EU Internet Forum at 10 YEARS:

European Commission

Celebrating the achievements of the first decade's cooperation to fight harmful and illegal content online

EU Internet Forum

Joining forces against illegal content

Outline

01. Introduction

The EU Internet Forum (EUIF) is approaching its ten-year anniversary. Its beginnings were marked by the rise in **ISIS propaganda online.** The idea underpinning the EUIF was to reach a **joint, voluntary approach** based on a **public-private partnership** to detect and address harmful material online. Since then, technological developments have brought about new opportunities but also challenges. Times and times again, we have seen how **online terrorism and extremism can spill over into real-world violence**, how online service providers can be exploited for **terrorist and violent extremist purposes,** spread and manufacture child sexual abuse material, or for **drug trafficking and trafficking in human beings.**

In less than 10 years, we have jointly transformed the previously scarce coordinated voluntary or legal response to online harms into **a robust mechanism**. With input from the EUIF, we strengthened a legislative framework in the EU addressing online harms with the Digital Service Act (DSA) and sectorial legislation. The **EU Internet Forum serves as a unique, voluntary and complementary platform,** bringing stakeholders from all corners of society together with different expertise and covering multiple kinds of online harms. We proactively work towards stopping terrorists, violent extremists, child abusers, human traffickers, drug traffickers, and other malicious actors from exploiting the Internet. The EUIF has delivered **concrete outcomes and guidance** for its members and has been **pivotal in establishing contacts and strengthening collaboration** among industry and law enforcement, as well as with other adjacent industries that play a role in preventing malicious activities online, such as internet infrastructure providers and financial service providers.

In that sense, the work of the EUIF is an undeniable example to how **cooperating together can bring about positive change,** establish **new partnerships, exchange experience,** and jointly address and help eradicate some of the most awful content online. The EUIF also proved how quickly it can **mobilise different stakeholders and develop joint responses**, such as in connection to Russian aggression against Ukraine or content online related to the 7 October 2023 attack and the Israel/Hamas conflict. It has also proven to be a **key player at international level** and is appreciated by third countries and other global initiatives. Additionally, the discussions in the EUIF advising on policy developments also contributed to the fact that the EU led the way with relevant **horizontal and sectoral legislations** and developing new structures, such as Europol's EU Internet Referral Unit.[1]

On the brink of the anniversary of the first decade of its work, this brochure provides an **overview of the EUIF's work**, the **current work strands**, and the **key actions and outputs** that have been taken by the EUIF to tackle threats in the digital spaces.

[1] EU Internet Referral Unit - EU IRU | Europol (europa.eu)

02. The EU Internet Forum

The EUIF was launched by the European Commission in December **2015** to address the misuse of the internet for terrorist purposes through two main strands of action:

1. reducing accessibility to **terrorist content online** and
2. increasing the volume of effective **alternative narratives online.**

The **objective** of the EUIF is to provide a collaborative environment for governments in the EU, their law enforcement authorities, the internet industry, and other partners to discuss and address the challenges posed by the presence of malicious and illegal content online on a voluntary basis. It is complementary to regulatory efforts undertaken at EU level such as the Terrorist Content Online Regulation[2], Digital Services Act[3], the Interim Regulation to combat online child sexual abuse (CSA)[4] and other legislative instruments proposed by the Commission, notably the long-term Regulation to prevent and combat CSA[5] and the Recast of the 2011 CSA Directive[6]. In addition, the newly amended Anti-trafficking Directive[7] also specifically addresses the online dimension of the crime.

In parallel and with the EUIF's involvement, the **EU Internet Referral Unit** was launched in Europol to detect and investigate malicious content on the Internet and in social media, which produces both strategic insights, but also provides information for use in criminal investigations.

In 2019, the EUIF expanded its area of activity to enhancing **the fight against child sexual abuse online**.

In 2022, the Forum's activities were further extended to tackle **trafficking of human beings and the prevention of drug trafficking.**

The EUIF addresses the different challenges via **technical meetings** and **workshops**, takes stock of its achievements (bi-)annual **Senior Official Meetings** and decides on its political steer in the annual **Ministerial Meeting**, chaired by the Commissioner for Home Affairs.

[2] https://eur-lex.europa.eu/eli/reg/2021/784/oj
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1731332492900
[4] EUR-Lex - 52023PC0777 - EN - EUR-Lex
[5] EUR-Lex - 52022PC0209 - EN - EUR-Lex
[6] EUR-Lex - 52024PC0060 - EN - EUR-Lex
[7] https://eur-lex.europa.eu/eli/dir/2024/1712

03. Membership

The EUIF is a multi-stakeholder Forum, chaired by the European Commission and brings together a wide range of institutions, organisations, and networks as active members. The membership grew significantly over the years to welcome new companies and civil society organisations (CSO) in order to respond to the exploitation of online services and different online harms.

The membership now includes:

- EU Member States and countries of the European Free Trade Agreement;
- European institutions and Agencies, such as Europol, Eurojust, the Fundamental Rights Agency, the European External Action Service, and the Council's Counter Terrorism Coordinator;
- Internet industry, including Amazon, Automattic, DailyMotion, Discord, Dropbox, Meta, MistralAI, Google, Internet Archive, Just Paste.it, Mega, Microsoft, Snap, Soundcloud, Telegram, Twitter, Twitch, Yubo, TikTok, Roblox and Zoom;
- The Global Internet Forum to Counter Terrorism;
- Tech Against Terrorism;
- The United Nations Office of Counter-Terrorism; United Nations Security Council Counter-Terrorism Committee;
- The EU Knowledge Hub on Prevention of Radicalisation (formerly the Radicalisation Awareness Network);
- Tech Coalition;
- Institute for Strategic Dialogue.

The EUIF also cooperates with non-members to address emerging exploitation holistically, as we have done for our workstreams on video-gaming, terrorist operated websites and TVE financing activities online.

04. Timeline

2015

The EUIF was officially launched[8] by the European Commissioner for Migration, Home Affairs and Citizenship, **Dimitris Avramopoulos** in cooperation with the Commissioner for Justice, Consumer and Gender Equality, **Věra Jourová** and the **Interior Ministers of the EU Member States** in December 2015.

The goal was to **transform the previously scarce structured voluntary cooperation,** to **protect the public from the spread of terrorist material, prevent terrorist activity online and use the Internet** to **challenge terrorist narratives and online hate speech.**

2016

The first official year of the EUIF focused on the implementation of the early tasks, such as focusing on **reducing the accessibility of terrorist content online, referrals, counter-narratives, hate speech,** and **empowering civil society partners.**

2017

Marked by several terrorist attacks in the EU the previous year, the EUIF continued focusing on r**educing the accessibility of terrorist content online, empowering civil society partners** to increase the volume of effective **alternative narratives online,** including via the **Civil Society Empowerment Programme** (CSEP).

2018

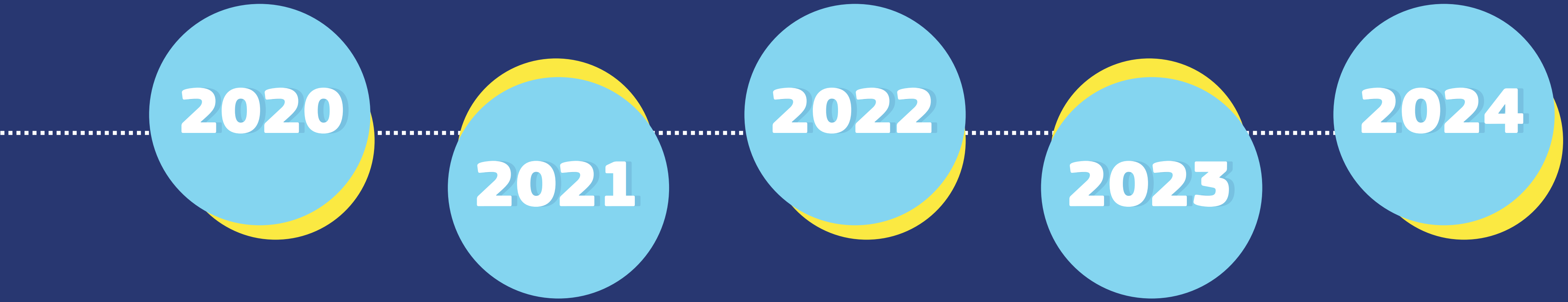
The EUIF conducted a first **reporting exercise** together with companies and states, increased its **outreach to small and new companies**, and focused on presenting and facilitating the **work for the TCO proposal.**[9]

2019

After the Christchurch terrorist attack in March 2019, the EUIF actively responded to the viral spread of terrorist and violent extremist content online by developing the **EU Crisis Protocol** (EUCP). **Alternative** and **counter-narratives** remained an area of interest, whilst identifying emerging challenges. **Child sexual abuse online** (CSA) for the first time featured on the agenda of the EUIF.

[8] EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online

[9] EUR-Lex - 52018PC0640 - EN - EUR-Lex (europa.eu)



2020

Challenges in addressing **violent right-wing extremist content online** continued to be an important topic. The **EUCP** was activated following the murder for French teacher Samuel Paty to prevent the dissemination of terrorist content online.

2021

The COVID-19 pandemic led to an increase in terrorist and violent extremist content (**TVEC**). The EUIF continued addressing **crisis response, violent right-wing extremism**, leading up to a development of the Knowledge Package, challenges in fighting **CSA** online, and examined **emerging challenges**, such as **algorithmic amplification** and **video-gaming.**

2022

The EUIF focused on developing evidence of **algorithmic amplification** together with **borderline content** and **violent extremism**, also looking into terrorist **financing activities online,** and **CSA**. The **Russian aggression against Ukraine** also influenced the work related to violent extremism. Additionally, the forum focused on **terrorist operated websites**.

2023

Preventing drug trafficking online and **trafficking in human beings** for the first time featured on the agenda of the EUIF. The EUIF continued its work on TVEC, including implementing the **TCO Regulation, algorithmic amplification, borderline content,** and **crisis response**. The EUIF also focused on the impact of the **7 October terrorist attacks** on the online threat landscape and changes in the modus operandi of terrorist and violent extremist actors online. Conversations on **CSA** continued in the EUIF.

2024

The EUIF focused on **generative artificial intelligence** (genAI), terrorist and violent extremist **financing activities online, drugs sales online,** and **CSA** – including the impact of end-to-end encryption (E2EE) on child safety online. It also conducted another tabletop exercise in **crisis response**, considering the situation in the Middle East and focused on the online/offline interplay of the threats. **Bystander footage** emerged as a new challenge. A Knowledge Package was also developed to help internet companies moderate drug trafficking content.

05. Terrorist and Violent Extremist Content Online

ALGORITHMIC AMPLIFICATION

Algorithms that provide a tailored and more structured user experience online by recommending content, sometimes can unintentionally amplify terrorist, violent extremist and borderline content or are intentionally exploited by malicious actors to disseminate their narratives. Thereby algorithmic recommender systems can potentially contribute to radicalisation. Malicious actors may use, for example, **alternative keywords** or **fake followers** to gain visibility. Controlling the spread of violent extremist and borderline content is increasingly challenging due to the **lack of common threshold and definitions**, as well as to **limited guidance from regulators** regarding borderline content.

EUIF Deliverable

The EU Internet Forum commissioned **a study**[10] on the **role and effects of algorithms in spreading terrorist, violent extremist and borderline content**, which was launched in August 2022 and the result shared in October 2023. The study examines the degree to which the five leading social media platforms in the EU, and in particular their **recommender systems** algorithmically amplify terrorist and violent extremist content to online users. The study also examines the **extent to which recommender systems amplify borderline content**, such as some forms of hate speech leading to violent extremism, disinformation and other forms of legal, but harmful content, that could lead to the creation of online filter bubbles, and recruitment and radicalisation of online users. The EUIF continues to address this challenge with its members.

BORDERLINE CONTENT

In the EUIF, we understand borderline content as content that is **legal from the point of view of terrorism legislation, however, it is harmful, can lead to radicalisation, or can be illegal in other ways,** such as in connection to hate speech legislation. As such, it is often a **combination** of disinformation/conspiracy theories and hate speech. Some of the most common types of borderline content identified in the EU are anti-migrant, anti-refugee, and xenophobic narratives, antisemitism, anti-Muslim hatred, anti-system/antigovernment (ASAGE), pro-Kremlin borderline content – also in connection to the Russian aggression against Ukraine, ecoextremism, and anti-LGBTIQ, anti-feminist, and misogynist content. This content can be also **amplified** on the platforms, as explained above, which is why it was introduced hand in hand with the topic of algorithmic amplification.

EUIF Deliverable

The EUIF developed a **Handbook on borderline content** to guide tech companies in the identification of harmful but legal content that can lead towards radicalisation[11]. The EUIF produced two iterations of this Handbook, in 2023 and 2024 to account for changes in the online threat landscape. This work followed agreement on a need for guidance during the EUIF workshop on Algorithmic Amplification and Borderline Content (organised on 29 September 2022). The first version of the handbook was drafted in cooperation with Global Internet Forum to Counter Terrorism (GIFCT) and aims at raising awareness about the need for making clearer links between hate speech and terrorist and violent extremist incidents or activities. It has the sole purpose of **providing non-legally binding guidance** on how to better understand and respond to borderline content that may lead to radicalisation and violent extremism.

[10] EU Internet Forum - Publications Office of the EU

Access to the EUIF wiki is required to access each of the below links:

[11] Handbook for industry - borderline content - EU Internet Forum - EC Extranet Wiki

COUNTER-NARRATIVES AND STRATEGIC COMMUNICATION

Terrorist and extremist actors are very successful in **capitalising on technology and online services** to spread their propaganda, and to radicalise and recruit supporters. Many civil society organisations have already been active in providing **alternative narratives and sharing moderate voices** to counteract the messages coming from these groups, but they often lacked the capacity and / or resources to produce and disseminate these messages effectively online. At the same time, **strategic communication** is inherently important in making sure we are **proactive** rather than reactive, communicate clearly, and have **guidance** ready for all kinds of situations, including in times of crisis. It is not simply about traditional communication - the transfer of information between one actor to another - but using all interactions between and with people to convey a message to shift attitudes away from radicalisation and towards prosocial behaviours.

EUIF Deliverable

Through the Civil Society Empowerment Programme (CSEP)[12], launched in 2015, the EU committed to capacity building, training, partnering civil society organisations with online service providers, and supporting campaigns designed to reach vulnerable individuals and those at risk of radicalisation and recruitment by extremists. An evaluation of the Programme was carried out in 2022, when the programme also concluded. A revised version, renamed the **Community Engagement and Empowerment Programme**, is planned in 2025.

Additionally, joint meetings between the EUIF and the Radicalisation Awareness Network Policy Support took place across the years to address strategic communication in the aftermath of terrorist attacks and specifically on online responses and offline impact related to the Israel/Hamas conflict.

CRISIS RESPONSE

The terrorist attacks of **March 2019 in Christchurch**, **New Zealand**, underscored the need for a swift, coordinated and joint response by law enforcement and online service providers to prevent **terrorist content going viral after an attack**. Since then, several other attacks were live-streamed online, such as the Halle synagogue attack in 2019 or the 2022 Buffalo, New York shooting. Recent years, however, have shown **an evolution of the online dimensions of terrorist attacks**, bringing new challenges, such as modification of content related to the attack or footage produced and disseminated by bystanders.

EUIF Deliverable

Following the 2019 terrorist attack in Christchurch, the EUIF developed the **EU Crisis Protocol** (EUCP)[13], a voluntary mechanism providing for a coordinated, rapid, cross-borders response to contain the viral spread of terrorist and violent extremist related content online. With this development, the EUIF also addressed the priorities of the Christchurch Call to Action. The EUCP was triggered in 2020 in response to the terrorist attack in Conflans-Sainte-Honorine, France. In addition, the EUIF organised an extraordinary meeting on 13 October 2023 to address the crisis following the 7 October terrorist attacks by Hamas. The EUIF organises regular tabletop exercises to ensure its effectiveness and compatibility with other existing crisis response mechanisms. Most recently the EUIF has also tested the interplay of the voluntary mechanism with obligations under the TCO Regulation in case of imminent threat to life.

[12] Civil Society Empowerment Programme - European Commission (europa.eu)

[13] EUIF_Factsheet_May_2023 1.2 (europa.eu)

FINANCING ACTIVITIES ONLINE

Terrorists and violent extremists across the **whole ideological spectrum** are using the internet to simultaneously spread their hateful ideologies to radicalise and recruit and finance their activities. This can include **soliciting donations and selling merchandise, with and without the use of cryptocurrencies**. Addressing this matter is all the more difficult because of **gaps in the current legal framework** for online service providers to detect and report terrorist financing activities, a general lack of legal framework regarding violent extremist financing activities and lack of cooperation between different financial service providers, online service providers and law enforcement to address this exploitation holistically.

EUIF Deliverable

Following two meetings to build an evidence base, involving financial institutions and payment providers, the EUIF developed guidance **'Towards Robust Terms of Service to prevent Terrorist and Violent Extremist Financing activities online'**[14] for industry. The EUIF continues this work with the goal to improve cooperation to better detect and report malicious activity online.

GENERATIVE ARTIFICIAL INTELLIGENCE

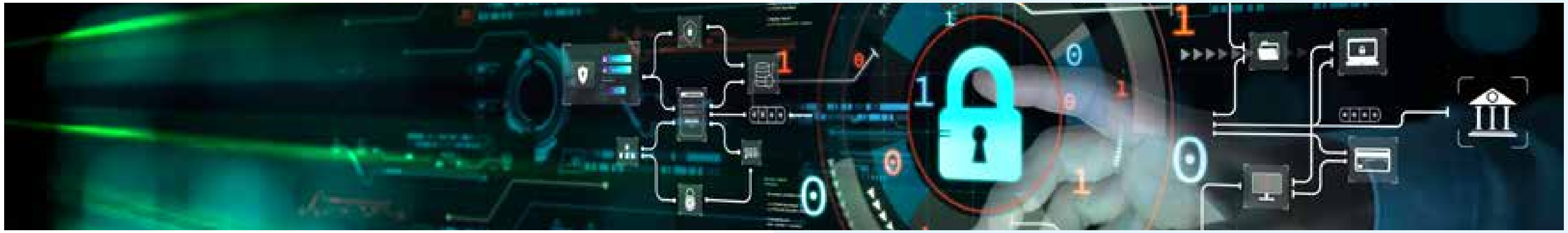
With the emergence of generative AI, including large language models, malicious actors were quick to exploit those means for terrorist and violent extremist as well as child sexual abuse purposes. Notably, the emergence of generative artificial intelligence tools **capable of creating text, visual content and soundtracks** presents new opportunities for malicious actors to spread borderline content, as well as extremist and terrorist propaganda. Additionally, the development of **deepfakes contents** poses a significant risk. At the same time, genAI also offers chances to **improve content moderation.**

EUIF Deliverable

The EUIF took an early stance to bring together companies developing generative AI with EUIF members in the EUIF Ministerial Meeting 2024 to address this issue holistically. The EUIF broadened its membership to companies developing generative AI tools and set-up a dedicated workstream on generative AI.

Access to the EUIF wiki is required to access each of the below links:

[14] Guidance Towards Robust ToS - EU Internet Forum - EC Extranet Wiki (europa.eu)



VIOLENT RIGHT-WING EXTREMISM

There is a lack of designations when it comes to violent right-wing extremist (VRWE) content online, including groups, symbols and other content, such as manifestos. This presents challenges for industry members taking action against the content and preventing the spread of violent right-wing extremist ideology.

EUIF Deliverable

The EUIF developed a **Knowledge Package of VRWE** groups online, symbols, and manifestos that are banned or proscribed under Member States' national law to support industry stakeholders in their voluntary content moderation. The input is provided by Member States and enriched by Europol and trusted researchers based on clear criteria. The Knowledge Package has been transformed into a searchable database available to EUIF members to support industry's voluntary content moderation efforts. The Knowledge Package is updated regularly to reflect new developments.

TERRORIST-OPERATED WEBSITES

There has been a **resurgence in the use of terrorist operated websites** (TOWs) to **share** and **archives** terrorist content as well as to **recruit** and to **raise funds**. Giving a sense of legitimacy to terrorist content, those websites are **difficult to detect and not subject to content moderation**. The obstacles are numerous: lack of a legal basis for companies to remove TOWs, varying legislation across jurisdictions, limited guidelines on the designation of entities as terrorist organizations, insufficient information about contact points within law enforcement and industry, lack of dedicated channels for flagging TOWs, and difficulties in identifying the website owner.

EUIF Deliverable

In addition to raising awareness of TOWs among internet infrastructure providers, the EUIF produced **two deliverables** to provide **guidance to industry on reporting processes and channels**. The first deliverable is a **Directory of Contact Points**, which aims to facilitate direct communication and voluntary collaboration between relevant stakeholders to remove TOWs. The second deliverable takes the form of a **Flow of Information Chart**[15] providing guidance to industry on how to flag a TOW most effectively to law enforcement.

[15] Terrorist Operated Website - Flow of Information Chart - EU Internet Forum - EC Extranet Wiki (europa.eu)

VIDEOGAMING

Despite potential positive social benefits, the connectivity offered by gaming platforms and communication services brings **risks of exposure** to extremist content and radicalisation. Malicious actors are exploiting video-gaming and adjacent platforms for **recruitment, spread of propaganda, terrorism financing and other illegal activities.** The concerns are heightened by the fact that many young people play video games, and the **unique design and features of gaming and related platforms can make them challenging to moderate.** Additionally, terrorist and violent extremist (TVE) actors exploit gamification elements to make their content more appealing and engaging to users.

EUIF Deliverable

A handbook on videogaming to empower gaming communities to counter the misuse of gaming-related spaces[16] was developed by the EUIF in June 2023. The first part of the handbook contains **inspiring practices from civil society organisations** and explores areas for collaboration between tech industry and CSOs. This part of the handbook was produced by Radicalisation Awareness Network (RAN) Practitioners[17] and is publicly available on the RAN Practitioners webpage[18]. The second part presents existing best practices from companies to empower their users, which is an internal product of the EUIF.

Access to the EUIF wiki is required to access each of the below links:

[16] Handbook for industry on empowering gaming communities - EU Internet Forum - EC Extranet Wiki

[17] About RAN - European Commission

[18] Countering the misuse of gaming-related content & spaces: Inspiring practices and opportunities for cooperation with tech companies, November 2022 - European Commission

06.Child Sexual Abuse Online

Over the past 20 years, the threat of child sexual abuse online has grown exponentially in both scale and methods. The volume of online **child sexual abuse material** (CSAM) and **grooming** reports has increased dramatically, fueled by greater connectivity and technological developments. New forms of abuse are emerging and known threats intensify. Grooming and sexual extortion ('sextortion') reports have almost tripled between 2022 and 2023, while a new wave of **AI-generated CSA** is already underway.

Meanwhile, more and more interpersonal communication services are becoming end-to-end encrypted (E2EE), which - in the absence of robust mitigation measures - could result in substantial amounts of online CSA going **undetected and unreported.**

Against this backdrop, in 2020 the Commission launched its new **EU Strategy for a more effective fight against child sexual abuse**, which provides the key reference framework to respond in a comprehensive way to the increasing threat of CSA, both in its online and offline forms.

EUIF Actions

EUIF members actively contributed to the preparations for the new Strategy and supported a number of key actions aimed at improving the coherence and effectiveness of the EU regulatory framework to tackle CSA online, including:

- Sharing evidence and data in preparation of the impact assessment for the Commission proposal for a long-term **Regulation to prevent and combat child sexual abuse**, launched in May 2022.
- Technical meetings to inform the **evaluation and impact assessment** for the targeted revision of the criminal law framework to combat child sexual abuse (Recast of Directive/2011/93).
- Written consultation to improve the effectiveness of CSA reporting by companies, to support implementation of the **CSA Interim Regulation**.
- Technical meeting in October 2024 to share learnings and insights from the Lantern programme - a groundbreaking initiative bringing together technology companies to **share signals** about CSA-related activity.

GENERATIVE ARTIFICIAL INTELLIGENCE

Thanks to publicly available AI platforms, offenders can produce **exponential numbers of digital images and videos depicting child sexual abuse**. Offenders create **AI-generated** CSAM by entering text prompts or by artificially modifying existing images of children, based on known CSAM as well as 'innocuous' images. The latest trends include the development of videos and audio cloning.

Text-to-text and text-to-chat AI models can also provide offenders with **tools and instructions** for grooming, sextortion or hands-on sexual abuse of a child, or information on how to escape prosecution.

The proliferation of AI creates new and significant challenges for law enforcement. The higher volume of CSAM available online can also contribute to a "normalisation" of such content, which in turn may lower barriers to offending.

EUIF Deliverable

The EUIF took an early stance to bring together companies developing generative AI with EUIF members in the EUIF Ministerial Meeting 2024 to address this issue holistically. The EUIF broadened its membership to companies developing generative AI tools and set-up a dedicated workstream on generative AI.

07.Trafficking in Human Beings Online

The cooperation with the internet companies is instrumental to reduce trafficking in human beings by engaging actively in prevention and awareness raising, which can be pursued by very different means including advertisements targeting potential victims and also potential users of exploited services. There are good examples of collaboration between private and public actors, i.e. law enforcement at the first place, which should be further explored. Companies and Internet providers can also support (non-profit) awareness raising campaigns by acting as a multiplier, particularly when it comes to messages targeted to the general public.

EUIF Actions

The EU Internet Forum endorsed the inclusion of trafficking in human beings amongst its activities on 17 November 2022 at senior official level. The EU Anti-trafficking Coordinator convened a technical meeting with the companies on 5 May 2022 on trafficking in human beings following Russia's military aggression against Ukraine and she also convened the EU Internet Forum on 1 June 2023 with the objective at expert level to reinforce already existing actions, to increase cooperation with the private sector and to define concrete actions, commitments and mutual support to tackle trafficking in human beings online.

08. Drug Trafficking Online

Criminals increasingly use state of the art technology to facilitate their illicit activities, including the sale of drugs. The shift from the darknet to social media platforms brings in a worrying trend, creating additional challenges for companies and law enforcement authorities, notably when it comes to monitoring the vast volume of online content, which can be temporary, fragmented and rapidly changing. Moreover, the linguistic, geographical and cultural diversity of the drug markets, including the widespread usage of emojis, makes it even more difficult for social media companies to recognise, assess and moderate such content on their platforms.

To respond to challenges posed by the rise of drug trafficking online it was agreed during the Senior Official Meeting of the EU Internet Forum on 16 November 2022 to include drug sales online in the work of the Forum on the technical level.

EUIF Deliverable

On 8 February 2024, the Commission shared with the members of the EU Internet Forum a Knowledge Package to support internet companies in better moderating drug trafficking contents on their platforms. The Knowledge Package was developed in close cooperation with the EUIF member countries, the companies, and the EU agencies (European Union Drugs Agency[19] and Europol).

The Knowledge Package is a multilingual collection of over 3 500 names (including slang and idioms), acronyms, symbols and emojis used by drugs traffickers to advertise their products online. Most terms use the Latin alphabet (including with diacritics), with some terms using the Cyrillic alphabet. These have been assembled into one Excel workbook, a format from which the data can be easily extracted.

The Excel workbook and accompanying text is made available to all EUIF members via the EUIF Wiki. The EUIF continues to work on addressing this issue and improving guidance delivered to its members. In this context, a technical meeting on the implementation of the Knowledge Package was organised on 23 September 2024.

[19] As of the entry into application of Regulation (EU) 2023/1322 on 2 July 2024, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) was replaced by the European Union Drugs Agency (EUDA).

09. Global Cooperation

GLOBAL INTERNET FORUM TO COUNTER TERRORISM

The GIFCT is an NGO aiming to prevent terrorists and violent extremists from exploiting digital platforms. Founded by Meta (formerly Facebook), Microsoft, YouTube and X (formerly Twitter) in 2017, it was established to foster technical collaboration among member companies, advance relevant research, and share knowledge. The European Commission is part of the Independent Advisory Committee to the GIFCT and actively participates in the GIFCT working groups to address challenges of transnational nature and promote global response.

CHRISTCHURCH CALL

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** and continued so since its **transformation into a charity in 2024**. It ensures close cooperation and synergies with the EU Internet Forum and the Commission pro-actively supports the goals of the Christchurch Call, including by participating in its workstreams.

10. Outlook

The breadth of topics and products testifies to the relevance of the work of the EUIF. To fully capitalise on the potential of this unique forum, it is key to **remain on top of new threats** to address them **quickly** and where possible **proactively**.

Looking ahead, seeing how the online dimension can be exploited for a plethora of harms, there is also a **potential to grow the scope of the EUIF** to be able to provide a **holistic assistance** and serve as a **one-stop-shop to exchange expertise**. Especially so since the response by the policy makers, law enforcement, and the internet companies needs to evolve to be able to combat the illegal and malicious activities online as quickly as the online world evolves. Moreover, since **threats are becoming multi-faced, hybridized, and cross-sectoral, it is necessary to foster cross-sectoral cooperation, exchange on the best practices, and integrate new tools into our toolbox.**

European Commission

EU Internet Forum

Joining forces against illegal content