HOW IS EUROPOL KEEPING ONLINE SPACES SAFE?

24 Nov 2021

Press Release

Feature article

Terrorism is a constant threat to societies all over the world and terrorists' use of the internet and social media has increased enormously in recent years. Jihadist groups, in particular, have demonstrated a sophisticated understanding of how social networks operate and have launched well-organised, concerted social media campaigns to recruit followers. These campaigns promote or glorify acts of terrorism and violent extremism and have led to viral online content in the past.

As a response to this, in 2015 the Justice and Home Affairs Council mandated Europol to create the EU Internet Referral Unit (EU IRU), as part of the wider EU Internet Forum, to reduce the impact of internet content promoting terrorism or violent extremism.

MONITORING TERRORIST CONTENT ONLINE

In recent years, the international community has been dealing with largely uncharted territory when it comes to online extremist content. However, the adoption of the EU(2021)/784 Regulation of April 2021 , which addresses the dissemination of online terrorist content, will change the European Counter Terrorism Centre's working relationship with Member States and tech companies and the responsibilities of the EU IRU will evolve along with this legislative change. In the coming months, Member States will be in a position to demand the removal of content from Online Service Providers themselves through a platform called PERCI. This platform is a technical solution built by

Europol and managed by the EU IRU to facilitate the implementation of the new regulation. Before this, the process to take down terrorist content online was entirely voluntary on the part of the tech companies.

> “
> ‘This is a historic moment because it touches upon the fundamental aspects of human rights and freedoms,’ says a specialist from the EU IRU. ‘On one hand we need to be sure, as Europeans, that we do not impact these rights and securitise the area; but at the same time we have to take real action to control the abuse of the internet by malicious actors. It’s a difficult balance to strike, but it has to be done.’
> ”

The vast majority of tech companies have taken significant steps to protect their platforms against terrorist abuse. Nevertheless, the online environment remains an attractive space for terrorist criminal networks who continue to target the services offered by the tech companies for recruitment, fundraising and propaganda purposes.

FIGHTING TERRORISM AND MIGRANT SMUGGLING

But how exactly does the EU IRU help keep online spaces safe? ‘It’s a round-the-clock operation,’ says the specialist, ‘once we identify terrorist content itself, we try to map its trace on the internet. We collect all publicly available information around this content and create a ‘referral package’ to be exploited for different purposes: to assess the threat, to support investigations and to suggest eventual referral to Online Service Providers.’ Referral is the transmission of a notification of internet content by Europol or Member States to the Online Service Providers.
Based on these referrals, the EU IRU also coordinates Referral Action Days. These are organised on a regular basis, both on Europol premises and remotely. Referral Action Days facilitate direct cooperation with law enforcement representatives in EU Member States and are imperative in Europol’s ongoing fight against terrorism. Since 2015, the EU IRU has organised a total of 23 Referral Action Days.

The EU IRU consists of four separate teams and employs a number of specialists with a variety of skills, including operational, linguistic, technical and research expertise. Specialists who work with Arabic, for example, are hired not only for these capabilities but also for their acute understanding of how the process of radicalisation to violent extremism works. ‘Language is very important in the phenomenon of jihadism,’ explains a specialist in this field, ‘but you also need to have a deep understanding of how the jihadist networks abuse the online environment to recruit and radicalise people.’

The scope of the EU IRU is not just limited to jihadist content either. Since the attack in Christchurch, New Zealand in 2019, there has been a surge in right-wing extremist content online. The EU IRU has recently taken steps to address non-jihadist content and has brought in experts to build this capacity within the European Counter Terrorism Centre at Europol. The EU IRU additionally provides support to Europol's European Migrant Smuggling Centre by flagging content used by traffickers offering smuggling services to migrants and refugees.

COLLABORATION AND TRUST

The EU IRU is in a unique position whereby it can map terrorist networks across borders and see how they are linked to cases in a variety of Member States. It is this global view that is instrumental ir dismantling criminal networks and providing information for investigations. The establishment of the EU Internet Forum, and subsequently the EU IRU, has greatly enhanced the voluntary cooperation between government, tech companies and civil society to counter online terrorism and violent extremism as part of the public-private partnership.

> ‘In the EU IRU, the European Counter Terrorism Centre, and Europol more generally, we respect fundamental rights and freedoms within a robust legal framework,’ says the specialist, ‘and this is why we are trusted by the international community, the companies we engage with, and Member States. We are very committed to building this trust- and trust is our biggest achievement at Europol.’

CRIME AREAS Terrorism
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

Source URL: https://www.europol.europa.eu/newsroom/news/how-europol-keeping-online-spaces-safe