2019

EU IRU Transparency report

Table of Contents

List of acronyms and abbreviations 3

1. Aim and scope of the report 4

2. Context 4

Mandate of the EU IRU 4

Legal framework 5

The EU IRU 5

The EUIF and GIFCT 5

3. Referrals 6

RADs in 2019 6

4. Terrorist propaganda monitoring and analysis 7

The CtW portal 7

Strategic and thematic analysis 7

5. Support to MS investigations 8

In-depth: operation AMAQ 8

6. The SIRIUS project 9

7. Horizon2020 projects 10

8. Outreach activities 10

Collaboration with tech companies 10

Ongoing processes and events 10

EU Crisis Protocol 10

The Tabletop Exercise 11

List of acronyms and abbreviations

AQ	Al-Qaeda
CBRN	Chemical, Biological, Radiological, Nuclear
CT	Counter-Terrorism
CtW	Check-the-Web
ECTC	European Counter Terrorism Centre
EMSC	European Migrant Smuggling Centre
ER	Europol Regulation
EU	European Union
EUIF	EU Internet Forum
EU IRU	European Union Internet Referral Unit
GIFCT	Global Internet Forum on Counter Terrorism
HTS	Hay’at Tahrir al-Sham
IRMa	Internet Referral Management application
IRU	Internet Referral Unit
IS	Islamic State
LEA	Law Enforcement Agency
MS	Member State
OSP	Online Service Provider[1]
RAD	Referral Action Day
TP	Third Party
TTX	Tabletop Exercise

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

1. Aim and scope of the report

This is the third 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 2019. 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 designated 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 (OSPs) and provide support to MS and Third Parties (TPs) in the context of Internet investigations. 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.

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 resilient 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.

[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

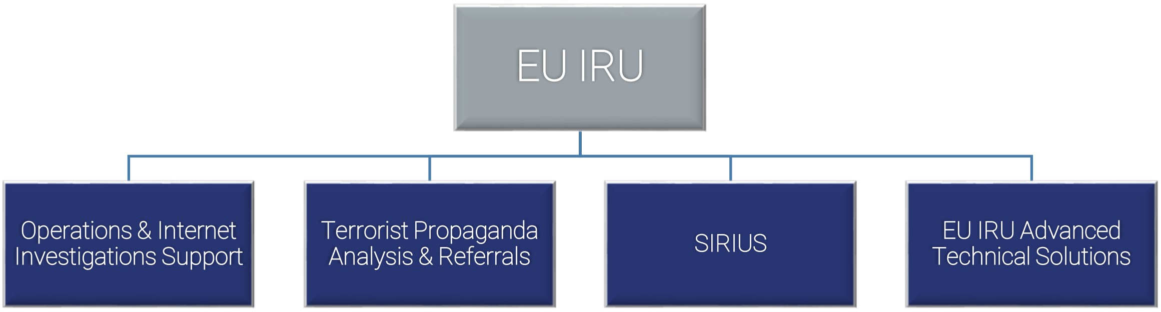
Legal framework

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[4].

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[5].

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 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 (LEAs) and judiciaries to help them cope with the complexity of accessing electronic evidence from non-EU-based OSPs 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 LEAs as well as carrying out market research on products to be integrated in EU IRU workflows. It also develops tools for flagging and collecting publicly accessible online terrorist content while implementing technology applications to strengthen EU IRU capabilities.

The EUIF and GIFCT

The EU IRU engages with a number of cooperative online service providers that are members of global initiatives working to stymie online terrorist content; these initiatives are namely the EU Internet Forum (EUIF), where the EU IRU is a key stakeholder, and the Global Internet Forum on Counter Terrorism (GIFCT). These forums provide platforms for communication and the exchange of best practices

[4] 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

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

between all stakeholders and the involved OSPs, on topics related to content detection and removal, resilience mechanisms and pro-active measures, crisis responses, research on current and future trends as well as policy and legislative initiatives.

3. Referrals

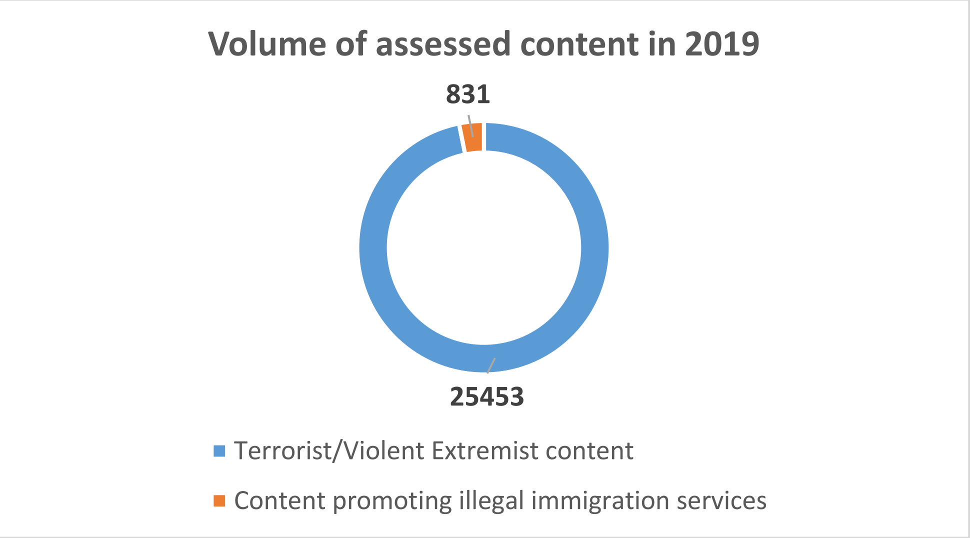
One of the core tasks of the EU IRU is the coordination of referral activities by flagging online terrorist and illegal immigration content. Regarding the referral of terrorist content, the Unit focuses, in agreement with MS, on propaganda releases by Al-Qaeda (AQ), the Islamic State (IS), Hay'at Tahrir al-Sham (HTS), including their affiliate groups, and individual supporters of these groups.

In accordance with the principles set in the EU Directive 2017/541 on combatting terrorism, the Unit assesses content against Europol's mandate and performs a manual evaluation of the content. Following this assessment, the content is assessed against the terms and conditions of the relevant OSP. Referring content to an OSP does not does not constitute an enforceable act. Thus the decision and removal of the referred terrorist content is taken by the concerned service provider under their own responsibility in reference to their terms of use.

In order to support its referral capability, in 2016 Europol established an in-house technical solution called the Internet Referral Management application (IRMa). The tool is designed to manage a semi-automated referral workflow, involving the detection of terrorist content online, assessment, de-confliction and referral of URLs by the EU IRU team members.

Referrals to the online platforms are made both following requests received from MS and as a result of open source research by the EU IRU team. Referrals can also target propaganda linked to high profile events. A further objective of this process is to gather information to better understand the tactics and modus operandi of the core disseminators of online terrorist propaganda.

In 2019, in terms of referral activities, the EU IRU has produced the following figures:



RADs in 2019

Direct cooperation with LEA representatives in EU MS is championed during the Referral Action Days (RADs), which the EU IRU has been organising since September 2016. During the targeted RADs there is a swift exchange of best practices between MS IRUs and OSPs with the aim of enhancing the referral process and improving critical elements such as feedback and response times. The RADs' format allows the EU IRU and national IRUs to focus their referral activity on a single OSP or a limited number of platforms, while the relevant OSP gains insight into the work of the IRUs to better understand the processes and challenges faced by practitioners in the referral process.

In 2019, the EU IRU organised a total of seven RADs. Among them, in November 2019 the EU IRU coordinated a Joint Action that focused on manuals and tutorials on Improvised Explosive Devices, including CBRN (Chemical, Biological, Radiological, Nuclear)[6]. A total of 1733 items were referred to the involved OSPs with a request to be reviewed against their terms of service. The joint operation also included dark web investigations focusing on the trade of CBRN explosive agents in dark web markets. That same month, the EU IRU organised RADs targeting major IS-branded media outlets online. A more detailed description of this RAD can be found below (p. 8).

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 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. The report ''Online jihadist propaganda: 2018 in review'' – in its second edition - was published on Europol's website[7] and provides an overview of the major trends and developments in the propaganda of the "Islamic State" and "al-Qaeda". In addition, two EU IRU thematic reports from 2018 were published online in 2019, namely ''On the Importance of Taking-Down Non-Violent Terrorist Content'' and ''Women in Islamic State Propaganda'', on VoxPol and Europol's websites respectively[8].

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.

[6] 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

[7] EU IRU, *Online jihadist propaganda: 2018 in review*, August 13, 2019, https://www.europol.europa.eu/publications-documents/online-jihadist-propaganda-%E2%80%93-2018-in-review

[8] EU IRU, *On the Importance of Taking-Down Non-Violent Terrorist Content*, VoxPol, May 8, 2019, https://www.voxpol.eu/on-the-importance-of-taking-down-non-violent-terrorist-content/ and EU IRU, *Women in Islamic State Propaganda*, June 14, 2019, https://www.europol.europa.eu/activities-services/europol-specialist-reporting/women-in-islamic-state-propaganda

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 2019, the EU IRU supported 251 EU MS operations and delivered the following products and services:

2019 Operational Support

Intelligence notifications	6
Cross-match Reports	1
Intelligence Packages	314
Preliminary Forensic Reports	9
Provision of Expertise	94
TOTAL	**424**

In-depth: operation AMAQ[9]

In November 2019, the EU IRU, in coordination with specialised Units from both EU MS and Third Parties, organised RADs targeting major IS-branded media outlets online, such as the Amaq News Agency, al-Bayan Radio, Halummu and Nashir News Agency. The EU IRU coordinated the RAD in line with its mandate and in compliance with the applicable procedures. This process is based on the referral by the EU IRU of branded terrorist propaganda to OSPs who are responsible for evaluating it to establish any potential breach of their terms of service. Items referred included videos, publications, and social media accounts supporting terrorism and violent extremism.

The action distinguished itself from the previous ones as it targeted terrorist content shared not only by the online channels and groups, but also by "core disseminators" (users) in various OSPs, in particular Telegram. The action caused notable disruption to the group's communication strategy, a drastic decrease in IS supportive accounts and furthermore forced the IS network to partially renounce the terrorist organisation's established branding, at least on Telegram. The action induced the terrorist group to de-centralize its propaganda machinery and IS affiliates and supporters dispersed in a multi-platform environment.

[9] Europol, *Referral Action Day Against Islamic State Online Terrorist Propaganda,* November 22, 2019, https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda; and Europol, *Europol and Telegram Take on Terrorist Propaganda Online,* November 25, 2019, https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

6. The SIRIUS project

+3,800 users

42 countries

+600 forum messages

32 tools

SIRIUS is the Centre of Reference within the EU for knowledge sharing on digital cross-border investigations. It was launched in 2017 by Europol to help the EU law enforcement community cope with the complexity of accessing electronic evidence from non-EU-based OSPs for the purposes of criminal investigations.

A project proposal was later submitted under a call for proposals of the Partnership Instrument of the EU envisaging a wider scope for the project and including new activities, products and services. The proposal was successful, and since 2018 SIRIUS has been run as an EU-funded project, in compliance with a Grant Agreement signed with the European Commission.

By the end of 2019, SIRIUS had developed to include a large community of law enforcement and judicial authorities interested in learning more about lawful procedures in order to gain access to e-evidence stored by OSPs that are based outside the EU.

It provides products and services to a community of more than 3,000 users, ranging from knowledge products (e.g. explaining the type of data that can be requested from OSPs and which could be useful for the investigation or prosecution of crimes) to tools facilitating digital investigations, to training courses, both face-to-face and online.

The main project achievements of 2019 include:

- The second SIRIUS yearly Codefest, a two-day event that brought together a selected number of Law Enforcement officers specialised in computer programming from across Europe to work together on a new tool helping digital investigators. The tool was later made freely available to the whole SIRIUS community.
- The third SIRIUS yearly conference[10], a two-day event which brought together over 300 LEAs, Judicial Authorities, policy makers and OSPs to discuss challenges and latest developments in the field of cross-border access to e-evidence.
- The first edition of the EU Digital Evidence Situation Report[11], a new flagship product of SIRIUS that provides an analysis of the status of access of EU MS to e-evidence held by OSPs based outside the EU. Data was collected from transparency reports of selected OSPs, surveys and interviews with OSPs, LEAs and Judicial Authorities. The findings helped shed light on the perspective of companies in the e-evidence process, as well as common challenges encountered by LEAs and Judicial Authorities.
- The establishment of a close cooperation with Eurojust in order to open the provision of SIRIUS products and services to the judicial community, as well as to increase opportunities for the

[10] Europol, *Addressing Access to Cross-Border Electronic Evidence in the EU at the Third Annual Sirius Conference,* October 25, 2019, https://www.europol.europa.eu/newsroom/news/addressing-access-to-cross-border-electronic-evidence-in-eu-third-annual-sirius-conference

[11] EU IRU, *Sirius: European Union Digital Evidence Situation Report 2019,* December 19, 2019, https://www.europol.europa.eu/newsroom/news/sirius-european-union-digital-evidence-situation-report-2019

sharing of knowledge and best practices on cross-border access to e-evidence between the law enforcement and the judicial communities.

7. Horizon2020 projects

The EU IRU and SIRIUS are not the only players in Europe contributing to increasing the capacities of EU LEAs 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 LEAs.

In 2019, the unit therefore prepared an overview of the H2020 calls for proposals of interest and identified the projects whose results could help inform the work of the unit and of the SIRIUS community.

The unit is currently advising, in the capacity of Advisory Board member, or monitoring, ten specific projects. It also regularly takes part in events organised by the European Commission with the objective of creating new synergies and avoiding duplication and fragmentation.

A first tangible achievement was reached in 2019 when these projects participated in the SIRIUS conference, during which they presented their findings and upcoming activities.

8. Outreach activities

Collaboration with tech companies

One of the EU IRU's strategic key priorities in the field of prevention is the engagement with the private sector. Voluntary cooperation with the tech industry, based on mutual trust, is at the core of the EU IRU business. The Unit engages with OSPs that are exposed to terrorist content or are being exploited in the context of a terrorist activity. It supports their effort to deliver safer services to their users, through the exchange of best practices on the detection of terrorist content, expertise on trends and methods used by terrorist organisations or examples of pro-active measures to improve resilience. Cooperation with the private sector is fundamental in prevention and during 2019 the EU IRU built upon the trust-based relationship with the industry. The Unit's expertise informed major OSPs about edge cases and new forms of online abuse, supporting them to improve their detection mechanisms, build resilience and prevent the re-uploading of terrorist content.

As terrorists demonstrate continuous adaptability and exploit the potential of any tech service regardless of its size, the EU IRU needs to continuously expand its outreach and engage with newly exploited OSPs to inform about the extent of their abuse and offer support. On the basis of a tailored engagement plan, the Unit reaches out to about 200 platforms globally, on which terrorist jihadist content has been identified. The first outreach to the affected OSPs is initiated in the context of the referral process.

Ongoing processes and events

EU Crisis Protocol

In the aftermath of the 15 March 2019 terrorist attack in Christchurch, New Zealand issued a call for an international response to "eliminate terrorist or violent extremist content online". The speed and volume of Internet abuse during and in the immediate aftermath of the attack, as well as the vast number of

OSPs whose platforms and services were misused and exploited, highlighted the limitations of existing processes to address such threats.

In a bid to address this issue, New Zealand convened the Christchurch Call to Action Summit which took place in Paris on 15 May 2019. The Summit was chaired jointly by New Zealand's Prime Minister Jacinda Ardern and French President Emmanuel Macron. The meeting brought together a number of countries and tech companies, and resulted in the adoption of the Christchurch Call, which established common measures to tackle future threats. The European Commission, as a signatory of the Christchurch Call, committed to deliver on the commitments of the call through the EU Internet Forum. To this effect, Europol was requested by the European Commission to draft the European Crisis Protocol.

The draft Protocol was presented to the European Commission and EU Member States on 16 July 2019 within the framework of the EU Internet Forum. The Protocol 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 (and in particular Europol), OSPs and other relevant stakeholders in accordance with relevant legislation and within the relevant mandates, and to ensure effective coordination and management of the crisis[12].

The Tabletop Exercise

On 11 September 2019, the EU IRU organised a tabletop exercise (TTX) with EU Member States' LE authorities, third countries and OSPs at Europol's headquarters, under the umbrella of the European Commission-led EU Internet Forum[13].

The aim of the exercise was to inform and work on the development of the EU Crisis Protocol, to enable a coordinated response to a cross-border massive abuse of the Internet in the context of terrorism or violent extremism. The exercise was attended by EU MS (Belgium, Cyprus, Denmark, Finland, France, Germany, Italy, the Netherlands, Portugal, Slovenia, Spain, Sweden and the United Kingdom); third countries (Australia, Canada, Jordan and New Zealand); OSPs (Facebook, Files.fm, Google, Justpaste.it, Mega.nz, Microsoft, Telegram, Twitter and YouTube); and Tech Against Terrorism (an initiative working with the global tech industry to tackle terrorist use of the internet).

The TTX worked through a set of scenarios, each designed to simulate realistic examples of terrorist incidents and the dissemination of terrorist propaganda.

The TTX, the first of its kind since the launch of the Christchurch Call to Action, marked a milestone towards closer cooperation between all parties involved in improving the fight against terrorism online.

[12] European Commission, *Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol,* October 7, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009

[13] Europol, *Tabletop Exercise at Europol on Terrorist Content Dissemination Online*, September 16, 2019, https://www.europol.europa.eu/newsroom/news/tabletop-exercise-europol-terrorist-content-dissemination-online