International Conference

The Abuse of Livestreaming, Gaming and Virtual Reality Services and Platforms by Terrorist Actors

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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 Conference on "The Abuse of Livestreaming, Gaming and Virtual Reality Services and Platforms by Terrorist Actors", at the Council of Europe premises from 6 November to 7 November 2023.

Terrorism and violent extremism continues to evolve and change. A whole suite of online technologies has enabled terrorists to communicate, network, co-ordinate their activities and plan attacks in relative secrecy. Terrorists and violent extremists have long shown to be adept at using any new technology they can to broadcast footage of terrorist attacks, promote ideas of hatred and violence, radicalise and recruit new members while evading detection and disruption.

Given these challenges, the Conference focused on ways to prevent and respond to issues relating to terrorist adaptation of new technologies, in particular the pattern of using live streaming, gaming, and video-sharing services. The Conference benefited from the expertise of high-level experts, practitioners, and policymakers in this area, alongside representatives of regional and international organisations supporting global efforts to address these issues.

The Conference explored the most recent research and insights into current threats, motivations behind terrorist adoption of new technologies, challenges related to live-streamed terrorist attacks and strategies to reduce their impact. Major platforms have put in efforts to counter this issue, but cooperation with smaller platforms is crucial, as extremists often migrate to smaller, less regulated platforms.

The Conference also examined the wave of legislative developments regarding terrorist activity online. While these new legislative and regulatory instruments represent a significant step forward, there remain significant challenges for States and tech companies to comply with the evolving legal landscape due to the inherent difficulty in suppressing and countering terrorist activity online.

Moreover, as youth can be particularly vulnerable to the phenomenon of radicalisation to terrorism, experts and practitioners explored ways to prevent young people from being exposed to or drawn into violent extremist spaces online. Speakers also highlighted the need to prevent the spread of damaging ideologies which are often interlinked with violent extremism, such as misogyny and toxic masculinity, which are strongly prevalent in the gaming community.

As a safe, secure, and open internet is an essential feature of a modern democratic society, the Conference emphasised the importance of respecting human rights and fundamental freedoms, particularly the freedom of expression. In a world where each technological advancement can be adopted and abused by terrorist actors, it is crucial to disrupt terrorism in all its manifestations while also ensuring that ordinary citizens can take full advantage of these technologies in a peaceful and responsible manner.

Session I: New Technology, New Opportunities? Terrorist and violent extremist adoption and innovation

The first session addressed some of the issues concerning the abuse of new technologies by terrorist and violent extremist actors. It primarily looked at the current threats, the primary motivations behind terrorist adoption of new technologies and the ways in which such technologies could be abused by terrorists and violent extremists.

The question of why terrorist and violent extremist actors adopt new technologies can be linked to the significant role technology plays in our modern society. Some speakers suggested that this trend is expected, given the widespread use of technologies in all aspects of our everyday lives. For instance, the Internet has for many years been utilised in recruitment, thus it would be unusual if it were not adopted by terrorists and violent extremists in the same manner.

Terrorists are driven by the opportunities presented by the availability of new technologies. One speaker addressed the issue of video games as a vector of propaganda, as they offer platforms that can influence large audiences. Further factors underlining this statement included low moderation, easy ways to produce content and the "grey zone" between fiction and reality. This has been seen in other contexts, with online personalities circulating Russian propaganda in video games to justify the war in Ukraine.

This session also addressed the risks of radicalisation and the assessment of threats in the Digital Space. Looking at the process of radicalisation, aspects of online networks that make violent extremism attractive to individuals is the sense of community. Individuals that are vulnerable to radicalisation have a strong desire to be part of a group, community or identity in which they are told people will treat them with respect. The role of the COVID-19 pandemic was also emphasised, as many people spent significantly more time online, which was seen to have triggered many people's feelings of insecurity, and which in turn may have led to a higher level of vulnerability. These factors were highlighted as creating "a perfect storm" for radicalisation.

The session also looked at how practitioners can assess the risk that a radicalised individual may be moving towards committing an attack. For example, it was observed that almost all terrorist attacks have been preceded by published manifestos which are often spread as a source of information and to radicalise others. As such, it was emphasised that these published manifestos can be used to detect individuals who are planning to commit an attack.

The role of multiplayer games, which allow for stronger communities compared to other social media platforms, was highlighted. This depends on the common

goal the players share, which in turn can lead to a strong sense of identification with the group. Further indicators of radicalisation include expressions of anger and leakage, which means that the individual is specifying that they are going to commit an attack. It was, therefore, emphasised that the social and psychological aspects of the issue of violent extremist's adoption of new technologies cannot be forgotten if we are to understand the full picture.

Session II: Gamification of Terrorism: Gaming Platforms, Virtual Reality and the hidden corners of the internet

The second session of the Conference was aimed at understanding the risks posed by new technology and how these tools may be abused by terrorist actors to prepare or plan terrorist attacks, or to recruit new members. This was examined by looking at how gaming platforms are used by violent extremists, including how concepts of gaming have been applied by some communities to increase engagement with terrorist propaganda.

The session addressed the challenges of extremism on gaming platforms. These include a lack of awareness and knowledge of the issue, the relatively easy process of starting chatrooms or servers, and the lack of policies, reporting functions and content moderation.

Speakers discussed the reasons behind why terrorists and violent extremists use gaming platforms, explaining that these actors utilise these platforms to reach their intended audience. Part of the reasons why extremists use gaming spaces is not because they have a connection to gaming; instead, it is because they encounter little resistance when they use these platforms.

This session placed particular emphasis on the increasing harms across a variety of ideologies within the gaming space. While it was emphasised that games and gaming cultures have always had a sense of misogyny, sexism, homophobia and racism, this has currently been "weaponised". Research was also presented demonstrating that two-thirds of gamers reported that they had seen extremist content more generally, which was specifically prevalent on platforms where there is little to no moderation and in multiplayer video games.

A notable phenomenon which has reportedly been increasing is one where attacks have echoed video games and gaming culture, or heavily used gaming-related platforms in the preparation or broadcasting of an attack. This phenomenon is known as "gamification" and broadly refers to the use of gaming and game design elements outside of gaming contexts. For instance, a UNOCT report highlighted that extremists have used virtual leader boards to maintain "high scores" of body counts from attacks. Examples mentioned by speakers included the Christchurch attack in 2019, where the perpetrator livestreamed the attack wearing a camera - this attack produced a video-game-like view of the incident.

The response to extremism on gaming platforms requires strengthened cooperation between public and private actors, cross-jurisdictional policies and international collaboration. Speakers observed that there is a lack of cooperation between the gaming industry and public authorities in this space and that there is a need to bring policymakers, gamers and game developers together.

However, speakers emphasised that while there are serious issues of extremism that need to be addressed, there are many pro-social benefits of video games. Creating and fostering inclusive and diverse gaming spaces and gaming communities was mentioned as an important way to encourage online engagement that is resilient to extremism. As such, there are also benefits to exploring and empowering gamers and gaming communities to contribute to the solutions. Equally, the importance of allowing initiatives to be led by gamers themselves was highlighted, including prioritising the empowerment of gamers through investments in reporting features and community management.

Session III: Enhancing international cooperation to prevent the abuse of internet platforms by terrorists and violent extremists

The third session was dedicated to the challenges relating to international cooperation to prevent the abuse of internet platforms by terrorists and violent extremists.

It was recognised that online games have emerged as an additional tool for recruitment and propaganda. Minimal to no moderation on some platforms can result in extremists operating in relative safety and anonymity, which can also make them attractive for other criminal activities such as illicit use of cryptocurrencies. However, the nature of these services themselves can pose significant challenges to law enforcement since it impacts their ability to investigate crimes, but also to access data. For instance, gaming services have evolved with disruptive technologies, causing issues such as multiplicity, which means that one gaming session can involve multiple platforms and providers, making it difficult to identify the specific provider that collects the data. This presents challenges for law enforcement in investigations, as the data collected originates from different services.

Given that accessing data from foreign services is particularly challenging, this session placed emphasis on requesting e-evidence from such services. For many countries, generally depending on their national laws or lack of resources, accessing e-evidence is very difficult and requests can take a long time to process. Panellists thus explored some of the key international initiatives aimed at improving national capacities to request e-evidence across borders. Often, law enforcement agencies only have access to limited information, which poses challenges for proceeding with investigations. In this respect, the OSCE project "E-Vidence" aims to enhance the ability of law enforcement agencies to request e-evidence when investigating the online components of crimes, including terrorism-related cases, while also adhering to human rights.

A similar initiative is EUROPOL's SIRIUS project which is designed to help law

enforcement and judicial authorities to improve access to e-evidence during criminal investigations. At the Council of Europe, the Second Additional Protocol to the Cybercrime Convention, opened for signature in 2022, Is an landmark instrument for these purposes. The Additional Protocol looks to ensure that national authorities, prosecutors, and investigators have the tools to preserve and obtain electronic evidence, and the means to co-operate with the private sector.

Finally, several key recommendations for overcoming challenges in this area were presented. Improving the technical skills and resources for law enforcement agencies remains a key priority for many States, as there need to be wider capacities to request and share e-evidence across borders. In terms of improving requests to private sector companies, law enforcement agencies were also encouraged to adopt a flexible online investigation approach but also to use standardised templates to ensure that an initial request is as complete as possible. Several recommendations were also made for internet service providers. For example, it was suggested that they assess whether new products or services may present particular challenges for the purposes of electronic evidence.

Session IV: Livestreamed terrorism: detecting and suppressing attacks in real-time

During the fourth session, the discussion centred around the challenges related to live-streamed terrorist attacks and the ways to quickly reduce the spread of these live-streamed incidents across the internet.

It was recognised that terrorist threats in the online landscape are transnational, overlap in violent extremist ideologies, and take place across multiple platforms. Livestreamed terrorism can be viewed as a very modern expression of the "propaganda of the deed", a virtual demonstration of terrorism that can immediately reach global audiences and thus have a profound impact.

While generally only a small number watch the initial livestreamed attack in real-time, a key issue is that the footage can be watched afterwards on a variety of different platforms. For instance, under 200 people watched the livestream of the Christchurch attack, but within the first 24 hours, the video was uploaded millions of times on different platforms.

As such, while it is worthwhile focusing on how to disrupt the livestream as quickly as possible, it is also crucial to prevent the spread of this type of content after the livestream has ended. However, aware of the current technical capacity to identify certain forms of content, the videos are often edited or adjusted in order to evade identification and content moderation, or otherwise linked to smaller platforms lacking any meaningful moderation.

Looking at technical solutions to tackle live-streamed attacks and to identify a livestream when it is happening, the session explored the Hash-Sharing Database operated by the Global Internet Forum to Counter-Terrorism (GIFCT), which collects "hashes", numerical representation of the original content (such as images, videos or documents), which can be used as a unique identifier for terrorist content. Hashes can thus enable tech companies to see whether that content is present or being shared on their particular platform, though this solution cannot capture all variations and edits to the initial content.

Beyond technical issues, a notable subculture has grown around the perpetrators of such attacks. Thus, beyond the initial livestream, other users cite and praise the attackers, using them as a means to spread propaganda. This phenomenon where people express admiration for notorious attackers has evolved as a significant vector for radicalisation and the glorification of terrorist violence.

Speakers highlighted the need for effective responses to livestreamed terrorism, stressing the need for better coordination and communication with smaller platforms. Effective crisis response protocols need to be in place to limit the reach of content before it is viewed by a high number of people. However, as the online environment is inherently tied to the offline environment, the importance of not placing the sole responsibility on social media and internet companies was also emphasised. It was highlighted that there is a need to encourage mainstream media to exercise responsible journalism and not directly share the content and avoid re-directing readers to other spaces where such content can be found.

Session V: Policy and regulatory approaches to terrorist abuse of new technologies

The fifth session focused on examining the current policy landscape aimed at preventing terrorists and violent extremists from abusing the platforms and technologies discussed throughout the Conference.

In recent years, there has been a wave of legislative developments with regard to countering the spread of terrorist content online. For instance, the European Union's Regulation (EU) 2021/784 on terrorist content online, which establishes rigorous new rules requiring online hosting service providers to remove flagged terrorist content within one hour, or the United Kingdom's Online Safety Act, which requires online platforms to take action against illegal or "harmful" content. As facing this fast-changing and complex legislative landscape can be particularly difficult for private sector companies and national authorities, this session explored initiatives particularly provided for smaller tech companies that may encounter challenges in this complicated area. Tech Against Terrorism's Online Regulation Series, a living handbook providing a

comprehensive overview of global online regulation, was presented as an important repository of key developments in these areas.

At the global level, the session also looked at some of the work being done by the United Nations through the Security Council and Counter-terrorism Executive Directorate (CTED). It was noted that the latest review of the United Nations Global Counter-Terrorism Strategy included new references to the abuse of technology for terrorist purposes, encouraging Member States to prevent the online space from becoming a safe haven for terrorists. Among other important initiatives at the level of the UN, sanctions lists remain a key component in the UN policy framework against terrorism. These lists provide public authorities and private companies with the legal basis to prevent and block listed terrorist groups from accessing certain ICT services, procuring new technologies, and more broadly from abusing information and communication technologies for terrorist purposes.

The session also explored one of the key problems in the legislative and regulatory space which stems from a lack of clarity around the definition of terrorist content and that some lawful content is also being removed. This can present significant freedom of expression issues. This type of content is often referred to as "legal but harmful" or "borderline content", in other words material which is not necessarily breaking the law, but may lead to radicalisation to terrorism. This type of content is often created in a way that makes it difficult for moderators or automated moderation tools to identify and remove.

The session closed with recommendations on further action. For instance, building risk assessments and ensuring that there are cross-jurisdictional standards for content moderation was seen as crucial. Additionally, as new legislation and regulation comes into place, States were encouraged to regularly evaluate and review the practical implementation to ensure that they are effective, proportional and in line with applicable human rights standards.

Session VI: P/CVE, Youth and Gender: Building safe and reliable entertainment spaces free from violent extremism and terrorism

The last session of the Conference discussed the importance of preventing and countering violent extremism (P/CVE) in relation to young individuals at risk of being drawn into violent extremism conducive to terrorism.

Children and young people increasingly engage in virtual play, with research demonstrating that nine out of ten children now play video games, often starting from a very young age. There are a lot of positive aspects to this development, particularly as video games can provide young people with the ability to play with friends and others across cultures and borders online in a way that traditional forms of play never could. Speakers thus highlighted that games can be used as a way to foster more inclusive communities. For instance, some video games provide young people with opportunities to learn history or promote cultural understanding, which can be a welcome factor in building resilience to violent extremism and terrorism. There are also some notable positive trends in the content of video games in recent years, with more diverse female characters and characters of different ethnic, religious and cultural backgrounds, for example.

However, panellists also discussed some of the required improvements in this area, with several speakers noting that online extremism can be a highly gendered issue. Harmful ideologies such as extreme misogyny have long been prevalent in the gaming community itself. However, several reports highlighted that online expressions of misogyny accelerated during the COVID-19 pandemic, which is often combined or associated with other highly problematic issues such as antisemitism, racism and the spread of conspiracy theories. With nearly half of the gaming community identifying as women, preventing the spread of these damaging ideologies has only become more important.

Furthermore, the panel discussed the potential to raise the critical thinking skills and media literacy of young people and children. Speakers presented initiatives aimed at empowering young people and encouraging them to take an active role in identifying and watching out for the signs of terrorism and extremism. For instance, Hedayah's "Tech2Protect" programme demonstrated the use of technology to enhance a culture of peace and prevent extremism. In this programme, young people received training and were provided with a safe space to think of solutions to counter extremist content online.

Panellists emphasised the importance of raising awareness among key stakeholders, such as parents and social workers, on the way young people online spaces. It was noted that it can be crucial for them to

understand how entertainment in the online world works, particularly as many online subcultures can be very opaque and confusing for those not immersed in the language and imagery. To address the harmful ideologies and narratives in the gaming community, there is a need to build shared frameworks to address these issues among governments, civil society groups, educational institutions and the companies operating such gaming services and platforms.

Key Takeaways from the Conference

The Conference covered a wide array of interrelated topics in what is a complex, challenging and changing area. A few key takeaways can be extracted to help guide further Council of Europe action and events in these areas:

- Terrorist groups have long shown the ability to adapt to emerging technology, adjusting their tactics as new capabilities enable them to spread their ideologies to a variety of target audiences. The Conference stressed the importance of understanding and countering terrorist and violent extremist abuse of new and emerging technologies for the purposes of spreading their violent ideologies or providing operational support to attacks. While recent legislation, policies and initiatives have helped to mitigate many aspects of this phenomenon, there remain many challenges and threats in these areas.

- To specifically counter the issue of violent extremism and terrorism on gaming services and gaming-adjacent platforms, there is a need for deeper cooperation between public authorities, law enforcement, game developers and publishers, including internet service providers. Such cooperation is not only necessary with regard to the prevention of terrorist abuse of online services, but also in raising awareness of the nature and prevalence of online threats, as well as improving response tools such as the sharing of e-evidence.

- Increased attention needs to be given to medium- and smaller-sized platforms, as these platforms often have minimal to no moderation protocols and practices, resulting in extremists operating in relative safety and anonymity. For instance, while disrupting the initial livestreaming of terrorist attacks is critical, action should also be taken to limit the spread of such footage to other, smaller platforms.

- While there have been significant positive changes in the wider video game industry and content of video games themselves, harmful ideologies such as misogyny, toxic masculinity, and racist attitudes and behaviours are still heavily present in the gaming community. As these ideologies can foster toxic online cultures that tolerate or can even lead to violent extremism, enhancing understanding of such ideologies among governments, law enforcement and educational institutions, among others, is needed.

- Preventive measures are crucial, particularly to build resilience among younger people who spend large amounts of time online. While there may be a need for improved awareness of the gaming-terror nexus, there is also the potential positive role video games could play in educating gamers on violent extremism and terrorism. P/CVE action

could take this into account in the design and implementation of their programmes, potentially boosting reach and resonance with their target audience.

- A primary feature of online gaming is the social aspect, as platforms can foster a sense of community and belonging. As such, the Conference also highlighted the potential to empower gamers and internet users, as they are often in a suitable position to address extremism in their community. However, this is contingent on the development of suitable reporting functions, content moderation policies and other initiatives to prevent extremist from proliferating on gaming-related services.

- The challenge of balancing respect for human rights and safety and security online should also be carefully considered. Effective safeguards should be developed to tackle terrorist content online, while simultaneously, securing a free and open internet for legitimate users. This is particularly relevant in the context of content moderation policies with regards to "borderline content", considering the current lack of definition clarity on many services as to what constitutes terrorist content. States and service providers should ensure respect for human rights when implementing counter-terrorism actions in the online landscape, particularly when it comes to freedom of expression issues around content that may be objectionable but is otherwise lawful.