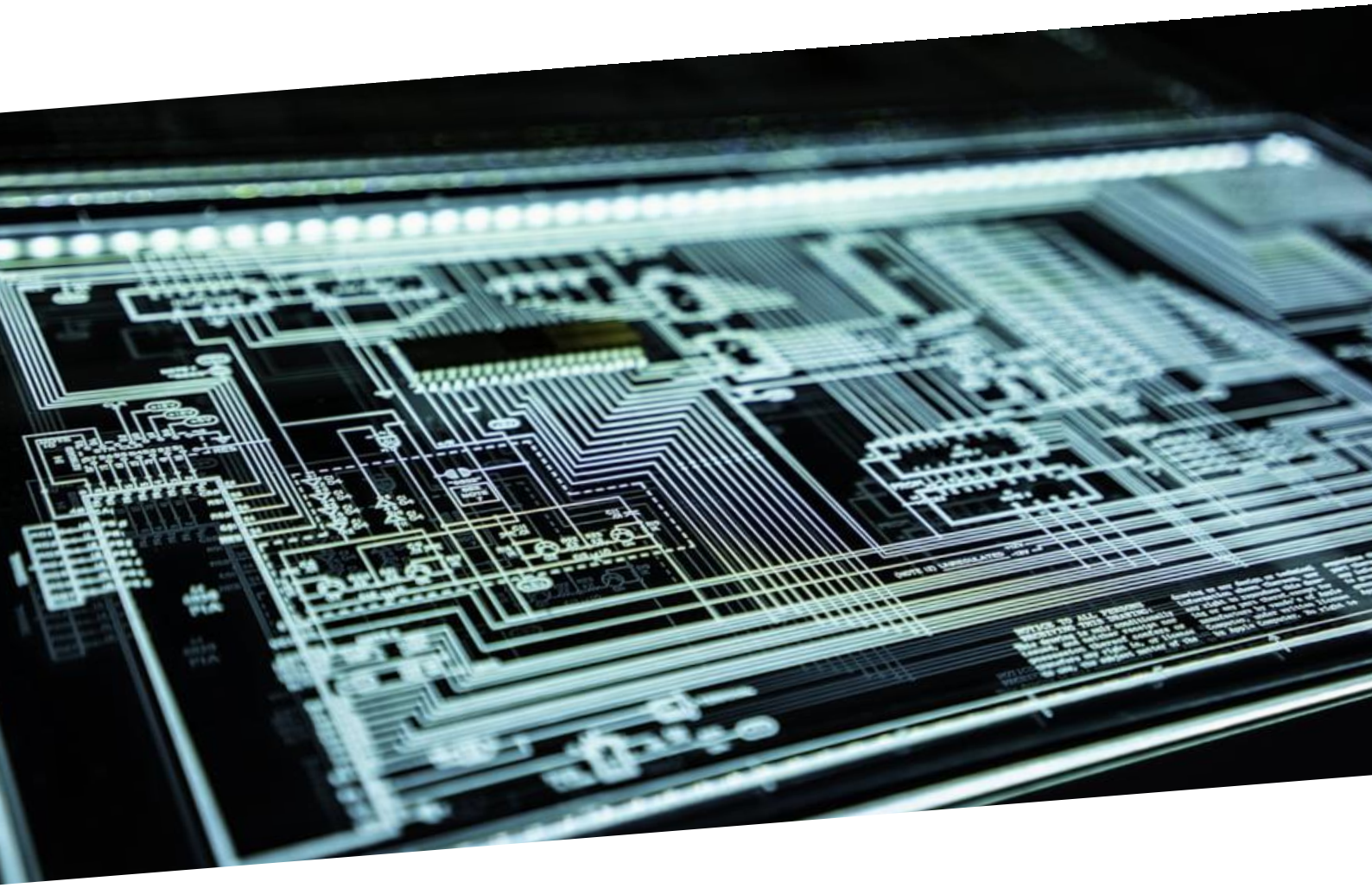
FRISCO

Fighting Terrorist Content Online

FRISCO Final Conference Report & Conclusions

"*Fighting Terrorist Content Online: Progress, Challenges & Perspectives*"



DEMOKRITOS · TREMAU · INACH · MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER · CIVIPOL · learn · Violence Prevention Network · IVSZ

Funded by the European Union

TABLE OF CONTENT

Funded by the European Union

INTRODUCTION

The TCO regulation came into force more than two years ago. Soon after, the **FRISCO (*Fighting Terrorist Content Online*) project** was launched to **support micro and small tech platforms** in their content moderation and compliance efforts. Since then, the FRISCO Project has successfully provided support through **information, tools, training, best practice materials, collaboration and research**. The FRISCO project comes to an end in November 2024, but the fight against online terrorism remains a top priority at EU level, requiring a combination of legislative, non-legislative and voluntary measures. Significant progress has been made, but challenges remain to maximise the effectiveness of the TCO Regulation and related countermeasures.

To celebrate and ensure its continued success, the FRISCO project held its **final two-day conference in Brussels on Thursday 17 and Friday 18 October 2024**. This event aimed to open new streams of cooperation and practice by bringing together experts and practitioners from different fields (EU officials, policy makers, law enforcement, regulators, tech sector representatives, academics, researchers, NGOs, etc.) to discuss **strategies to curb online terror**. The focus was on **bridging the gaps** between policy, practice, law enforcement and research, as well as between the different components of **P/CVE (Preventing and Countering Violent Extremism)** at EU level.

This final conference had **five objectives**:

1. **Present the results and products of the FRISCO project** in a comprehensive manner, while ensuring their continued success and dissemination
2. **Bring together experts and practitioners to build partnerships and share experience,** knowledge and best practice in a single forum.
3. **Present the main successes and challenges related to the implementation of the TCO Regulation** and, more generally, to compliance with EU digital regulation (e.g. DSA), based on the experience of key stakeholders.
4. **Examine the online terror threat landscape**, highlighting key trends and their link to offline events, thanks to insights from the European research community
5. **Assess the effectiveness of countermeasures** and discuss practical solutions for countering harmful narratives, content distribution strategies and malicious use of new technologies.

The programme included **five sessions** over two days, with Day 1 (17 October) focusing on "Terrorist Use of the Internet: Trends & Regulations" and Day 2 (18 October) on "Countering Online Terror: Practices & Responses".

1. **A changing threat landscape?** Terrorist Use of the Internet – Trends & Challenges
2. **Navigating the EU's Digital Regulation Landscape**. TCO Regulation & Digital Services Act – Practicalities & Insights
3. **Seeing through the Eyes of Tech Platforms**. From Micro to (Very) Large Tech Platforms – Needs, Capacities & Challenges.
4. **Moderating Harmful Content:** Challenges, Debates & Approaches in a Trust & Safety Perspective
5. **Improving our Counterterrorism Response** – Perspectives, Partnerships, Practices

Funded by
the European Union

Please note that the agenda and detailed programme are available on **our website**. The conference welcomed over **87 participants** representing **63 organisations** over the two days. Over the course of 5 sessions**, 28 speakers** took to the stage for a total of **14 presentations and 2 panel discussions**.

Following their insightful contributions which made the event a success, we would like to extend our warmest thanks to all our participants and speakers, listed in alphabetical order:

- **Dr. Dimitra CHONDROGIANNI** - Greek E-Commerce Association, ALLIES
- **Diarmuid COEN** – Coimisiún na Meán (Ireland)
- **Anne CRAANEN** – Institute for Strategic Dialogue
- **Anna DE MARCHI** – European Commission (DG CNECT)
- **Stéphane DUGUIN** – CyberPeace Institute
- **Dr. Julia EBNER** – University of Oxford (Violent Extremism Lab)
- **Lydia EL-KHOURI** – Textgain
- **Hadelin FERONT** – META
- **Yolanda GALLEGO-CASILDA GRAU** – European Commission (DG HOME)
- **Arda GERKENS** – ATKM (Netherlands)
- **Yann LESCOP** – Point de Contact
- **Dr. Beatriz LOPES BUARQUE** – London School of Economics
- **Charlotte MARIEN** – European Commission (DG HOME)
- **Louise MELOY** – Tech Against Terrorism
- **Lucile PETIT** – Arcom (France)
- **Yolina PETROVA** – Identrics
- **Dr. Erin SALTMAN** – Global Internet Forum to Counter Terrorism (GIFCT)
- **Dr. Christina SCHORI LIANG** – Geneva Centre for Security Policy (GSCP)
- **Andrew STANIFORTH** – SAHER, Tech Against Terrorism Europe
- **Fabian WICHMANN** – EXIT Germany
- **Cecilia ZAPPALA** – Youtube

And finally, a special thanks to our speakers and moderators from the FRISCO Project:

- **Isabelle ARNSON** – Tremau
- **Pál BOZA** – Tremau
- **Dr. Athanasios DAVVETAS** – National Centre of Scientific Research – 'Demokritos'
- **Louis-Victor DE FRANSSU** – Tremau
- **Giulia DINO GIACOMELLI** – GDG Inspire
- **Rositsa DZHEKOVA** – Violence Prevention Network
- **Alexandra KORN** – Violence Prevention Network
- **Pierre SIVIGNON** – Civipol

Funded by
the European Union

CONFERENCE SUMMARY

Day 1 (17 October 2024). Terrorist Use of the Internet: Trends & Regulations

The conference kicked off with an overview of the **FRISCO project** ('*Fighting Terrorist Content Online*'), which aims to help micro and small Hosting Service Providers (HSPs) comply with the TCO Regulation and foster collaboration between stakeholders to counter online terror and create a safer online environment. Running from 2022 to 2024, FRISCO focused on **tool development, identification of best practice, and awareness raising**. As the project draws to a close, the focus is now on the **sustainability** of its results.

Yolanda GALLEGO-CASILDA GRAU (Head of Unit, D.3 Prevention of Radicalisation at the European Commission, DG HOME) addressed the conference with opening remarks, highlighting the importance of the **TCO Regulation** and reminding participants of the crucial need for **cooperation** between civil society, academia, tech platforms and EU Member States in the face of evolving online threats. She further noted the first European Commission report on the implementation of the TCO Regulation showing significant progress, with around **350 removal orders** as of December 2023 and that future policy initiatives to combat the spread of terrorist content online are likely to focus on **prevention and social inclusion**. Several **challenges** were also highlighted, including platform compliance, the adaptability of terrorist actors, the intersection with gaming and emerging AI threats.

Session 1. A Changing Threat Landscape? Terrorist Use of the Internet: Trends & Challenges

The aim of this first session was to draw on the latest academic research to provide an **overview of the threat landscape**, and to pave the way for **recommendations**. The session opened with insights from the **FRISCO mapping report**, published in early 2023, including the use of dead drop techniques and decentralised platforms.

Dr. Julia EBNER (Leader of the Violent Extremism Lab at the Centre for the Study of Social Cohesion, University of Oxford) began by pointing out the interplay between **identity and extremism**, analysing the drivers of violent behaviour in online groups through the findings of recent studies (2022, 2023). These studies introduce a **novel language-based framework** ('*fusion-based NLP framework*') for assessing the risk of online users to engage in pro-group violence by analysing (terrorist) manifestos. In short, Dr. EBNER showed that strong **linguistic markers** have been identified, such as identity fusion, offensive language towards out-groups, and violence-justifying norms, which - when combined - suggest a higher risk of violent behaviour. To improve counter-terrorism efforts, these findings argue for the inclusion of **socio-psychological markers** in risk assessment frameworks, **identity-centred interventions**, and for government agencies, intelligence services, police forces, courts and tech platforms to make more data available to researchers.

Anne CRAANEN (Senior Research and Policy Manager at the Institute for Strategic Dialogue) presented a snapshot of the **hybridised threat landscape online**. Research based on three main

Funded by the European Union

methodologies (i.e. large-scale analysis of social media data, ethnographic analysis of extremist communities, rapid response analysis) suggests **shifts in extremist mobilisation**, with movements becoming **less structured**, forming **opportunistic alliances** and using **disinformation** to coordinate hateful activities and integrate extremist views into the political mainstream ('**mainstreaming**'). Based on two case studies of recent events (i.e. the Israel-Gaza-Lebanon war and the Southport riots), Ms. CRAANEN provided insights and recommendations. In short, **policy responses to far-right extremism should adapt to its decentralised, multi-platform nature**, focusing on both large and smaller high-risk platforms. Where legislation applies, it should tackle illegal content, while for borderline content, **alternative approaches** should be considered. Strategies must address **non-ideological factors**, such as social isolation and support for violence, and respond to the hybridisation of extremism and misinformation. A long-term strategy to counter extremism is essential, emphasising digital literacy, **social cohesion** and **resilience building efforts**.

Dr. Beatriz LOPES BUARQUE (Fellow at the London School of Economics and Political Science) then explored how **conspiracy theories** and online subcultures contribute to **radicalisation**. Conspiracy theories thrive on epistemic (understanding), existential (control) and social (group identity) motives. Certain '**paranoid style**' theories (e.g. 'white genocide', 'great replacement', 'cultural Marxism', 'deep state') are more likely to radicalise by promoting **narratives of persecution**, **good versus evil** and urgent catastrophe prevention. Drawing on Lacan's concept of '**fantasy**', Dr. LOPES BUARQUE showed that these theories attract individuals by fulfilling desires for understanding and superiority, often bringing together like-minded individuals online. Factors such as **authoritative performances** and **algorithmic recommendations** increase the risk of radicalisation, while **generative AI** can exacerbate threats through deep fakes and the amplification of extremist narratives. Key risks include terrorist attacks, public displays of racism, xenophobia and sexism, biassed education and targeted shaming campaigns.

Dr. Christina SCHORI LIANG (Head of Counterterrorism and PVE at the Geneva Centre for Security Policy) concluded the session with insights into the **misuse of advanced technologies by terrorist actors**. Key risks include technological innovations that could be exploited by terrorists, such as **3D printing** for weapons production, **autonomous drones** using AI, and **social media manipulation** through bot networks. The influence of powerful tech companies and the '**poly-pandemic**' of Covid-19 (health crisis plus societal instability) further complicate the landscape, while we are experiencing an era of '**truth decay**'. Against the backdrop of the war in Ukraine, characterised by the commercial use of space, AI, drones and 3D printing, the importance of reckoning with **violent non-state actors sharing tactics globally** was highlighted, such as the need to **regulate autonomous weapons**.

Session 2. Navigating the EU's Digital Regulation Landscape. TCO Regulation & Digital Services Act: Practicalities & Insights

The aim of this second session was to **explore the issues surrounding the implementation of the TCO Regulation and the Digital Services Act** (DSA), identify **progress and challenges**, and gain insights on how best to navigate the EU digital regulatory landscape through operational best practices from key stakeholders. Lessons from the FRISCO project, particularly on the **readiness and capacity of micro and small HSPs**, were presented at the beginning of the session. Although many HSPs have already adapted, challenges remain, particularly for smaller platforms that lack the resources. A question was put to the audience to identify **obstacles to the implementation of the TCO Regulation**. The responses collected included: insufficient platform collaboration, knowledge gaps, non-responsiveness of HSPs, political factors, resource constraints, platform structure, data accuracy and cost allocation.

Anna DE MARCHI (Case Handler for the DSA at the European Commission, DG CNECT) and **Charlotte MARIËN** (Policy Officer at the European Commission, DG HOME) provided a **comparative analysis between the TCO Regulation and the DSA**, highlighting **differences** in scope and enforcement, but also **synergies** between the two regulations. In terms of objectives, the **TCO Regulation focuses on harmonising rules to combat terrorist content online** and prevent radicalisation. In contrast, the **DSA has a broader objective** of harmonising due diligence obligations and liability exemptions, in particular emphasising the increasing responsibility of social media platforms and the empowerment of users. **Recent updates** show significant activity under both regulations. Since 2002, more than **1,100 removal orders and 36,000 referrals** have been issued under the TCO Regulation, with 24 member states registered and 19 infringements closed. Meanwhile, from 2023 to early 2024, **24 Very Large Online Platforms (VLOPs)** have been designated under the DSA, **60 requests for information** have been received, **8 proceedings** have been initiated and **2 risk assessment cycles** have been launched. The scope of both regulations also differs significantly. The **TCO Regulation includes a clear definition of the content it regulates**, which includes a list of persons and groups associated with terrorism and **applies to HSPs offering services in the EU** without imposing additional responsibilities based on their size. Conversely, the DSA as a horizontal legal act **does not define what constitutes illegal content** (instead referring to national and EU *lex specialis*) and exempts small and medium-sized enterprises (SMEs) from certain rules while placing **additional obligations on VLOPs**. When it comes to the instruments used, the TCO primarily employs **removal orders** as its main regulatory tool, allowing for cross-border content regulation without requiring automated tools and including a mechanism for user complaints. The DSA, while also using removal orders, provides a framework that includes a notice and action mechanism, trusted flaggers, and mandates risk assessments for content that may be harmful but is not illegal (e.g. disinformation).

Lucile PETIT (Head of Online Platforms Regulation at Arcom, France), **Arda GERKENS** (President at ATKM, Netherlands) and **Diarmuid COEN** (Director of Investigations at Coimisiún na Meán, Ireland) concluded with a **panel discussion on common challenges related to the TCO Regulation and the DSA**. Key topics included differences in **application**, **transparency** standards, **removal order** procedures and the use of the **PERCI platform** (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*), as well as **crisis response strategies**, **risk assessments** and support for companies' compliance efforts. In summary, the **TCO** is recognised for its **enforceable, direct approach** to removing harmful content, while the **DSA** prioritises **transparency and legal compliance**, although it faces challenges, particularly with non-European platforms. Effective **cross-jurisdictional cooperation** and **training** were identified as essential to improve the impact of regulation.

Day 2 (18 October 2024). Countering Online Terror: Practices & Responses

The second day of the conference began with **insights from the FRISCO project** into the **challenges faced by micro and small HSPs** in complying with the TCO Regulation. A key challenge identified was how to **engage and support** small platforms, which often have **limited resources**, **different priorities** and **low awareness of counter-terrorism regulations.** Small HSPs may lack the resources or familiarity with **AI detection and monitoring tools**, as well as proactive content moderation strategies, making it difficult to implement these solutions. The FRISCO project highlighted that small HSPs have **limited capacity to invest in such technology**, highlighting the **need for holistic solutions** that are better tailored to their needs. The project's findings suggest that **size, knowledge and resources** are closely related factors that should be considered in future **regulatory support** for these platforms.

Funded by
the European Union

Session 3. Seeing through the Eyes of Tech Platforms. From Micro to (Very) Large Tech Platforms – Needs, Capacities & Challenges.

The aim of the third session was to look at the issues raised so far from the **point of view of tech platforms**, to identify their **needs, capabilities and challenges**, and to highlight the **progress** made over the last two years.

Louise MELOY (Senior Intelligence Analyst at Tech Against Terrorism) began by looking at **the targets and dissemination strategies of terrorist actors** to better understand how they misuse online platforms to spread propaganda online. Terrorists use the internet for **strategic communication**, **operational needs** and to exploit **emerging threats**. Case studies highlight persistent risks, such as Telegram's limited content moderation. Cases such as the IS-K (Islamic State - Khorasan Province) attack on Moscow's Crocus City Hall show the **overlap between terrorist and disinformation content**, while **generative AI** extends the life of terrorist crisis material online. The **gamification** of terrorist **live streams** draws users into more extreme, less regulated spaces. Offline, terrorist propaganda such as IS-K's campaigns target **high-profile EU events** (e.g. the Champions League and the Paris Olympics), inciting attacks and amplifying their impact.

The floor was then given to the two other projects in the TCO cluster, **Tech Against Terrorism Europe** and **ALLIES**, represented by **Andrew STANIFORTH** (Director at SAHER - Tech Against Terrorism Europe) and **Dr. Dimitra CHONDROGIANNI** (Project Manager at the Greek E-Commerce Association – ALLIES), with whom the FRISCO project has been working for two years, with the shared objective of **addressing the challenges faced by small platforms** in moderating terrorist content and achieving compliance. First, speakers highlighted the critical need for collaboration between governments, academia and businesses to support HSPs, as well as the lack of expertise and resources that hamper small HSPs in content moderation and compliance, and a relative lack of empathy for their unique challenges. They also highlighted the vulnerabilities small platforms face, such as being 'soft targets' for exploitation, complex regulatory requirements and limited access to moderation tools. Speakers emphasised the need for efficient, unified reporting systems, continuous threat monitoring and training on how to identify and regulate terrorist content. The resources (tools, training, etc.) provided by both projects to address these challenges were also presented.

Hadelin FERONT (Counter-Terrorism Public Policy Manager at META) and **Cecilia ZAPPALA** (Head of EU Government Affairs and Public Policy at YouTube) concluded the session by **sharing insights** from the VLOPs perspective into new tools and frameworks for **moderating terrorist content online** and **enhancing compliance** with the TCO Regulation and the DSA while maintaining community standards. Emphasising **a shift from enforcement to prevention**, these platform representatives presented innovations in removal processes and proactive strategies, aiming for a **collaborative ecosystem** that fosters safer online spaces. Key elements include **clear, detailed policies** and thorough documentation of internal tools, which are crucial for regulatory compliance and efficiency. Platforms also prioritise **empowering users and protecting their voices**, **banning dangerous organisations**, and using **advanced detection technologies**. Some of the moderation frameworks presented focused on the following objectives: removing terrorist content with **AI-powered tools**, promoting quality information, limiting the spread of **borderline content**, and rewarding trusted creators.

Funded by the European Union

Session 4. Moderating Harmful Content: Challenges, Debates & Approaches in a Trust & Safety Perspective

Yolina PETROVA (VP of AI & Data Solutions at Identrics), **Lydia EL-KHOURI** (Project Manager at Textgain) and **Yann LESCOP** (Head of Projects and Studies at Point de Contact) in a **panel discussion** on the topic of **moderating harmful content** shared their **insights on the challenges, debates and approaches to content moderation**, particularly considering advances in **AI tools**. The panel explored the evolving role of AI in content moderation, highlighting that AI currently serves as a **support tool for human moderators** by pre-analysing content and protecting the **mental health** of moderators. While AI prioritises content for review, **human oversight remains essential**, especially for **understanding context, humour and cultural nuances**. Panellists emphasised the need for **AI and humans to work together**, with ongoing training on AI capabilities to improve effectiveness. There was a focus on whether content moderation tools should be **general or specific to terrorism**, noting that while dedicated tools would be ideal, adapting existing technologies is often more practical. The panel stressed the need for tools that are **accessible to small platforms**, which may lack the resources and technical capacity to adopt advanced technologies. There is scepticism about the ability of small platforms to **move from basic tools to more sophisticated ones**, despite the desire for free solutions. Panellists raised **concerns about future regulation**, in particular the 2026 EU's **AI Act**, which could complicate tool development due to unclear guidelines and potential restrictions on existing technologies. They stressed the importance of **clear regulatory definitions** and **increased education** on regulations such as the AI Act to avoid hindering technological progress.

During the **Q&A session**, panellists noted that Civil Society Organisations (CSOs), especially smaller ones, often see AI as too complex or expensive, and need **awareness and education** to consider adopting it. They emphasised the role of a trusted global network of **independent flaggers** for content moderation and stressed the need for **balanced and unbiased AI training**, urging close collaboration between developers and academics. The discussion concluded that **the future of content moderation will depend on balanced human-AI integration**, **accessible tools** for smaller platforms, and **clarity from policy makers**.

Session 5. Improving our Counterterrorism Response – Perspectives, Partnerships, Practices

The fifth and final session of the conference focused on why practices and partnerships are needed for **improving counter-terrorism responses**.

Stéphane DUGUIN (Chief Executive Officer at the CyberPeace Institute) discussed the response to the **weaponisation of disruptive technologies** (e.g. integrated, immersive, decentralised) by terrorist actors, beginning with case studies of cyber-attacks in Costa Rica (2022) and Sweden (2024), and highlighting the **challenges of compartmentalising tools in the face of interconnected cyber and terrorist threats**. In the face of such challenges, the need for a **hybrid strategy emphasising a dynamic, holistic approach** to security and policy was highlighted.

Dr. Erin SALTMAN (Director of Membership & Programs at the Global Internet Forum to Counter Terrorism) then focused on **partnerships**, addressing the complexities of countering violent extremism online and highlighting the **need for collaborative efforts among technology companies to tackle cross-platform extremist content**. It was recalled that the online threat landscape is characterised by diverse, overlapping ideologies exploiting different online services, **cross-platform and transnational issues**, and a **dynamic and adversarial environment.** Key strategies discussed included **prevention**, an **incident response framework** that includes identification,

Funded by the European Union

validation and action phases, and the importance of **adapting and sharing knowledge** while respecting human rights.

Fabian WICHMANN (Senior Case Manager at EXIT Germany) concluded with a discussion on **practical strategies for countering narratives and integrating online and offline interventions**. The **growing importance of the online sphere** was highlighted, alongside recognition of changes in the offline landscape, in particular the link between online and offline radicalisation. Future challenges were outlined, in particular the need to **anticipate technological developments** related to **synthetic media and AI.** This includes engaging in **ethical discussions** about AI, promoting **AI literacy**, and **working with civil society** and technology initiatives, while ensuring that adequate resources are allocated to manage these developments. The presentation identified **additional challenges** such as **disinformation**, **gaming**, regulation and **free speech**, **hybrid ideologies**, and the impact of **cryptocurrencies and fintech**. Importantly, it was noted that an **exclusive focus on risks could overlook opportunities** to use technology constructively. While discussions often highlight the negative aspects of technology, it is important to explore how it can be used to **create innovative solutions to counter extremism**. Overall, the presentation called for a **nuanced understanding** of the evolving landscape of extremism, the **dual role of technology**, and the importance of considering **demographic and ethical factors** in addressing these issues.

Overall, the session highlighted the need for **collaborative, multi-stakeholder frameworks** that can adapt to **the hybrid nature of modern threats**, particularly as cyber and physical risks converge. The call for **innovation and ethical adaptability** underscored the need to address the multifaceted challenges of online terrorism while **fostering ongoing partnership-building efforts** to improve prevention and response to incidents.

CONCLUSIONS: FINDINGS & RECOMMENDATIONS

The final conference of the FRISCO project brought together a diverse group of experts, stakeholders and practitioners to discuss the pressing issues surrounding terrorist content online. Over two days, participants engaged in thoughtful discussions and shared insights on the evolving threat landscape, the role of tech platforms, and the need for collaborative approaches to counter terrorist content and radicalisation online.

Key Insights

An evolving and complex threat landscape – The conference underlined the multifaceted nature of terrorist content and activities online, highlighting how very different platforms are being exploited by terrorist actors. The latter are increasingly using disruptive technologies, such as generative AI, to spread propaganda online and potentially carry out attacks. The hybridisation of threats complicates the monitoring and regulation of online content.

An innovative regulatory framework between progress and challenges – The conference highlighted the crucial role of the TCO Regulation in combating the dissemination of terrorist content online, as well as its differences and synergies with the Digital Services Act. While recent updates showed significant activity under both regulations and that this innovative and strengthened legal framework has underpinned great progress, challenges remain, including non-compliance by certain platforms and the difficulty of monitoring non-European entities.

A key role for tech platforms, unique challenges for small ones – The key role (to be played) by tech platforms in disrupting terrorist activity online was highlighted, such as the unique challenges faced by smaller platforms. Despite significant progress over the past two years, many still lack the resources to implement effective moderation strategies, highlighting the need for tailored solutions that fit their operational realities. Best practices can be learned from larger platforms, and collaborative frameworks that provide accessible tools and training are essential to empower these micro and small HSPs.

The need for collaborative partnerships and approaches – The importance of cross-platform and multi-stakeholder partnerships was reiterated. Collaboration between tech platforms, EU institutions, governments, academia and civil society organisations is crucial to creating a unified response framework to counter online violent extremism. Ongoing dialogue and knowledge sharing will strengthen these partnerships and increase their effectiveness. Education reforms that emphasise critical thinking and digital literacy from an early age are critical to equipping future generations to recognise and resist extremist content.

Moderating harmful content and countering extremist narratives – Among the various priorities identified during the conference, the importance of effective content moderation and proactive counter-narratives was highlighted. In terms of content moderation, a consistent theme emerged throughout the conference: the balance and necessary synergy between AI and human moderation. While AI tools can increase efficiency, the need for human oversight remains critical. Similarly, addressing the narratives used by extremist actors is paramount to countering radicalisation. There is an urgent need for anticipatory approaches that use technology to develop proactive solutions, while investing in capacity building within civil society organisations to support their work building resilience to extremist ideologies.

Funded by
the European Union

Recommendations

1. Tailor Solutions for Small Platforms – Ensure that the resources produced by the TCO cluster are widely available. Where necessary, develop additional resources and training specifically for small HSPs to improve content moderation and compliance, focusing on easy-to-use tools and threat awareness.

2. Boost Multi-Stakeholder Collaboration – Strengthen cooperation between tech platforms, EU bodies, governments, academia, and civil society to share best practices and resources for dealing with terrorist and harmful content.

3. Improve Regulatory Compliance – Where necessary, provide additional guidance and workshops to ensure that tech platforms, especially the smaller ones, understand the TCO Regulation and DSA requirements, with accessible resources for ongoing support.

4. Responsible Use of AI – Promote AI in content moderation responsibly by creating guidelines to reduce algorithmic bias and improve transparency.

5. Invest in Human Moderation – In addition to automated tools, ensure that content moderation is always done with a human in the loop, and that human moderators are psychologically supported and trained in cultural awareness, bias detection and resilience to facilitate sensitive, effective moderation.

6. Promote Research and Innovation – Support research into the drivers of online radicalisation and invest in advanced detection tools to inform policy and identify extremist content, including AI-generated media.

7. Emphasise Educational Initiatives – Integrate digital literacy and critical thinking into education to help young people critically engage with online content and recognise extremist narratives.

8. Encourage Counter-Narratives – Support initiatives that create counter-narratives to extremism, working with civil society to produce engaging content with wide reach.

9. Stay Ahead of Emerging Threats – Continually monitor trends in online extremism, including synthetic media, and update policies and tools to proactively address these threats.

10. Leverage Cross-Platform Strategies – Develop coordinated frameworks for platforms to share data and jointly tackle extremist content, especially in cases of viral misinformation and coordinated attacks.

The FRISCO Final Conference, "Fighting Terrorist Content Online: Progress, Challenges & Perspectives", highlighted the urgent need for a multifaceted and collaborative approach to addressing the challenges posed by terrorist use of the internet. As stakeholders continue to navigate this complex landscape, the insights and recommendations shared during the event will be invaluable in guiding efforts to effectively combat terrorist content online. By fostering collaboration, using technology responsibly, and prioritising tailored solutions, we can work together to create a safer online environment for all.

Funded by
the European Union

About FRISCO

FRISCO ("*Fighting Terrorist Content Online*") is an EU-funded project implemented by a team of 8 partners across Europe. Our main objective is to raise awareness among small tech companies and online platforms and to help them comply with the EU Regulation on Terrorist Content Online (TCO Regulation). By supporting the fight against terrorist content in Europe, we are helping to prevent and counter violent extremism online and to create a safer online environment.

Follow us

friscoproject.eu
frisco-eu-project
FRISCOproject

Funded by the European Union

Disclaimer: This report is part of the EU-funded project FRISCO (https://friscoproject.eu/). Views and opinions expressed are however those of the speaker(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.