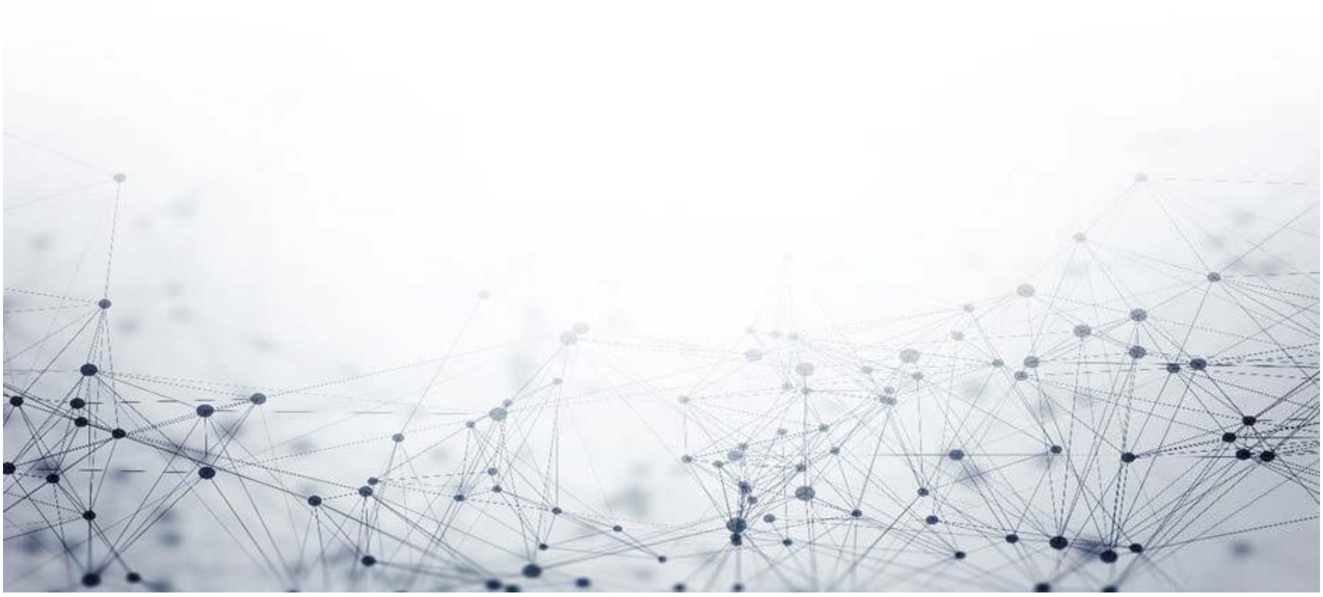
2020
EU IRU
Transparency Report.

EU IRU REPORT



AUTHORS
EU Internet Referral Unit

Catalogue number	QL-AR-21-001-EN-N
ISBN	978-92-95220-34-8
ISSN	2600-4747
DOI	10.2813/14039

Cite this publication: Europol (2021), 2020 EU IRU Transparency Report, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

Table of Contents

List of acronyms and abbreviations

CBRN	Chemical, Biological, Radiological, Nuclear
CRWG	Crisis Response Working Group
CT	Counter-Terrorism
CtW	Check-the-Web
ECTC	European Counter Terrorism Centre
EMSC	European Migrant Smuggling Centre
ER	Europol Regulation
EU	European Union
EUCP	EU Crisis Protocol
EUIF	EU Internet Forum
EU IRU	European Union Internet Referral Unit
GIFCT	Global Internet Forum on Counter Terrorism
IRMa	Internet Referral Management application
IRU	Internet Referral Unit
LEA	Law Enforcement Agencies
MS	Member States
OSP	Online Service Providers[1]
RAD	Referral Action Days
RW	Right Wing
SWG	Sub-Working Group
TP	Third Parties
TTX	Tabletop Exercise

[1] The working definition of 'Online Service Providers' (OSP) used in this report is any company providing online services to EU citizens.

1. Aim and scope of the report

This is the fourth edition of the European Union Internet Referral Unit (EU IRU) Transparency Report. The overall objective of this annual exercise is to offer a clear picture of the EU IRU, by providing visibility into its mandate, its legal framework and into how it enforces its policies.

The present report intends to give an account of the EU IRU's major activities in 2020. More specifically, the two pillars on which its work is based fall under the scope of this report:

1. Prevention activities, which aim to reduce public accessibility to online propaganda produced by terrorist organisations; and
2. Investigative support, delivered by the EU IRU upon request of EU Member States (MS).

2. Context

Mandate of the EU IRU

In the wake of the series of terrorist attacks that shook Europe in 2015, EU MS decided to implement a coherent and coordinated European prevention approach. On 12 March 2015, Ministers of the Justice and Home Affairs Council of the EU mandated Europol[2] to establish a dedicated unit aimed at reducing the level and impact of Internet content promoting terrorism or violent extremism.

The EU IRU, which is part of Europol's European Counter Terrorism Centre (ECTC), started its operations in July 2015 with a mandate to refer terrorist and violent extremist content to Online Service Providers (OSP) and provide support to MS and Third Parties (TP) in the context of Internet investigations.

In line with Europol's Regulation[3], the EU IRU's mission is to link the virtual face of terrorism to its physical aspect, by bridging the gap between prevention and investigation capabilities. The EU IRU detects and refers the core disseminators of terrorist propaganda, with the aim of not only restricting public access to terrorist propaganda, but also identifying and facilitating the attribution and prosecution of perpetrators. Its ultimate objective is to reduce the accessibility of terrorist content online by providing a sustained referral capability to MS, and to provide a core Internet-based investigation support capability to respond to the MS' operational needs.

In order to fulfil its mission, the EU IRU works in close collaboration with the two other components of the ECTC: the Counter-Terrorism (CT) Operations Unit and the ECTC Expertise and Stakeholder Management Unit. This collaboration ensures that the mission of the ECTC can be coherently implemented through the provision of high-quality operational support and advanced strategic products, and that the ECTC proactively engages in the CT field both within the EU and beyond.

The special European Council of 23 April 2015 on the migration situation in the Mediterranean Sea, as part of the political direction given to EU agencies, called for Europol and the EU IRU to expand its mandate in order to

[2] Justice and Home Affairs Council, Outcome of The Council Meeting - 3376th Council meeting, 12 and 13 March 2015, https://www.consilium.europa.eu/en/meetings/jha/2015/03/12-13/

[3] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016, https://www.europol.europa.eu/publications-documents/regulation-eu-2016/794-of-european-parliament-and-of-council-of-11-may-2016

contribute to the disruption of illegal migrant smuggling networks[4]. In this context, the EU IRU also provides support to Europol's European Migrant Smuggling Centre (EMSC), by flagging detected Internet content used by traffickers to offer smuggling services to migrants and refugees.

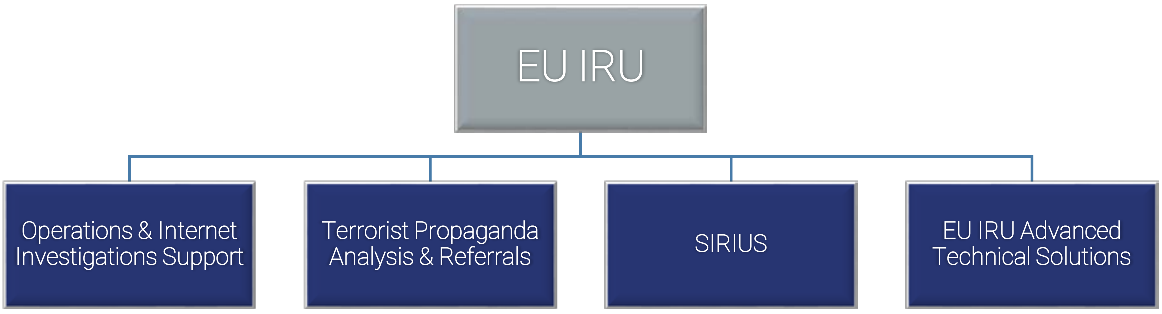
Legal framework

The EU IRU operates under clearly defined rules. Its tasks and activities are carried out in full compliance with the Europol Regulation (ER), as well as the EU legal framework, in particular the Directive (EU) 2017/541 on combating terrorism[5].

Furthermore, Europol has put in place a comprehensive, robust and tested data protection regime which ensures the highest standards of data protection. This aims at ensuring the protection of personal data processed in Europol's systems. At the same time it serves the needs of operational units in preventing and combating terrorism, organised crime, and other forms of serious crime affecting two or more MS[6].

The EU IRU

The EU IRU capabilities are supported by staff members who have a rich diversity of knowledge and skills, ranging from experts in religiously inspired terrorism, translators, ICT developers and law enforcement experts in CT investigations.


EU IRU
Operations & Internet Investigations Support
Terrorist Propaganda Analysis & Referrals
SIRIUS
EU IRU Advanced Technical Solutions

In accordance with its mandate, the EU IRU delivers through the following four teams a variety of services and products:

- Operations and Internet Investigations Support – the EU IRU provides support to EU MS's online investigations, through operational support, expert advice, coordination and assistance and the delivery of ad hoc tailored reports.
- Terrorist Propaganda Analysis and Referrals – The EU IRU performs the referral and analysis of jihadist propaganda online. It also provides policy advice at EU level, and acts as a hub for knowledge sharing on the topic.
- SIRIUS – The SIRIUS team provides products and services to EU Law Enforcement Agencies (LEA) and judiciaries to help them cope with the complexity of accessing electronic evidence from non-EU-based OSP for the purposes of criminal investigations.
- EU IRU Advanced Technical Solutions – A team of ICT experts and developers provides horizontal support to the Unit, by performing research on breakthrough technologies and OSINT advanced techniques for LEA as well as carrying out market research on products to be integrated into the EU IRU workflows. It also develops tools for flagging and collecting publicly accessible online terrorist content while implementing technology applications to strengthen the EU IRU capabilities.

[4] Council of the European Union 2015, Special meeting of the European Council, 23 April 2015 – statement, accessible at https://www.consilium.europa.eu/en/press/press-releases/2015/04/23/special-euco-statement/#

[5] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

[6] For more information: Europol, *Data Protection & Transparency*, https://www.europol.europa.eu/about-europol/data-protection-transparency

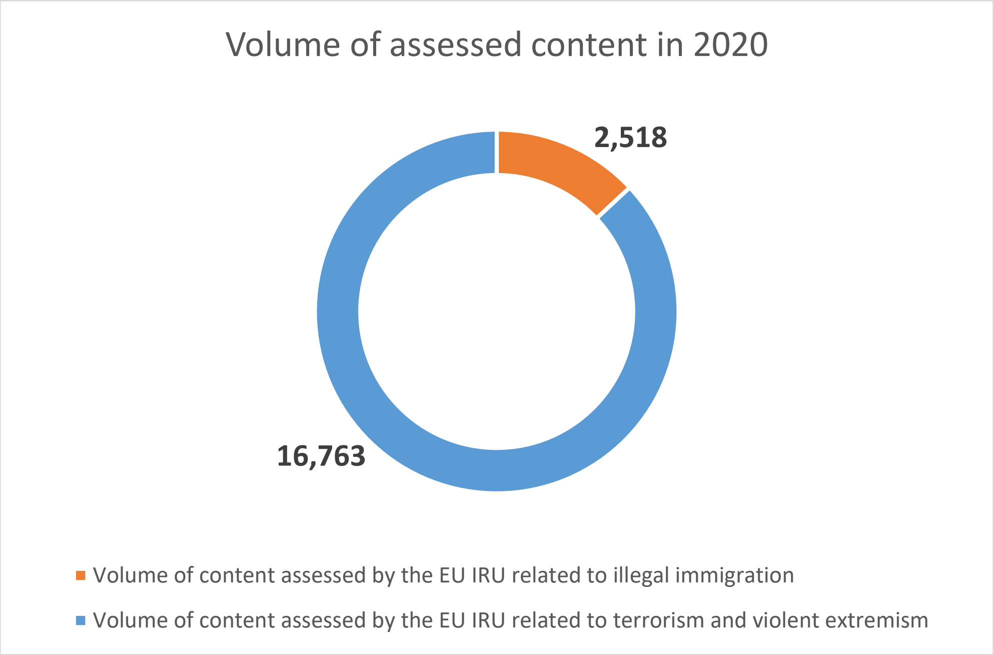
3. Referrals

One of the core tasks of the EU IRU is referral by flagging terrorist content online and cooperating with OSP for their voluntary review and possible removal of such content. Referrals are made both following requests received from MS and as a result of open source scanning by the EU IRU. Priority is given to propaganda material linked to a high profile event and relayed by high profile accounts. A further objective of this process is information gathering with a view to better understanding the tactics and modus operandi of the major online propagandists, and providing strategic and technical analysis to EU MS and TP.

Prior to the OSP voluntary consideration of the compatibility of content with their terms and conditions, the EU IRU performs a manual evaluation to assess the contents' eligibility for referral. The Europol Regulation (ER) provides the mandate for referring Internet content. Annex I of the ER lists the forms of crimes which are facilitated, promoted or committed e.g. terrorism, migrant smuggling and trafficking in human beings. The EU IRU relies upon EU legislation, such as the EU Directive on combating terrorism, to define offences that fall within the forms of crimes for which Europol is mandated.

In the framework of the Analysis Project Check-the-Web (AP CtW) and based on threat assessments, the EU IRU has a proactive focus on three priority groups: Islamic State, al-Qaeda and Hayat Tahrir al-Sham, including their affiliates and individual supporters. The envisaged amendment of AP CtW (end of 2021) widens the scope to terrorism and violent extremism in general, irrespective of its motivation. The amendment of AP CtW will also entail a review of the proactive focus of the unit. As a standard, this is based on threat assessments.

In 2020, in terms of referral activities, the EU IRU produced the following figures:



RAD in 2020

Europol is mandated to coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the MS.

On a regular basis, the EU IRU organises and coordinates Referral Action Days (RAD) together with the competent authorities of the MS, both on Europol premises and remotely. RAD facilitate direct cooperation with law enforcement representatives in EU MS.

RAD can have different forms. Thematic RAD target illegal terrorist online content in specific areas such as CBRN and instructional material (i.e. manuals, tutorials etc.) Platform-specific RAD inform affected OSP of the ways in which their services are being abused by terrorists and/or violent extremists, and by which means.

These RAD allow for the swift exchange of best practices between the EU IRU, national IRUs in MS and OSP with the aim of enhancing the referral process and improving critical elements such as feedback and response time.

In 2020, the EU IRU organised and coordinated a total of 3 RAD with EU MS and TP. One had a focus on instructional terrorist material online, one was platform-specific and one had a focus on jihadist content in Western Balkan languages[7].

4. Terrorist propaganda monitoring and analysis

The CtW portal

The EU IRU manages the Check-the-Web (CtW) portal to build upon its historical knowledge and expertise. Accessible only to law enforcement, the CtW portal is an electronic reference library of jihadist terrorist online propaganda. It contains structured information on original statements, publications, videos and audios produced by jihadi terrorist groups and their supporters.

The CtW portal is an operational tool to support EU MS not only for the purposes of identifying new content, groups or media outlets but also new trends and patterns in terrorist propaganda, as well as operational leads for attributing crimes to perpetrators. Its goal is to improve the EU Intelligence picture on modus operandi of online terrorist propagandists and online CT challenges in EU MS and beyond.

Strategic and thematic analysis

The team is in a unique position to perform analysis on data from a variety of sources, including the CtW portal, referral activities and EU MS contributions. The strategic analysis performed within the EU IRU looks at emerging trends in the field of online jihadi terrorist content from different angles, such as its dominant themes and narratives, regional focus, dissemination patterns and the use of new technologies.

In 2019, the EU IRU produced a total of 13 strategic and thematic reports, describing trends and patterns in terrorist or violent extremist propaganda, including key changes in the abuse of technology for propaganda dissemination. The report 'Online jihadist propaganda: 2019 in review' – in its third edition - was published on Europol's website[8] and outlined the major trends and developments in the propaganda of the most prominent

[7] Europol, *Europol Coordinates Referral Action Day to Combat Manuals and Tutorials on Improvised Explosive Devices Including CBRN*, December 5, 2019, https://www.europol.europa.eu/newsroom/news/europol-coordinates-referral-action-day-to-combat-manuals-and-tutorials-improvised-explosive-devices-including-cbrn

[8] EU IRU, *Online jihadist propaganda: 2019 in review*, July 28, 2020, https://www.europol.europa.eu/newsroom/news/online-jihadist-propaganda-2019-in-review

Sunni jihadist organisations – the Islamic State and al-Qaeda – as well as their affiliates and offshoots. In particular, the review aimed to analyse how these organisations have responded to shifting political realities and attempted to overcome setbacks.

Furthermore, the EU IRU produces and shares the 'Weekly Message' with EU MS, a weekly analysis of jihadist propaganda and new dissemination techniques that has the primary objective of keeping EU MS abreast of the latest trends on the topic.

5. Support to MS investigations

The EU IRU has developed its own methodology and toolset to support EU MS in online investigations, both in the immediate aftermath of a terrorist attack and in the framework of structured and consolidated CT operations. Upon the request of EU MS, the EU IRU supports competent authorities by providing operational support through criminal, technical and forensic analysis and, when appropriate, on-the-spot deployments. The EU IRU delivers fast and actionable analytical support and in-depth operational support on the basis of real time social media analysis.

In 2020 the EU IRU supported 156 EU MS operations, including horizontal support provided to other areas, and delivered the following products and services:

2020 Operational Support	
Intelligence notifications	1
Cross-match Reports	2
Intelligence Packages	305
Provision of Expertise	97
Other Reports	4
TOTAL	**409**

6. The SIRIUS project

SIRIUS
PLATFORM:
+5100
users
44
countries
+1000
forum
messages
36 tools

SIRIUS is a central reference point in the EU for knowledge sharing on cross-border access to electronic evidence. More than half of all criminal investigations today include a cross-border request to access electronic evidence (such as data from messaging or email services, or social media) and the SIRIUS project aims to help investigators cope with the complexity and volume of information in a rapidly changing online environment.

The SIRIUS project was launched in 2017 by Europol, and in 2018 it received funding from the European Commission within the framework of the Partnership Instrument of the EU. Since then, the Project has been run as an EU-funded project in compliance with a Grant Agreement (2018-2021). From 2022, the Project will enter into its second phase and will be funded by a grant received under a new Contribution Agreement.

By the end of 2020, SIRIUS had a significantly enlarged community of law enforcement and judicial authorities interested in learning more about lawful procedures in order to gain access to e-evidence stored by OSP that are based outside the EU.

It provides products and services to a community of more than 5,000 users, ranging from knowledge products (e.g. explaining the type of data that can be requested from OSP and which types could be useful for the investigation or prosecution of crimes) to tools facilitating digital investigations, to training courses, both face-to-face and online. SIRIUS also created interactive ways of learning processes and procedures for gaining access to electronic evidence, such as the SIRIUS game.

The main project achievements of 2020 include:

- Signature of the Contribution Agreement for SIRIUS phase 2[9]: the signature of the Contribution Agreement (CA) between Europol and the European Commission introduced the second phase of the project, which will have a duration of 42 months. Moreover, with the new grant Eurojust became a full co-beneficiary entity within the project. The CA entered into force on 1 January 2021 and will end on 30 June 2024. The overall budget for the Action is nearly €3.5 million. The second phase of the project aims, among other objectives, to expand its geographical focus to include third countries based on the interest of Law Enforcement and judicial authorities.

- The second edition of the EU Digital Evidence Situation Report[10]. The objective of this report is to draw a picture of the status of access of EU MS to electronic evidence held by foreign-based OSP. The second report was drafted in 2020, looking at data related to 2019.

- SIRIUS game: In partnership with CENTRIC, the SIRIUS team created a browser-based game to offer an immersive learning experience to the SIRIUS community. The purpose of this project was to use gamification to teach the following:
  - Main steps of online investigations;

[9] Europol and Eurojust sign new Contribution Agreement expanding cooperation on the SIRIUS project, https://www.europol.europa.eu/newsroom/news/europol-and-eurojust-sign-new-contribution-agreement-expanding-cooperation-sirius-project

[10] EU IRU, *Sirius: European Union Digital Evidence Situation Report 2020*, December 1, 2020, https://www.europol.europa.eu/publications-documents/sirius-eu-digital-evidence-situation-report-2nd-annual-report

- Key concepts related to e-evidence;
- Cross-border requests to foreign-based OSP;
- SIRIUS products and services.

- SIRIUS Virtual Events: As the COVID-19 pandemic restricted all forms of travel, the traditional format for the yearly SIRIUS conference was replaced by a series of events, held virtually, over three consecutive days. Despite the online nature of the events, the SIRIUS Virtual Events succeeded in gathering more than 1000 attendees over three days.

- SIRIUS e-evidence Series: A training series of six self-paced online learning sessions was published in 2020. The 'series' format serves the two-fold purpose of breaking down the data request and disclosure process, providing more in-depth insights on the different steps involved, while also giving the audience the option of selecting and focusing on a specific topic of choice. All episodes are available in English, French, Italian and Spanish.

- OSP Finder – a dynamic database of more than 250 OSP was created and it contains basic information on their services, ways to lawfully engage in requesting data disclosure and a summary of the companies' policies. This database is constantly updated on the basis of the expertise and information developed by the entire SIRIUS community.

7. Horizon2020 projects

The EU IRU and SIRIUS are not the only players in Europe contributing to increasing the capacities of EU LEA in the field of digital investigations. In the 2014-2020 financial period, and especially via the Horizon 2020 Programme, the European Commission has funded a number of Research and Innovation projects that gathered key academic and industry actors from all over Europe to develop new knowledge and technologies for LEA.

In 2020, the unit got an active role in two of the H2020 Projects, namely INFINITY and AIDA, and maintained its advisory or monitoring role in the capacity of Advisory Board member on ten specific projects.

Within the framework of the H2020 Project INFINITY, the EU IRU is leading two work packages[11] related to the user requirements and the operational evaluation of the system. This project, launched in June 2020, gathers seven LEA including Europol and 13 technical partners. Synthesising the latest innovations in virtual and augmented reality, artificial intelligence and machine learning with big data and visual analytics, INFINITY will deliver an integrated solution that aims to revolutionise data driven investigations.

The EU IRU is also actively involved in the H2020 project AIDA as a contributor, launched in September 2020. This project aims to provide LEA across the EU with a modular capacity to acquire, (pre)process, enrich, analyse and visualise multi-source Big Data in real-time, while maintaining full compliance with fundamental rights and applicable legislation including privacy and protection of personal data.

[11] The definition of H2020 on the work package is a major sub-division of the proposed project. Work packages are both the backbone and building blocks of any Horizon 2020 project. The work package structure is the means through which the concept presented in the project proposal is realized.

8. Outreach activities

Collaboration with tech companies

Beyond the referral of terrorist content, the EU IRU has established regular engagement with a number of online platforms across the world, with the aim of helping them enhance their resilience against terrorist abuse. Whilst most platforms have auto-detection mechanisms in place to proactively identify and suspend content, others, especially smaller platforms, rely solely on referrals and may require further assistance to reinforce their prevention mechanisms.

In 2020, the EU IRU collaborated with platforms that were identified as being the most prominently used by terrorists to promote terrorist content, focusing on the following two priority areas (depending on the platforms' services and/or capability):

-Referral process: through the establishment of trusted-flagger accounts and the development of solutions, ensuring feedback and swift response time to referrals;

-Identification of terrorist content: through targeted Referral Action Days, exploring how their services have been abused and by which terrorist networks, as well as detailing trends and methods used by terrorist organisations to evade content moderation efforts.

EU Internet Forum (EUIF)

The EU IRU outreach policy to tech companies in the fight against online terrorist propaganda, whilst aligned closely with the operational needs of the EU MS, has been performed within the framework and objectives of the EU Internet Forum[12]. In this regard, the EU IRU, in cooperation with the EU Commission, contributed to the Forum's objectives related to right wing terrorism and the implementation of the EU Crisis Protocol (EUCP).

Responses to right wing terrorism

The EU IRU participated in a series of EUIF technical workshops that were dedicated to addressing the dissemination of right wing terrorist and violent extremist content online. The objective of the workshops was to increase awareness of the issues related to right wing terrorist and violent extremist content on the Internet, to discuss the challenges that MS and the tech industry are facing and the measures that may be put in place to tackle the issue.

EU Crisis Protocol implementation

The EU IRU contributed to the EU Internet Forum's objective on the implementation of the EUCP[13] with the following activities in 2020:

[12] The EU Internet Forum is a platform launched by the EU Commission on 3 December 2015, bringing together EU Interior Ministers as well as a number of Internet companies, Europol, GIFCT and EU institutions/organisations such as the EU CTC. The aim of the Forum is to address in a coordinated, yet voluntary, manner, the phenomenon of the spread of terrorist and violent extremist propaganda to a large proportion of the global online population.

[13] The EU Crisis Protocol is a collective response to viral spread of terrorist and violent extremist content online and is a voluntary mechanism to enable a coordinated and rapid response to cross-border crises in the online space, stemming from a terrorist or a violent extremist act. The Protocol aims to facilitate rapid assessment of the online impact of terrorist attacks, secure and timely sharing of critical information between EU Member States Law Enforcement and other Competent Authorities, Union bodies (in particular Europol), Online Service Providers and relevant stakeholders, to ensure effective coordination and management of the crisis.

Consultation process with practitioners from MS

In order to identify outstanding issues and further develop the implementation of the EUCP, in 2020 the EU IRU launched a consultation process with practitioners from MS and national IRUs.

The consultation process involved a series of initiatives such as a workshop, a survey, online meetings and a tabletop exercise. A requirement that transpired from the consultation process with MS was the development of an operational guide (EUCP Playbook). Practitioners had identified a lack of operational guidance for the practical implementation of the EUCP by LEA in the event of a crisis. To this end, the EU IRU committed to deliver a EUCP Playbook at the beginning of 2021 that would specify the operational processes for law enforcement.

GIFCT Crisis Response Working Group

Parallel to the consultation process with MS, the EU IRU engaged with the tech industry to contribute to setting up international standards in crisis response. To this end, it co-chaired, alongside DG Home and Microsoft, the Global Internet Forum to Counter Terrorism (GIFCT) Crisis Response Working Group (CRWG). The CRWG was established with the aim of fostering effective collaboration across industry, government and first-responders to minimise the spread of terrorist or violent extremist content online stemming from a real world terrorist incident. The CRWG is composed of representatives from the public sector, private companies and civil society. One of the activities of the CRWG was to explore the operational and investigative requirements of law enforcement during an attack or a protocol-driven event and examine how industry can safeguard these requirements. The EU IRU leads this stream of work through a sub-working group (SWG) dedicated to this topic. Participants in this group included representatives from governments and LEA. The outcome of the SWG in 2020 was to identify a set of principles for collaborative action during a crisis protocol incident.