European Commission

EUIF YEAR IN REVIEW 2022

EU Internet Forum

Joining forces against illegal content

OUTLINE

INTRODUCTION

From Christchurch to Bratislava, we have seen how **online extremism** can spill over into **real world violence**. Online communication technologies have made it easier for terrorists and violent extremists to communicate across borders and have amplified terrorist propaganda and the spread of extremism. The terrorism threat landscape continues to evolve as extremists **adapt their tactics** and use of online tools to **amplify their reach** and **evade detection** by law enforcement.

Below is an overview of some of the current threats when it comes to how extremist individuals and networks are using the online space to radicalise. As the threats evolve, the response of policy makers, internet companies, and law enforcement must also evolve to combat the actors of today. The **EU Internet Forum** is working proactively with its partners to stop terrorists from using the internet to radicalise, recruit and incite to violence.

EU Internet Forum

The EU Internet Forum (EUIF) was launched in 2015 by the European Commission to address the misuse of the internet by malicious actors. As of 2019, the forum is also addressing Child Sexual Abuse online and is now starting to look at the use of the internet for drug traffic and trafficking of human beings.

Chaired by the European Commission, the EUIF provides a collaborative environment for governments in the EU and EFTA, law enforcement, the internet industry, civil society, academia, and other members, to discuss and address the challenges of malicious and illegal online content.

The main strands of action of the EUIF are:

- Reducing accessibility to **terrorist and violent extremist online content**
- Increasing effective counter and **alternative narratives** online
- Enhancing the **fight against child sexual abuse** and exploitation online

In 2022 the EUIF has also addressed at technical level challenges related to the **sale of drugs** and **trafficking of human beings online.**

THE THREAT LANDSCAPE

ALGORITHMIC AMPLIFICATION

Extremist content continues to be shared via major **social media platforms**, **search engine results**, and other **digital platforms** despite measures to prevent the spread of violent content online. The **recommender systems** that power social media platforms - the software that decides what content users will see and when they see it - as well as design features of platforms, can be exploited to spread terrorist and violent extremist content and promote extremist views through the spread of borderline content.[1]

Algorithms that provide a tailored and more structured user experience online by recommending content, sometimes **unintendedly amplify** both violent extremist and borderline content. For example, malicious actors may insert extremist propaganda in the middle of seemingly benign content to evade detection or use **alternative keywords**, bypassing existing measures to counter violent content online, thus entailing algorithmic amplification. Extremists can also gain visibility by tricking a platform's algorithm with **fake followers**.[2] Unintentional algorithmic amplification occurs when searches on a topic lead users to other more extreme content being recommended by the platform's algorithm.

Controlling the spread of extremist and fringe content is increasingly challenging. This is due to the **lack of common threshold and definitions**, as well as to **limited guidance from regulators** when it comes to legal but potentially harmful content (see box below on borderline content). Content moderation alone is not sufficient, but clearer and more **consistent content moderation guidelines** and common definitions would ensure smooth cooperation between public sector, private sector, and civil society.

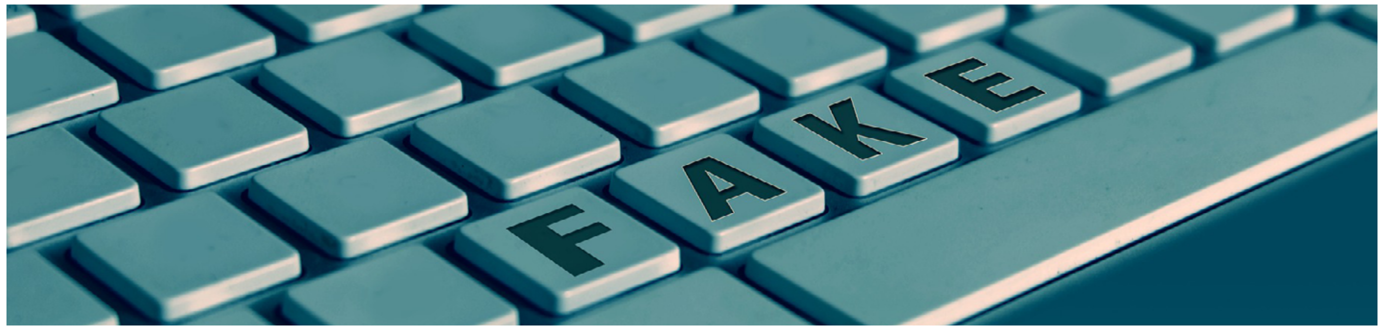
[1] RAN Policy Support, Consolidated Overview, 'Malign Use of Algorithmic Amplification of Terrorist and Violent Extremist Content: Risks and Countermeasures' (2021)
[2] Recommended Reading: Amazon's algorithms, conspiracy theories and extremist literature (2021) Institute for Strategic Dialogue

BORDERLINE CONTENT

Borderline content, also known as **harmful but legal content**, is content that comes close to infringing on the community guidelines[3] of social media platforms or laws regulating online illegal content. It is usually a combination of **disinformation/conspiracy theories** and **hate speech**. In other words, content that is considered inappropriate in the public debate but does not exceed the barriers of free speech and is not illegal.

If an expression of opinion is not illegal but is categorised as 'borderline' this means it **is very close to being illegal**, but it is not. YouTube, for instance, defined borderline content as "videos that don't quite cross the line of our policies for removal but that we don't necessarily want to recommend to people".[4] Some of the **most common types of borderline content** identified in the EU are anti-establishment/anti-institutions, antisemitic, anti-trans, misogynistic, anti-migrants, racist, or against COVID-19 measures.

'Safety by design'[5] measures have been identified as ways to prevent the spread of borderline content via automated systems. A focus on content is not enough and **preventative measures** must consider **behavioural patterns** and **propagation tactics** used by malicious actors, including manipulation. Responses to the spread of borderline content and preventative measures to consider include **digital and media literacy**, **critical thinking** and **democracy-strengthening programs** to foster **resilience**.



[3] Private rules drafted and enforced by the social media platforms
[4] https://blog.youtube/inside-youtube/inside-responsibility-whats-next-on-our-misinfo-efforts/
[5] Safety by design focuses on the ways technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur.

TERRORIST OPERATED WEBSITES

Following the entry into application of the Terrorist Content Online Regulation (TCO)[6] which requires hosting service providers to remove or disable access to terrorist content, there is a resurgence in the use of terrorist operated websites (TOWs). While these websites can be used to **share information** and keep **archives of old content**, they can also be used for **recruitment**, **radicalisation** and **raising funds**. They can be operated by terrorists (designated entities) or run as support or fan sites.

Terrorist operated websites pose several challenges. Firstly, unlike social media platforms they are **not subject to content moderation**, it can be hard to detect extremist content, and there is a lack of expertise to determine which content is violent extremist or terrorist. Moreover, these websites can easily be found online, and they give a sense of legitimacy and authority to terrorist content. On the legislative front, companies often **lack a legal basis to remove TOWs**. In addition, legislation and processes vary from one Member State to the other and there is limited indication on the designation of entities as terrorist organisations. Another challenge is terrorist actors applying different measures to circumvent the takedown of these websites, including **domain name hopping**, **redirection** and creation of **back-up domains**.[7] Moreover, infrastructure providers must gather the **evidence base** proving that a website is operated by a terrorist or violent extremist organisation, and they must manage the efficient and long-term removal of the website while ensuring that freedom of speech is respected. Other more operational challenges identified by infrastructure providers include: a lack of knowledge about **contact points in law enforcement and industry** as well as appropriate channels to flag terrorist operated websites and difficulties in **identifying the owner of such a website**.

[6] Terrorist Content Online Regulation (TCO)
[7] Maura Conway and Seán Looney. 2021. Year in Review (Brussels: RAN Policy Support)

FINANCING ACTIVITIES ONLINE

In recent years, extremists and violent extremist groups across the whole ideological spectrum have been using the internet to **fundraise through social media platforms and websites**. Activities online include **soliciting donations** and **selling merchandise**, with and without the use of cryptocurrencies. Across the EU, **individual donations** remain one of the primary means of funding for terrorist and violent extremist organisations, often not covered by **traditional counter terrorism measures**. These fundraising activities are not always illegal, and the **boundaries between activism, extremism and terrorism** are blurred, but they contribute to **spreading ideologies** and radicalising. With the increased availability of **crowdfunding websites**, there are new opportunities to reach large numbers of donors and raise larger amounts of money.[8] Some right-wing groups known to raise funds through physical events have also **shifted to online methods for funding**, including crowdfunding.

While it is currently unclear what the full picture of the scale is, extremists and terrorists, including extreme right-wing users and groups, are using **cryptocurrency** and virtual assets service providers (VASPs). Bitcoin and Monero appear to be the most common forms of cryptocurrencies used by right-wing extremists, especially those concerned with being de-platformed from sites using traditional payment processors.

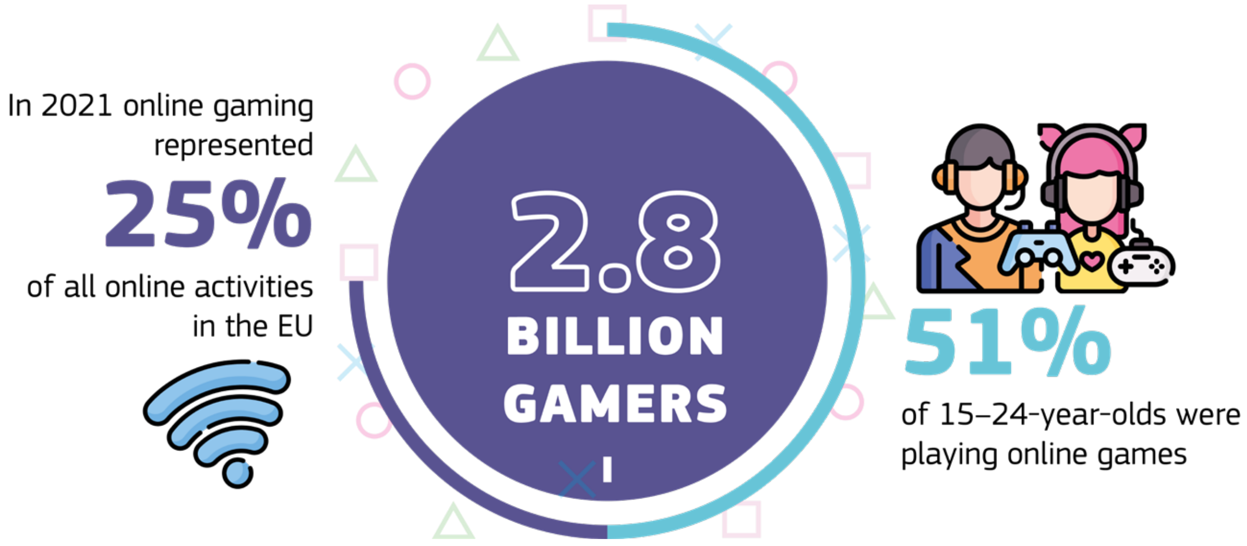
The potential for misuse of non-fungible tokens, or **NFTs**, is of concern, as they may be used by illicit actors to circumvent sanctions and to launder the proceeds of criminal activities. NFTs have been minted by conspiracy theorists, as NFTs have **increased in popularity as an art-form and commodity** amongst the wider public. According to think-tank the Soufan Centre, last September a pro-ISIS supporter minted an NFT that glorified an Islamic State Khorasan (IS-K) attack in Afghanistan, making it the second U.S. designated terrorist group to **experiment with NFTs**, along with the Russian Imperial Movement (RIM).[9]

[8] Maura Conway and Seán Looney. 2021. Year in Review (Brussels: RAN Policy Support)
[9] https://thesoufancenter.org/intelbrief-2022-september-16/

VIDEO GAMING

It is estimated that there are over **2.8 billion online gamers worldwide**. One of the draws of online gaming is that it allows players around the world to play and interact with each other. This can be done through **adjacent communications platforms** that have been specifically designed for gaming, such as Steam, Twitch, Discord, and DLive.[10] Online gaming can have many **positive social benefits**, and for some has been an essential outlet, especially during times of social isolation due to the COVID-19 pandemic. But the **connectivity** offered by gaming and adjacent communication platforms also brings **risks**, such as the **potential exposure to extremist content, hate speech and radicalisation**.

Due to the sheer size of the online gaming community, there is inevitably an **overlap between radicalised individuals and those who play video games** and mix with others through gaming (adjacent) platforms. While there is **no current evidence for a causal link** between enjoying video games and becoming radicalised, we can find radicalised individuals on these platforms who express their ideological beliefs while communicating with others.[11] The **lack of sufficient moderation** and **pushback of violent ideologies** on these platforms can lead radicalised individuals to feel supported in their views and emboldened to take action. Challenges to moderation include the **difficulties in moderating audio-visual live streams** and moderating in **languages other than English**. Violent extremist and terrorist actors also strategically exploit this space to target children vulnerable to harmful content. For these reasons, it is important for the gaming communities to be involved in creating safe spaces for users.



In 2021 online gaming represented **25%** of all online activities in the EU

2.8 BILLION GAMERS

51% of 15–24-year-olds were playing online games

[10] RAN Policy Support, Research, 'Video Gaming and (Violent) Extremism: An Exploration of the Current Landscape, Trends and Threats', 2021

[11] Ibid

INCEL VIOLENCE & VIOLENT MISOGYNY

Incels, or 'involuntary celibates' continue to be an **online subculture** or online community of interest to policy makers. Incels have been described as mostly male, white, and heterosexual and their views are characterised by frustration over sexual rejection and **hatred of women** whom they blame for their own inability to form sexual relationships.[12] Some self-identifying incels share **deeply misogynistic content promoting violence against women** on platforms such as Reddit, Twitch, Discord and others. Some within the incel community become radicalised online through the **high volumes of extreme content** they consume. In 2020 in Hanau, Germany, a 43-year-old German man shot and killed ten people at two shisha bars. A confession letter and manifesto shared by the Hanau shooter promoted various conspiracy theories, contained hate speech against migrants, and misogynistic and **male supremacist** messages. Another example of incel violence was the Plymouth shooting in the UK in 2021, where Jake Davison, a frequent contributor to incel forums, shot and killed five people and injured two others before fatally shooting himself. The 22-year-old expressed misogynistic and homophobic views through **video content uploaded to incel forums**, portraying himself as a man in despair who raged against his mother and his failure to find a girlfriend.

There are multiple **crossovers between** the incel ideology and other hateful ideologies and views, such as misogyny, racism, harmful conspiracy theories, the endorsement of violence, and the far-right. Two key indicators for involvement in the incel community are **isolation** and **spending a lot of time online**. There is a risk that we will see increased membership of this community and **increased potential for violence** as a result. According to research by the Center for Countering Digital Hate which analysed the most influential and largest incel forum over an 18-month period, the study found a 59% increase in mentions of mass attacks, widespread approval of sexual violence against women, with 9 in 10 posters expressing support for paedophilia.

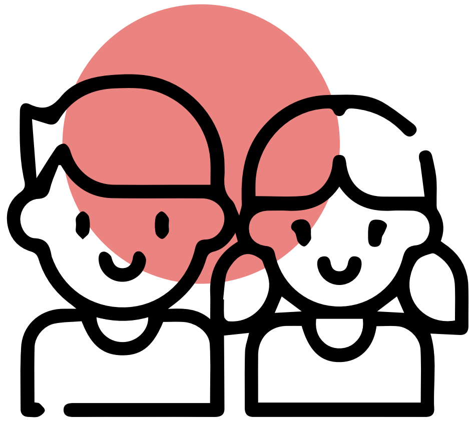
[12] https://www.theguardian.com/tv-and-radio/2022/nov/07/the-ultimate-enemy-is-women-the-secret-world-of-incels

RUSSIAN AGGRESSION AGAINST UKRAINE

Violent extremist content related to **recruitment and fundraising** in the context of the Russian aggression against Ukraine has been identified by law enforcement, internet companies and Member States as a current challenge in the online space. The internet is also being used for radicalisation purposes through the use of **propaganda and disinformation**. Russia has in fact been preparing the information battleground for years prior to its attack in February this year.[13]

The EU Internet Forum is addressing the spread of violent extremist online content related to the current Russian war of aggression against Ukraine. A panel in the June Senior Officials meeting was dedicated to sharing knowledge about 2022 EUIF right-wing extremist (RWE) content spread by both pro-Ukraine factions and pro-Kremlin mercenaries or other Russian forces. Pro-Russia RWE groups identified include white supremacist group Russian Imperial Movement, Russian right-wing paramilitary organization Wagner Group, Neo-Nazi group DSHrG Rusich. Pro-Ukraine right-wing groups include Azov Battalion, Wotanjugend, Right Secto. **Russian private military companies** are openly **recruiting and fundraising** on social media platforms. Some internet companies have established **moderation teams** dedicated to moderating content related to the war, some are **removing graphic content**, and using **warning labels** about **fact-checking**.[14] Member States neighbouring Ukraine are concerned about **anti-establishment movements** being fuelled by **pro-Kremlin actors** and the potential for violent actions against governments.

[13] EUvsDisinfo
[14] https://therecord.media/how-ukraine-is-forcing-companies-to-rethink-content-moderation/



VULNERABILITY OF CHILDREN

There has been a dramatic increase in detected cases of **child sexual abuse** in recent years, and the EU is committed to stepping up global efforts to tackle these heinous crimes. But children are facing other threats online, such as the spread of violent extremist content that can lead them to being radicalised or to normalising the concept of violence. Europol's TESAT 2021 and 2022 refer to the decrease in the ages of suspects involved in law enforcement investigations and of those participating in right-wing online communities. Gaming platforms and gaming communication services popular among young people and children are used for spreading right-wing terrorist and extremist propaganda.[15] Europol reports international networks of individuals on the internet, mostly adhering to siege culture and accelerationist ideas, which concern predominantly very young males, as young as twelve years old.[16]

[15] Europol Terrorism Situation and Trend report, TESAT, 2022, p. 44
[16] Europol Terrorism Situation and Trend report, TESAT, 2022, p. 52

UPDATES ON EUIF RESPONSE

KNOWLEDGE PACKAGE OF VIOLENT EXTREMIST GROUPS, SYMBOLS AND MANIFESTOS

The Knowledge Package consists of **lists of groups, symbols and manifestos** that are banned or proscribed under Member States' national law. These lists are **updated every year** by Member States and Europol and are complemented by **assessments** provided by trusted **researchers**. The first edition of the Knowledge Package was released in November 2021 and presented at the EUIF Senior Officials meeting on 16 November 2021. Information provided by Member States has been consolidated and the Knowledge Package has been inputted into a **protected database** to make it easier to search through.

The Commission is in the process of preparing the **second edition** of the Knowledge Package to be released in 2023, having gathered **inputs from Member States and Europol** which will be complemented with recent research. Feedback on the knowledge package found that it was a useful reference for **evaluating legal removals of content** related to violent extremism. It was also suggested to add **online financing of terrorist groups** through sales of **merchandising containing right-wing extremist symbols** to the knowledge package.

HANDBOOK ON BORDERLINE CONTENT

The establishment of the Handbook on Borderline Content was agreed during the Workshop on Algorithmic Amplification and Borderline Content organised by the EUIF on 29 September. The handbook gathers inputs from participants of the workshop on **working definitions** of borderline content, **case studies**, **concrete examples of borderline content** leading to radicalisation, and **existing policies** to prevent the spread and amplification of such content. **Contributors** to the handbook include GIFCT, Tech Against Terrorism, EU Observatory of Online Hate Speech, several EU Member States, researchers, and the European External Action Services (EEAS) Strategic Communications division.

EU Internet Forum

THE HANDBOOK OF BORDERLINE CONTENT

Existing policy, definitions and preventive measures to identify legal but harmful content leading towards radicalisation

European Commission

HANDBOOK ON VIDEO GAMING

Following the EUIF meeting on video gaming held in October 2021, the EUIF has developed a handbook to provid**e guidance to companie**s on how to empower their users to **identify, report and counter harmful content** on their platforms.

The first part of the handbook introduces **inspiring practices** from **civil society** that empower users, informs about **potential areas of collaboration** between P/CVE actors and companies, and discusses **different types of cooperation** that can be beneficial to all. It contains **six key recommendations** for the tech industry. In addition, it includes **contact details** for the **different initiatives** to enable companies to reach out to organisations and find out more about an initiative or to explore potential collaboration. This part of the handbook was produced by Radicalisation Awareness Network (RAN) Practitioners and is publicly available on the RAN Practitioners webpage.

The second part contains **best practices from the industry.** This section contains information on ways to **raise awareness, reporting mechanisms, content moderation provisions,** and actions to counter violent extremist and terrorist **narratives.** It also includes information on existing collaboration with civil society organisations, **evaluation measures** and **findings,** as well as information on **follow-up support** for users after being exposed to harmful content. This second section of the handbook is only accessible to EUIF members and not publicly available.

EU Internet Forum

Countering the misuse of gaming related content & spaces

Inspiring practices from and for tech companies to empower their gaming communities

CRISIS COMMUNICATIONS GUIDELINES

Crisis communication is the use of communications to **engage with audiences affected by the crisis**, including local communities, minority communities, and the public. Proactive communication during a crisis is essential and should be **prepared** for in a **strategic manner**. In May 2022, the EUIF held an **exercise for Member States on crisis communication** in the aftermath of a terrorist attack. The exercise was delivered by the Radicalisation Awareness Network (RAN) Policy Support and attended by representatives from 22 Member States. The exercise was designed to give participants a better understanding of the **use and impact of communications** in the **aftermath of a terrorist attack** and focused on five different communication responses: the 'government response', 'security response', 'terrorist response', 'technology response' and 'community response'.

Following the outcome of the exercise, a set of **Communications Guidelines** were developed, elaborating **guiding strategic principles for Member States** to consider when developing and executing a crisis communications response. When combined, these recommendations represent the foundation of a comprehensive crisis communications response. The EUIF in collaboration with the EU Internet Referral Unit (EU IRU) also developed a **template** for companies to **notify an imminent threat to life**, as required by Article 14(5) in the Terrorist Content Online Regulation (TCO) Regulation.

STUDY ON ALGORITHMIC AMPLIFICATION

The EUIF has commissioned a *study on the impact of algorithmic amplification on the user's journey towards radicalisation*, launched in August 2022, looking into the **effects of algorithmic amplification** on the process of online radicalisation. The study is examining the degree to which social media platform machine-learning-based content delivery systems **amplify terrorist and violent extremist content**. It will consider what impact the **automatic dissemination** of such content has on the user's journey towards radicalisation, also assessing to what extent the machine-learning-based content delivery systems amplify borderline content such as **legal hate speech**, **disinformation** and other forms of legal but harmful content that can lead to radicalisation. The main objective of this study is to be able to show empirically the extent to which machine-learning-based **recommendation algorithms** lead to the creation of online "echo chambers" or "filter bubbles" of terrorist content, and the impact that this might have in the adoption of violent extremist beliefs and ideologies. Preliminary results of the study will be shared at the beginning of 2023 and **final results in Spring 2023**.

RAN POLICY SUPPORT STRATEGIC COMMUNICATIONS WORKSHOPS

RAN Policy Support held a Strategic Communications meeting in June on the *exploitation of technology by radicalising forces and creating an agile response to technological change*. Representatives from 14 Member States heard six presentations, an intervention and a keynote speech on the **emerging technological threats** predicted to have an impact on terrorist and violent extremists' ability to influence and recruit digitally in Europe. This was followed by a workshop in November on the **misuse of the virtual space by violent extremists**, following feedback from Member States to learn more about how virtual spaces are used by violent actors, and **new and emerging trends in online activity** of radical Islamists and violent right-wing extremists. Some concrete solutions that were proposed during the workshop included introducing standards for content moderation of new tech platforms (i.e., for virtual reality and the metaverse) and developing a comprehensive school curriculum, including digital literacy, to equip audiences with adequate skills to discern malign content online

THE CIVIL SOCIETY EMPOWERMENT PROGRAMME (CSEP)

The Civil Society Empowerment Programme (CSEP) was launched in 2015 to **support and empower civil society**, grass roots organisations and provide effective narrative alternatives to radicalisation online. Many civil society organisations were already active in providing **alternative narratives** and **supporting credible voices**, but they often lacked the capacity and/or resources to produce and disseminate these messages effectively online. Through the CSEP, the EU has engaged in **capacity building**, **training**, partnering civil society organisations with internet and social media companies, and **supporting campaigns** designed to reach **vulnerable individuals** and those **at risk of radicalisation** and recruitment by extremists. This programme came to an end in 2022 and an **evaluation of the impact and effectiveness** of counter- and alternative campaigns stemming from the CSEP programme is underway.

ADDRESSING TERRORIST OPERATED WEBSITES (TOWS)

During the EUIF technical meeting in March 2022, the need to address Terrorist Operated Websites (TOWs) was identified as one of the priorities of the EU Internet Forum in 2022. As mentioned above in the section on TOWs, challenges identified by law enforcement and internet providers include a **lack of knowledge** about **contact points and appropriate channels** in law enforcement and industry to **swiftly flag or refer TOWs**, and a lack of standardised reporting processes and responses to referrals. In response to this, the EUIF has set up a **Directory of Contact Points** for law enforcement and industry partners to facilitate swift and easy communication to remove TOWs.

In close consultation with industry and law enforcement, the EUIF has also developed a **Flow of Information Chart** for the industry, outlining the different steps to be taken when referring or flagging a TOW. This Chart includes guidance on what information law enforcement need to react to the flagging or the reporting of a TOW, and what follow-up action can be expected.

UPDATES IN GLOBAL COOPERATION

GIFCT
Global Internet Forum to Counter Terrorism

The European Commission has been active in three GIFCT working groups on 1) **algorithmic amplification**, 2) **transparency** and 3) **crisis response**. The Commission was also represented at the 2022 GIFCT Summit in July and presented the EU approach to crisis response, including the EU Crisis Protocol, recent activities, and legal obligations for tech companies to respond to imminent threat to life.

The Commission is also part of the **Independent Advisory Committee** of the GIFCT. The IAC is composed of Government and Civil Society representatives and was set up to provide strategic advice and directional input to the GIFCT.

GIFCT is also **actively involved in the EU Internet Forum** and has contributed to several meetings in 2022, including the *Crisis Communication exercise* in May, and the *technical workshop on algorithmic amplification and borderline content* in September.

CHRISTCHURCH CALL
TO ELIMINATE TERRORIST & VIOLENT EXTREMIST CONTENT ONLINE

The Christchurch Call is a community of over 120 governments, online service providers and civil society organisations acting together to eliminate terrorist and violent extremist content online. The Commission has been a **member of the Christchurch Call to Action** since its **foundation in 2019**. It ensures close cooperation and synergies with the EU Internet Forum. The Commission is also a member of the **Workstream on Crisis Response**.

European Commission **President Ursula von der Leyen** joined the 2022 Summit held in New York in September. She stressed the importance of addressing threats and challenges related to the **spread of borderline content**, and the need to implement stronger measures to **prevent the use of recommender systems** to amplify TVEC and borderline content, especially among children. She also highlighted the need to further develop **international cooperation on crisis response**.

SOURCES

- RAN Policy Support, Consolidated Overview, ‘Malign Use of Algorithmic Amplification of Terrorist and Violent Extremist Content: Risks and Countermeasures’ (2021)
- RAN Policy Support, Consolidated Overview, ‘Back to the Future? Twenty First Century Extremist and Terrorist Websites (2021)
- RAN Policy Support, Research, ‘Video Gaming and (Violent) Extremism: An Exploration of the Current Landscape, Trends and Threats’, 2021
- Europol Terrorism Situation and Trend report, TESAT, 2022
- Recommended Reading: Amazon’s algorithms, conspiracy theories and extremist literature (2021) Institute for Strategic Dialogue
- Europol ‘Policing in the metaverse: what law enforcement needs to know’, an observatory report from the Europol lab (2022)
- Maura Conway and Seán Looney. 2021. Year in Review (Brussels: RAN Policy Support)
- Extremist and Terrorist Websites (Brussels: RAN Policy Support)
- Michael Jacobson. 2010. ‘Terrorist Financing and the Internet.’ Studies in Conflict & Terrorism
- Stephane Baele, Lewys Brace, and Travis Coan. 2019. ‘From “Incel” to “Saint”: Analyzing the Violent Worldview Behind the 2018 Toronto Attack.’ Terrorism and Political Violence
- Lewys Brace. ‘A Short Introduction to The Involuntary Celibate Sub-Culture.’ CREST, 26 August 2021:
- Isabelle van der Vegt, Paul Gill, Stuart Macdonald and Bennett Kleinberg, ‘Shedding Light on Terrorist and Extremist Content Removal’, Special Resources, 3 July 2019,
- EUvsDisinfo