OSCE Organization for Security and Co-operation in Europe

OSCE The Representative on Freedom of the Media

OSCE Asian Partnership for Co-operation

Webinar:

Terrorist Use of the Internet: Designation of Illicit Content Online and Gaps in Regulatory Frameworks

12 March, 11:00 - 12:30 CET

OUTCOME DOCUMENT

The online event was organized by the **Action against Terrorism Unit** of the OSCE Secretariat's Transnational Threats Department (TNTD), with the support of the Albanian Chair of the OSCE Asian Partners for Co-operation Group and the OSCE External Co-operation Section. Over 180 participants (72 women and 110 men), among them experts and high-level officials from around the **OSCE area and beyond,** attended the event.

The event built on the OSCE round-table discussion on *Leveraging Innovation and Technology to Address 21st Century Security Challenges and Crises across the OSCE and Asian Partners for Co-operation* held virtually in November 2020.

The webinar of 12 March provided a platform for participants to review and examine the **current and emerging trends,** and key issues related to national regulatory and policy frameworks on designating illicit content online, as well as on the question how online platforms handle these challenges through their "terms of service". Expert discussions elaborated in particular how initiatives to address various forms of violent extremist and terrorist content online may negatively affect international human rights standards.

Among webinar panelists were representatives of different OSCE executive structures, as well as researchers and practitioners from Canada, Italy and Japan. Discussions reflected the growing concern over how **state responses can unintentionally limit freedom of expression**. While effectiveness in reducing unlawful content is crucial, strategies adopted by states, technology companies, and civil society also need to ensure respect for human rights.

In order to supplement state regulations and content removal with preventive efforts, states have a key responsibility to **enhance digital literacy and awareness** among their citizens, based on a public health approach that focuses on protective do-no-harm factors. One of the main messages of the event was that violent extremist and terrorist content online can be curbed effectively only through a combination of reactive and preventive efforts.

In their addresses, **Ambassadors Igli Hasani** (Permanent Representative of Albania to the OSCE, Chairperson of the OSCE Asian Partners for Co-operation Group) **and Alena Kupchyna** (OSCE Co-ordinator of Activities to Address Transnational Threats) underlined the escalation of threats posed by terrorist and violent extremist content, as well as other online harms. They acknowledged the ways how digital transformation is exacerbating those threats, and that states are struggling to respond in ways that are in line with international human rights standards.

The OSCE Representative on Freedom of the Media, Teresa Ribeiro highlighted the far-reaching effects that counter-terrorism and counter-"extremism" approaches have on media freedom across the OSCE area. She stated that anti-"extremism" laws, in particular, have been used to crackdown on journalists and others for reporting on or for speaking out about matters of public interest.

Dr. Eduardo Celeste from the School of Law and Government of the Dublin City University underlined the dual-edged nature of social media, being a tool that can both increase the capacity to exercise human rights and be used to infringe on the very same rights.

Central Asia was mentioned by one of the speakers as an example of a region with a growing digital economy, where now over half of the population has access to the Internet. Drawing on a research produced by **SecDev Group**, **Rafal Rohozinski** (CEO of SecDev Group) observed that the risk posed by online terrorist and violent extremist networks in Central Asia must be put in perspective. According to Mr. Rohozinski, terrorist and violent extremist ecosystems in the region are small but impactful. While having comparatively limited appeal, they proved to be resilient to government crackdowns, adapting and extending their reach via "amplifier networks"[1].

[1] *Social media amplification is the concept of taking an action such as a positive review and then sharing it far and wide across social media networks.*

Dr. Motohiro Tsuchiya from the Keio University in Japan, touching on the actual situation in Japan with relatively low risk of terrorism attacks, described that the immediate threat in Japan is perceived to be possible cyber attacks at the upcoming Olympic Games. He underlined the importance of finding the right balance between public policy, education, engagement and policing in addressing the risks and challenges in the increasingly interdependent, connected and digital world. In addition, Dr. Tsuchiya stressed the need to further discuss a legal framework acceptable internationally, in light of the fact that the Budapest Convention on Cybercrime has not been accepted as broadly as it could be wished.

A number of shared observations emerged from the discussions:

First, the absence of a universally agreed definition of terrorism and violent extremism has consequences. While there are universal understandings of the parameters of what constitutes a terrorist crime, social media platforms had to come up with their own (diverging) definitions. Consequently, they continue to face complex questions on where to draw the line between legitimate and illegitimate content. These challenges are difficult for human content moderators to respond to, let alone for Artificial Intelligence (AI) tools that are widely used in these efforts.

Second, state laws and policies can help shape progressive approaches to determining what is and what is not terrorist/violent extremist content. On the task of definitions, states cannot pass the buck to social media companies. Instead, working with inputs from civil society, they can set minimum standards for online platforms. Definitions of groups and content, and strategies to moderate them, must be balanced against crime prevention and rights promotion. Participants noted that the courts are setting out insightful positions in this regard, but that clearer definitions and guidance on “technological due process” and rule of law at the platform level are critical.

Third, civil society has a pivotal role to play in advocating human rights and minimizing effects of online terrorist and violent extremist content. Civil society has a key function in ensuring accountability and transparency as well as supporting regulatory clarity. Moreover, as the law often lags behind technological and societal developments, civil society is a repository of innovation. It plays a fundamental role in the prevention of violent extremism and terrorism, including in relation to promoting digital literacy, digital hygiene, mentorship and supporting the mitigation of online harms.

Fourth, there are tough dilemmas associated with preventing and countering violent extremism and terrorism online while ensuring respect for human rights. In Central Asia, as in other regions, there is a real risk that states might overreach in their effort to disrupt illegal content, leading to worrisome consequences, including encroachment on media independence (such as the rights of journalists to maintain confidentiality of sources, as well as attempts to restrict the use of encryption), indiscriminate surveillance and other instances in which anti-terrorist legislation can be abused to limit human rights. States should consider setting up accountability mechanisms to reconcile the competing approaches, including in partnership with civil society.

Fifth, empirically-informed debates are required to review the proportionality of interventions to regulate terrorist and violent extremist content. Overzealous takedown of content can lead to the suppression of free speech and self-censorship. Moreover, AI-enabled or automated content removal can also entrust companies with critical decisions over free speech, which should be more appropriately taken by public authorities. When introducing regulations on removal deadlines, states should consider timelines, which are manageable also for small-scale service providers, in order to avoid ensuing financial penalties. Moreover, a system of appropriate oversight is required to ensure that norms and regulations are human rights-compliant. The principles of necessity and proportionality are key, and states should work to apply the least restrictive interventions possible and ensure that these measures are subject to oversight.

Finally, it is important not just adopt a regulatory and rights-based approach, but also one that is informed by good practices and lessons learnt**.** There is evidence that overly aggressive takedowns of violent extremist and terrorist content often does not work, and in fact can make a situation worse. Also, there is a growing repository of good practices among states, social media companies and civil society groups about what works - including public education activities, digital safety campaigns, redirect interventions and other nudge strategies.

The webinar panel concluded that multilateral approaches are essential to address the real and growing threats posed by online violent extremism and terrorism. Informed by a human rights framework, good practices and lessons learnt, and shaped by tighter definitions of what constitutes violent extremist and terrorist content, a multi-stakeholder approach is essential to achieving results. States have a key role to shape norms and interventions, but they must be careful of overreach.

Report prepared
by Dr. Robert MUGGAH
Principal, SecDev Group

Annex 1

WEBINAR AGENDA

11:00 – 11:10 Opening remarks

- **Ambassador Igli HASANI,** Permanent Representative of Albania to the OSCE, Chairperson of the OSCE Asian Partners for Cooperation Group
- **Ambassador Alena KUPCHYNA,** Co-ordinator of Activities to Address Transnational Threats, OSCE Secretariat

11:10 – 12:00 Expert Presentations

- **Dr. Teresa RIBEIRO,** OSCE Representative on Freedom of the Media
- **Dr. Edoardo CELESTE,** Assistant Professor in Law, Technology and Innovation, School of Law & Government, Dublin City University
- **Mr. Rafal ROHOZINSKI,** CEO, SecDev Group
- **Dr. Motohiro TSUCHIYA,** Dean and Professor, Faculty of Policy Management, Keio University in Japan

Moderator: Ms. Georgia HOLMER, Head, Action against Terrorism Unit, Transnational Threats Department, OSCE Secretariat

12:00 – 12:10 Rapporteur comments

- **Dr. Robert MUGGAH,** Co-founder, Igarape Institute and Principal SecDev Group

12:10 – 12:30 Questions and Answers