, as terrorists multiply their propaganda across several services, migrate to unregulated and encrypted platforms, or create and host their own websites.

The Digital Conference benefited from the expertise of highly qualified experts, practitioners, and policymakers in this area, alongside representatives of regional and international organisations supporting global efforts to address these issues. Expert speakers shared state-of-the-art research into the trends and evolution of the terrorist communications landscape, while practitioners shared insights into a suite of tools and techniques available to counter and prevent terrorists and violent extremisms from spreading.

Furthermore, the Conference explored some of the key issues related to accessing and obtaining electronic evidence from private internet companies for the purposes of investigating and prosecuting suspected terrorists and violent extremists. The existing response mechanisms aiming at removing or restricting access to illegal content were presented and analysed, alongside due consideration of the importance of respecting human rights and fundamental freedoms, particularly freedom of expression. Human rights should not be seen as inhibiting these efforts, but as complementing and guiding efforts to tackle terrorist communications online and offline.

The Digital Conference also highlighted the importance of further international cooperation and public-private dialogue on these matters, supporting mutual understanding and the exchange of good practices to prevent terrorist propaganda, public provocation, recruitment and radicalisation in all its forms and manifestations.

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

The first session of the Digital Conference addressed some of the issues concerning radicalisation to terrorism and the ways in which a person can come to embrace terrorist ideologies and be driven to carry out violent actions or inspire further acts of terrorism.

Considering both the online and offline dimensions of this phenomenon, it was made suggested that these two dimensions should not be considered as entirely separate spheres. Given the widespread use of internet-connected devices, the lines between online and offline experiences are increasingly blurred, a phenomenon which can also be seen in terrorist communications.

Looking specifically at the online dimensions, terrorist and violent extremist it was observed that organisations can be seen to use a wide range of online platforms, such as messaging apps, social media, or even video games platforms, creating and distributing a vast array of content, including images, videos, audio recordings, text documents, etc. Many terrorist groups have also sought to own and operate their own websites with forums and message boards attached.

However, research suggests that radicalisation rarely occurs through fully online means. As such, offline spaces still play a significant role in terrorist radicalisation as in-person interactions with family, friends and acquaintances remains a common means of radicalisation to terrorism and violent extremism. Moreover, it was noted that while traditional forms of communication (such as written letters or paper documents) as they can be inconvenient, slower and have a smaller reach, they are also more difficult to monitor and intercept.

This first session also highlighted some of the main social and psychological aspects of radicalisation, notably with regards to the idea of a “continuum” of radicalisation. Online and offline, radicalisation can be viewed as a process which relies on multiple individual and environmental factors. At the individual level, there are certain indicators of general susceptibility to radicalisation were analysed, such as low impulse control or a criminal background. Drawing from similar research into public health, while there may be underlying susceptibility, individuals are less likely to radicalise unless certain environmental factors are also present. More research is needed to better understand what characterises such an environment in order to comprehensively prevent radicalisation to terrorism.

The session also addressed the issue of radicalisation from national perspectives, looking at the specific radicalisation environment online and offline. In particular, the speakers highlighted some of the key differences in the radicalisation strategies of several organisations, notably ISIL (Daesh), Al-Qaeda and affiliates, Al-Shabaab, and various violent far-right organisations. Some of these groups specifically target young people and children, who can be particularly vulnerable when exposed to terrorist content online.

Speakers also identified national prevention and intervention efforts to counter terrorist communications and prevent radicalisation, underlining the need for cooperation between public and private actors, civil society, as well as international and regional organisations. The role of education, particularly in terms of media literacy, was widely considered to be an important first line of defence against radicalisation.

Session II: Preventing and responding to terrorism narratives and public Incitement to commit terrorist attacks

The second session of the Conference was aimed at understanding how terrorist narratives and public incitement to commit violent attacks are spread and corresponding measures to prevent and respond to it by examining the outreach strategies and narratives of terrorist and violent extremist organisations such as ISIL(Daesh), Al Qaida and affiliates, as well as violent far-right groups.

It was recognised that practically all terrorist/violent extremist organisations, and their supporters, are engaged in strategic communication. However, some important distinctions can be made: on one hand, there is "organisational level" media production (e.g. from ISIL(Daesh), or Al Qaida), characterised by a hierarchical structure and high levels of logistics and planning. On the other hand, there is "community-based" communication (e.g. by various violent-far right networks), which is generally more nebulous and innovative, particularly when it comes to using new technologies.

Furthermore, counter-narratives were also highlighted by several speakers as an important tool to prevent and respond to terrorist communications. Strategic communications campaigns such as those run by the Communications Cell of the Global Coalition against Daesh are aimed at providing a counter to terrorist communications while also promoting social cohesion and bringing communities together. In general, speakers highlighted the challenges of adapting counter-terrorist communications strategies to the evolution of the terrorist landscape, as well as regional specificities.

Moreover, this session offered an overview of some existing tools to monitor and respond to the proliferation of terrorist content online. In particular, as online networks are exploited to inspire or encourage terrorist attacks, the role of online service providers was recognised as crucial.

Cooperation between the private and the public sector was recognised as a cornerstone of the response to terrorist communications. A major legislative shift in this area is the European Union's Terrorist Content Online Regulation (TCO Regulation) which creates obligations for hosting service providers to address the proliferation of terrorist content while also seeking to effectively balance freedom of expression online. The TCO Regulation foresees a rapid response mechanism to address imminent threats, particularly by removing terrorist content from their platforms within one hour, while also requiring certain safeguards and measures, such as preservation orders and the need to provide legal remedies for erroneously removed content. Under the Regulation, hosting service providers are also required to put in place several proactive technical or operational measures, including staff responsible for content moderation and means to identify and remove content.

Moreover, in order to identify and remove such content, online service providers can combine automated content moderation technologies, which can detect potential policy violations, with human scrutiny. Recognising that terrorists and violent extremist are able to adapt their communication strategies to bypass these moderation efforts, content moderation teams must continuously update their policies and approach in order to remain effective.

Session III: Preventing and disrupting recruitment to terrorism

The third session of the Conference was dedicated to the challenges of preventing and disrupting recruitment to terrorism and violent extremism.

The session placed particular emphasis on the issue of young people being manipulated and recruited into terrorist and violent extremist milieus, an issue that has only become more important as a result of the wide reach enabled by the internet has made it easier for terrorists and violent extremists to reach, influence and recruit young people worldwide.

Several different terrorist recruitment strategies were identified, which often differed depending on the main ideological axis of the movement (such as violent misogynist groups, ISIL(Daesh)-inspired movements, or violent far-right extremism). Furthermore, it was shown that terrorists and violent extremist groups use both sophisticated and coordinated media manipulation, often strategically avoiding content moderation efforts on mainstream platforms while also migrating to alternative sites with weaker or non-existent policies regarding violent extremist content.

A notable recent phenomenon is one where certain movements have "gamified" their online actions, applying gaming concepts to non-gaming contexts. This includes, for example, efforts to call on supporters and would-be attackers to gain new "high scores" in real-world violence. These elements can function to boost engagement while also inspiring further copycat attacks. While it was emphasised that video games and video game culture are not intrinsically problematic, there is still a need to examine the scope and prevalence of extremist misuse of gaming spaces for the purpose of radicalization to terrorism.

These issues are compounded by the notably fluid boundaries between the online world and reality for young people, as well as the often performative nature of online engagement. As such, it can be hard to differentiate between deeply held beliefs and virtual role-playing, or to draw a clear line between trolling and actual extremist ideologies.

During this session, international initiatives aimed at preventing terrorist recruitment were presented. Resolving these issues requires counter-terrorist specialists, policymakers and researchers to work closely with online platforms, including social media and gaming services, to curb the ability of extremists to exploit these spaces. Specific intervention models such as the Redirect Method were highlighted as potentially effective in this regard, which is an intervention model aimed at redirecting vulnerable users towards safer, non-extremist content such as mental health services, crisis counselling or other sites with compelling and credible alternative messages.

In this vein, the Conference also highlighted the contribution of the Countering Violent Extremism (CVE) Working group of the Global Counter-terrorism Forum (GCTF), which has worked on these issues for many years, including key texts such as the Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online.

However, more durable solutions to prevent recruitment may require early-intervention systems and enhanced primary prevention. There may need to be wider efforts to improve digital literacy, training and education which can improve and strengthen communities' resilience to terrorism.

Session IV: Preventing the proliferation of terrorist training material

During the fourth session, the discussion centred around the means and methods terrorists and violent extremists spread instructional material and guidance to potential recruits, current members, and would-be lone actors.

Looking at some of the typologies of certain kinds of training material, it was observed that this may differ depending on the level of organisation a particular terrorist or violent extremist group has. Drawing on the GIFCT Hash-Sharing Data Taxonomy Report, terrorist training material can be distinguished from other types of material, such as *ideological material* designed to further a particular movement's worldview, *inspirational material* to reinforce or further radicalise supporters.

While many terrorist groups produce outputs combining some or all of these elements, speakers focused on the latter category of instructional content as this can provide readers with specific knowledge on how to prepare and conduct terrorist attacks. Training material may thus provide dangerous step-by-step guides on issues such as how to perform reconnaissance on potential targets, how to prepare or use various types of explosives and weapons, or how to ensure operational secrecy.

In terms of content moderation by internet platforms of this type of content, it was noted that training material can pose a particular challenge and should be analysed and contextualised properly. This is due to the high volume of instructional content online which may be useful to terrorists and violent extremists, but is not explicitly terrorist in nature (such as general weapons handling instructions or various types of political literature).

Furthermore, a significant amount of training material provided guidance on non-violent aspects of terrorism, including, for example, guidance on how to reach out to potential supporters and recruits online, how to acquire and distribute financial resources, and how to forge or fake documents and papers for the purposes of travel to or from ISIL(Daesh)-held territories.

The session benefitted from the expertise of the Investigative Team to Promote Accountability for Crimes Committed by (ISIL)Daesh (UNITAD), which has a mandate to support domestic authorities to hold ISIL(Da'esh) members accountable for its crimes by collecting, preserving, storing evidence according to international standards. Notoriously, ISIL(Daesh) used the internet to distribute a wide variety of training and instructional materials to followers worldwide, and it has been observed that ISIL(Daesh) (as well as certain Al-Qaida-affiliated groups) have long seen the internet as a virtual training ground or an extension of the battlefield itself. These groups have produced guides on topics such as electronic warfare, interrogations, kidnapping, tunnelling, improvised explosive devices, as well as how to acquire material to construct improvised chemical, biological, nuclear or radiological weapons (CBRN).

This material has proven hard to remove completely from the internet, which presents a significant ongoing risk. In addition, it was underlined that while terrorist and violent extremist groups have tended to develop training material tailored to their specific ideology and objectives, there has also been a degree of cross-pollination as various terrorist and violent extremist actors have used such material to incorporate ideas and practices from other movements into their *modus operandi*.

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

Given that terrorist and violent extremist movements are increasingly reliant on a wide ecosystem of online platforms, this session was dedicated to understanding the key challenges and potential uses relevant to the identification, collection, and preservation of electronic evidence.

Online terrorist content, and its associated metadata, is increasingly used for the purposes of criminal investigations. Law enforcement practitioners highlighted the importance of electronic evidence in both national and international terrorist cases, emphasising the need to build and strengthen technical capacities to collect, preserve and analyse electronic data in order to successfully investigate and prosecute terrorist offences.

However, law enforcement face several important challenges in this regard, particularly due to the large amount of data that needs to be processed, the variety of different devices or applications (as well as encrypted applications), and the number of languages that may be involved. The Conference recognised that many law enforcement entities lack sufficient forensic expertise and tools to properly collect, store and preserve electronic data from such a wide range of potential sources.

Terrorist organisations and networks are constantly adapting their communication strategies as the available technology changes, migrating to encrypted or closed platforms to avoid detection. This has made gaining access to data on online services by tech companies quite challenging, especially when such platforms are operated or owned in one or more foreign jurisdictions. This situation often requires law enforcement authorities to work with international partners and intermediaries to gain access to vital electronic evidence and data. This situation can also be made more challenging by differences in legal frameworks, the lack of standardised policies in the digital sector, the length of formal procedures, and the perceived lack of responsiveness to requests for preservation and disclosure. The lack of harmonised, effective systems means that some national authorities have instead sought *ad hoc* arrangements or direct voluntary cooperation from online service providers, even in circumstances when there are available judicial cooperation or mutual legal assistance mechanisms.

A number of international and regional initiatives are attempting to address these issues. In particular, the Organisation for Security and Cooperation in Europe (OSCE) has provided a number of media and information literacy trainings for law enforcement authorities. Several projects have produced outputs such as the practical guide for requesting electronic evidence across borders, co-developed with the United Nations Office on Drugs and Crime.

Furthermore, initiatives such as EUROPOL's SIRIUS project are designed to help law enforcement and judicial authorities to improve access to electronic evidence during criminal investigations. This project is further supported by a set of recommendations which have been made for both law enforcement authorities and online service providers, which can be found in the SIRIUS EU Digital Evidence Situation Report.

There is a need for improved transparency and meaningful cooperation between the different public and private actors in this area, especially toward the development of efficient mechanisms and tools to collect, preserve and analyse electronic evidence while maintaining the chain of custody for its use as evidence in a court of law.

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

During the last session of the Conference, panellists discussed the importance of reinforcing human rights and rule of law mechanisms when countering terrorist content online. This remains a challenge for many governments and internet companies as there is a need to balance human rights, counterterrorism, and a free, open and secure internet.

Radical and extremist speech is generally protected under freedom of expression laws, and can only be restricted by States under exceptional, necessary, and proportionate circumstances. Online content is, however, generally subject to private moderation rules, community standards or terms of service are defined by online platforms themselves. These terms of service define obligations, limits, and conditions for the use of the platform beyond applicable legal provisions, and are generally enforced across all users, independently from the user's actual jurisdiction.

Speakers observed that these issues can be complicated by the emerging role private companies may have in counterterrorism, and the unclear scope of their corresponding tasks and responsibilities. Some of the challenges for tech companies therefore flow from continued challenges in the international counter-terrorism framework. While terrorism may be well-defined by national or regional legal frameworks, across jurisdictions there are significant differences towards core concept such as "terrorism" and "violent extremism". Private companies can struggle to clearly determine what content should be prohibited, removed and preserved. Though many companies rely on international terrorism lists to guide their actions, this can present significant risks as these lists may not be up to date with contemporary terrorist threats, or may be abused by certain States to restrict legitimate conduct by minority communities or certain protected classes, such as journalists, human rights defenders, or civil society organisations.

Private sector companies, unlike State bodies, are not directly bound by human rights law. Instruments such as the UN Guiding Principles on Business and Human Rights are a key set of non-binding standards which can guide private sector action in this area.

Key initiatives such as the Christchurch Call and its Advisory Network, launched jointly by New Zealand and France, support efforts to address terrorism and violent extremism while promoting human rights. The Advisory Network helps to ensure that there is an active role in this process for civil society groups, academia and human rights organisations in shaping responses to terrorism content online. Furthermore, the Global Internet Forum for Counter-terrorism (GIFCT), a non-profit organization and tech-led initiative, has worked to ensure that human rights are a core, complementary component of their work, requiring participating companies to uphold human rights values while also preventing terrorists and violent extremists from exploiting their digital services.

Panellists discussed the need for appropriate and effective safeguards for individuals to uphold their human rights when content is wrongfully removed or targeted. As such, in order to provide a clear human rights-based approach to countering terrorist content, there is a need to enhance and improve current international legal frameworks addressed towards private companies.

Key takeaways from the Conference

While covering a wide array of interrelated topics, this Conference only scratched the surface in what is a complex and challenging area. A few key takeaways can be extracted in order to help guide further CDCT action and events in these areas:

- Terrorists have shown to be innovative in using a variety of online communication platforms to spread their ideology, inspire or encourage terrorist attacks, and spread instructional material to would-be attackers. and personal networks. Terrorists and violent extremists deploy a variety of communication strategies largely according to the specificities of their organisation, ideology and target audience. Particularly in decentralised or post-organisational terrorist movements where lone actor attacks have become the norm, a significant amount of this material is aimed at encouraging and enabling individuals to carry out violent attacks.

- While this propaganda may be aimed at radicalising individuals to terrorism, radicalisation is often a complex, non-linear process which can depend on multiple individual and environmental factors. In order to comprehensively prevent and disrupt radicalisation, it is important to understand and identify risks related to individual characteristics and circumstances as well as local factors. Online and offline dimensions of radicalisation to terrorism are not to be considered as separate, but rather complementary and interdependent. While online spaces can offer terrorists and violent extremists ways to reach broader audiences, offline spaces and in-person interactions still play a critical role in terrorist radicalisation.

- Young people are increasingly targeted by terrorists and violent extremists, either to gain followers and sympathisers to their ideology and cause, or to directly recruit them. Many terrorist communication strategies are designed to appeal to younger audiences, for instance by using elements from pop culture, video games or memes in their communications. Specific preventive measures are needed to build resilience among the youth sector, particularly through education and training on media literacy.

- Early warning systems and response mechanisms, aimed at monitoring, preserving or removing such online content from internet platforms should be regularly updated and reviewed, in cooperation with national and international bodies, as appropriate, and to take into account key trends and patterns of terrorist abuse of the internet.

- Accurately identifying terrorist content online can be vital for the investigation and eventual prosecution of a range of terrorist offenses. While removing such content is vital to limiting the spread of terrorist propaganda, it is also necessary to properly collect and preserve such material in order to potentially use it as evidence in criminal proceedings. However, requesting access to electronic evidence, especially across borders, relies on international cooperation between states as much as it does with online services providers. To facilitate and improve the process of request for disclosure or preservation of data, there is a need for key actors on all sides to be properly trained and informed on key technical and legal issues of mutual interest.

- There have long been a number of challenges related to the lack of harmonised definitions of terrorist and violent extremist content. States and online service providers need to find suitable standards that appropriately take into account their respective responsibilities and roles in accordance with human rights and rule of law principles. Effective safeguards and systems should be developed and implemented in order to tackle terrorist content online while also preserving the free, open and secure nature of the Internet.