Съфинансирано от
Европейския съюз

Capacity Building Through Exchange of Good Practices & Research in the Security Domain

Module 2: Radicalism

Topic: Online Radicalisation

Author: Andrew Staniforth

Date: December 2024

Проект „Укрепване на капацитет, обмен на опит и изследователска дейност в сферата на сигурността“, номер BG65ISPR001-3.004-0002, с договор 812108-68-02.10.2024, е финансиран по Програмата на Република България по фонд „Вътрешна сигурност“ за периода 2021 – 2027 г.

Table of Contents

Introduction 3

Aim 3

Topic syllabus 3

Learning objectives 4

Learning outcomes 4

Reading list 5

Presentation notes 6

Topic content. 19

Sources of information 35

1. Introduction

This report provides the topic syllabus for the *Online Radicalisation* topic for Module 2 of the Internal Security Fund (ISF) project *Capacity building through exchange of good practices and research in the security domain* led by the European Institute Foundation. This report provides the aim, objectives, reading list, presentation notes, topic content and sources of information for delivery of this topic.

2. Aim

The aim of the *Online Radicalisation* topic is:-

> *"To examine and explore the impact of the internet and social media on the radicalisation and recruitment of individuals towards violent extremism and terrorism, including countermeasures to prevent terrorist content online."*

3. Topic syllabus

To ensure that all students attending have a clear understanding of 'Online Radicalisation' this topic is divided into four parts as follows:

- **Part 1: Online terror threats –** introducing the online terrorist threat landscape and how terrorists use the internet to conduct their operations, including for the recruitment and radicalisation of individuals to their cause. This first section will include a counter-terrorism investigation case study to showcase the threat posed by terrorist use of the internet.
- **Part 2: Online terrorist activity –** examining how terrorists use the internet, including research published by Tech Against Terrorism providing evidence of the scale of the threat and the operational challenges to detect and deter their online activities on multiple websites, platforms and other online services.
- **Part 3: Countermeasures –** exploring the concept of collaboration in counter-terrorism, and how public and private partnerships are required to tackle online terrorist content with research evidence encouraging the increased cooperation between law enforcement agencies and technology social media companies and the impact on law enforcement agency operating cultures and practices.
- **Part 4: Terrorist Content Online Regulation –** explaining the new EU TCO Regulation, including the reasons for enactment, provisions, powers and the proactive role and

responsibility of host service providers to remove identified terrorist content on their platforms and the challenges to comply with, and enforce, the regulations.

4. Learning objectives

The primary learning objectives of the *Online Radicalisation* topic are to:

1. Examine how terrorists use the internet to conduct their operations
2. Explore how online terrorists recruit and radicalise individuals to their cause
3. Examine the multiple threat vectors posed by the terrorist use of the internet
4. Identify the tactics used by terrorists to carry out their online operations
5. Explore the scale of the challenge to detect and deter online terrorist content
6. Examine how law enforcement specialist units are tackling online terrorist content
7. Explore the role of technology and social media companies in tackling online terrorism
8. Examine collaborative approaches between law enforcement agencies and social media companies to tackle online terrorist content
9. Examine the powers and provisions of the EU TCO Regulation
10. Explore compliance and enforcement challenges of the EU TCO Regulation

5. Learning outcomes

At the completion and conclusion of the *Online Radicalisation* topic presentation, students will be able to:-

- Explain why terrorists use the internet to conduct their operations
- Explain how terrorists use the internet to recruit and radicalise individuals to their cause
- Explain the multiple threat vectors posed by the terrorist use of the internet
- Explain the dangers posed by terrorist hosted websites on the surface web
- Identify the tactics used by terrorists to carry out their online operations
- Describe the scale of the challenge to detect and deter online terrorist content
- Explain the important role of specialist counter terrorism police units in tackling online terrorist content and the challenges they encounter
- Explain the role and function of the EU Counter Terrorism Internet Referral Unit at Europol
- Describe how collaboration and cooperation between law enforcement agencies and social media companies is crucial to tackle contemporary online terrorist content
- Explain how law enforcement agencies and social media companies may increase their collaborative approaches to better tackle online terrorist content together
- Explain the powers and provisions of the EU TCO Regulation
- Describe the challenges faced by small and micro host service providers in complying with the provisions of the EU TCO Regulation
- Describe the challenges of competent authorities in enforcing the provisions the EU TCO Regulation

- Signpost host service providers, technology and social media companies, as well as law enforcement agencies and other related stakeholders to EU training and tools to develop their knowledge, awareness and compliance with the EU TCO Regulation.

6. Reading list

The following list of reports, papers, websites and articles are recommended reading on the wider topic of *Online Radicalisation* which complement the topic presentation and will add value to the students learning experience and includes:-

1. Tech Against Terrorism, ***Transparency Report of the Terrorist Content Analytics Platform*** (22 August 2023) Available online at: https://techagainstterrorism.org/news/terrorist-content-analytics-platform-second-annual-transparency-report
2. Tech Against Terrorism, ***Patterns of Online Terrorist Exploitation*** (28 April 2023) Available online at: https://techagainstterrorism.org/news/patterns-of-online-terrorist-exploitation
3. Tech Against Terrorism Europe, ***The challenges that small and micro host service providers face in implementing the TCO Regulation*** (September 2024) Available online at: https://tate.techagainstterrorism.org/news/report-the-challenges-that-small-and-micro-hsps-face-in-implementing-the-tco-regulation
4. European Union, ***Counter Terrorism Agenda 2020*** (9/12/2020) Available online at: https://home-affairs.ec.europa.eu/document/download/9b54c533-139a-4662-99cf-b5f72220bb18_en?filename=09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf
5. Tech Against Terrorism, ***Mapping Far-Right Terrorist Propaganda Online*** (20 May 2024) Available online at: https://techagainstterrorism.org/news/report-mapping-far-right-terrorist-propaganda-online
6. European Commission, ***Report on the operation of the Terrorist Content Online Regulation*** (February 2023) Available online at: https://home-affairs.ec.europa.eu/document/download/506de61d-c53f-489f-a9e3-e16e78793e81_en?filename=202104_terrorist-content-online_en.pdf
7. European Commission, ***An Introduction to the Terrorist Content Online Regulation*** (April 2021) Available online at: https://home-affairs.ec.europa.eu/document/download/506de61d-c53f-489f-a9e3-e16e78793e81_en?filename=202104_terrorist-content-online_en.pdf
8. Staniforth, A ***Combatting terrorist content online: Proactive AI detection*** (4/1/2024) Policing Insight, Available online at: https://policinginsight.com/feature/innovation/combatting-terrorist-content-online-proactive-ai-detection/
9. Europol, ***European Union Terrorism Situation and Trends Report 2024*** (16 December 2024) Available online at: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat

10. Macdonald, S & Staniforth, A ***Tackling Online Terrorist Content Together – Cooperation Between Counter Terrorism Law Enforcement and Technology Companies*** (24 January 2023) Global Network on Extremism & Technology (GNET) Available online at: https://gnet-research.org/2023/01/24/tackling-online-terrorist-content-together-cooperation-between-counterterrorism-law-enforcement-and-technology-companies/

7. Presentation notes

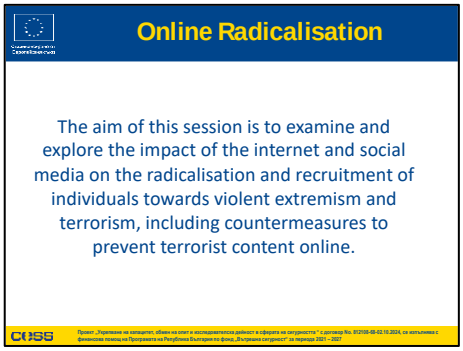
These presentation notes are intended to support and guide the trainer through the '*Online Radicalisation'* topic syllabus ensuring all learning objectives and learning outcomes are achieved. These presentation notes should be read in conjunction with the topic text in section 8 of this report detailed below. The presentation notes provide the key messages which should be covered and communicated to students during the session. The duration of this topic presentation, included question and answers sessions throughout the presentation, is approximately 90 minutes.

SLIDE 1 – Welcome & Introduction



Introduction, welcome, title of the session **'***Online Radicalisation – Analysing the role of the internet and social media in radicalisation and recruitment'.*

SLIDE 2 – Aim of the session



The aim of this session is to examine and explore the impact of the internet and social media on the radicalisation and recruitment of individuals towards violent extremism and terrorism, including countermeasures to prevent terrorist content online.

SLIDE 3 – Session syllabus



Analysing the role of the internet and social media in radicalisation and recruitment:

- Part 1: Online terror threats
- Part 2: Online terrorist activity
- Part 3:Countermeasures
- Part 4: Terrorist Content Online Regulation

SLIDE 4 – Online Radicalisation



Modern terrorism has rapidly evolved becoming increasingly non-physical, with vulnerable 'home grown' citizens being recruited, radicalised, trained and tasked online. It would be Unwise to underestimate how the internet has rapidly changed – and continues to change – the very nature of terrorism. The internet is well suited to the nature of terrorism and the psyche of the terrorist. In particular, the ability to remain anonymous makes the deep and darkest corners of the internet attractive to the terrorist plotter.

SLIDE 5 – Scale of the challenge



The dissemination of propaganda online is a strategic priority for terrorist groups. Terrorist groups and their sympathisers post an enormous volume of content, such that in the year up to September 2022 Facebook had removed a total of 54 million items of terrorist content. In the same period, YouTube removed 273,016 videos that promoted violence and violent extremism, while in 2021 Twitter suspended a total of 112,360 accounts for the same reason.

The dissemination of terrorist content is not confined to the biggest platforms nor is terrorist exploitation of online platforms limited to social media. A variety of other services are also exploited. For example, from December 2020 to November 2021, Tech Against Terrorism alerted 65 different tech companies to terrorist content on their platforms. These spanned 13 different service types, including file-sharing, archiving, link shortening, book subscriptions and web hosting.

For more than a decade, stakeholders have emphasised the importance of public-private partnership in tackling terrorists' use of the Internet, particularly cooperation with tech companies. Tech companies have publicly stated their commitment to cooperation with law enforcement and vice versa. Law enforcement in several countries has established specialist units, who work to identify online terrorist content and refer it to the host platform for removal.

The UK's Counter-Terrorism Internet Referral Unit (CTIRU), established by the UK Metropolitan Police in 2010, contributed to the removal of 310,000 pieces of content during its first eight years. Following the CTIRU model, the EU's Internet Referral Unit (EU IRU) was established in 2015 within Europol who believe cooperation with tech companies is a strategic priority, the aim being to exchange best practices and specific measures to improve the referral process and content moderation to better tackle online terrorist content.

SLIDE 6 – Part 1: Online Terror Threats



PART 1: Online Terror threats – Why do terrorists use the internet to conduct their operations?

SLIDE 7 – Part 1: Online Terror Threats



The Internet has revolutionized terrorism in many ways. For example, activities that were once conducted face-to-face, such as fundraising or training, are now conducted through websites and virtual training camps. Geospatial imagery, such as Google Earth, can be used to study locations and plan potential attacks. Hacking and cyber-attacks present the possibility that great harm can be done to a country's infrastructure from a computer halfway across the world. Likewise, the Internet has emerged as a dangerous tool for terrorist propaganda and recruitment purposes. There are at least nine key ways that the Internet has changed the way that terrorists use propaganda.

Limitless content: First, social media allows terrorist groups to provide limitless content directly to numerous websites or individuals, without having to go through a third party. Traditionally, the media had a monopoly on covering and interpreting terrorist incidents. Now, terrorists have the ability to instantly convey their messages directly to their target audience. The terrorists can also tailor their recruiting pitch, sending different messages to individuals based on their age, gender, location, or other factors.

Efficient recruitment: Social media provides terrorist organizations with an efficient way to recruit new members, spread propaganda, and spread their ideology to a large audience with minimal effort. Physical geography is no barrier to communications between potential recruits and terrorists. Terrorists can create any number of account names on social media platforms, making communication cheap, easy, and almost impossible to stop. Twitter and other social media platforms have attempted to thwart terrorist groups by suspending ISIS-supporting Twitter accounts, only to find that the accounts are replaced quickly by other ISIS-

supporting accounts.

Low barrier of access: Third, social media "lowers the barrier of access" to terrorist propaganda. Social media platforms provide individuals with ways to easily reach terrorist propaganda and terrorist users. Unlike terrorist websites, which typically require individuals to intentionally locate the specific site, individuals may also stumble across terrorist social media accidently.

Unregulated domain: Internet postings are not regulated as sources of news, and thus terrorists can post inaccurate information with almost no oversight or regulation. The Internet removes the ability to effectively pre-screen content by allowing for instantaneous broadcast of terrorist messages. Readers might con- sider terrorist Internet postings to be factually correct, and the stories may go unchecked.

Anonymity: Terrorists can use anonymity on the Internet to their advantage. The anonymity of the Internet has been found to foster higher levels of violence in people. Terrorists can encourage feelings of violence, drawing people to their cause. Anonymity also allows the terrorists to evade detection by law enforcement. Previously, if terrorists communicated by electronics, they were limited to using telephones or radios, which were at risk of being monitored by electronic surveillance tools such as wiretaps. Now, individuals can make countless usernames that mask their true identities on numerous platforms.

Expert knowledge: Terrorists can gain knowledge about social media in order to distort the prevalence and ranking of their messages on search results. Social media, in particular Twitter, allows terrorists to amplify their messages by posting links to their propaganda and "hashtags" at an unnaturally fast pace, causing the postings to place higher in search results and in content aggregated by third parties. ISIS and al Qaeda reportedly both use "bots," which are computer- controlled Twitter accounts that automatically send out content in a similar manner.

Multidirectional communications: The Internet allows for multidirectional communication between the terrorists and the potential recruits. Individual communication allows terrorists to craft propaganda specifically tailored for certain types of individuals. Further- more, interactive participation can foster a sense of cohesion and generate a sort of virtual community between the terrorists and potential recruits, thereby creating a sense of unity.

Targeting the vulnerable: Terrorist groups can use social media to search for and target individuals who might be particularly vulnerable to their ideology. For example, ISIS utilizes social media platforms that are popular with teenagers to attract and recruit young people, who are more susceptible to its propaganda. Terrorists can craft their propaganda to appeal to certain vulnerable populations by portraying their organization as the solution to individuals' problems. Furthermore, terrorists can weed out less susceptible populations by blocking apparent nonbelievers from their communications.

Encryption privacy: Encryption allows terrorists to maintain private networks of communication without law enforcement oversight. Encrypted communications cannot be easily accessed by law enforcement, and as such, recruitment efforts and other terrorist activities can take place in relative secrecy. As more websites and smartphone applications turn to encryption, its ability to hide such communications and actions will likely be a growing

concern. In September 2014, Apple and Google announced plans to strengthen encryption of data stored on smart- phones using their operating systems. Two encrypted messaging applications, WhatsApp and Kik, have been especially popular with ISIS. These applications make it much more difficult for law enforcement to intercept communications than would otherwise be possible on Twitter or Facebook.

SLIDE 8 – Part 1: Online Terror Threats



Cyber terrorist case study: An early of example of the terrorist's creative use of the Internet is the case of Younes Tsouli. When police officers raided a flat in West London during October 2005, they arrested a young man, Younes Tsouli. The significance of this arrest was not immediately clear, but investigations soon revealed that the Moroccan born Tsouli was the world's most wanted 'cyber-terrorist'. In his activities Tsouli adopted the username 'Irhabi 007', (Irhabi meaning 'terrorist' in Arabic), and his activities grew from posting advice on the internet on how to hack into mainframe computer systems to assisting those in planning terrorist attacks. Tsouli trawled the internet searching for home movies made by US soldiers that would reveal the inside of US military bases. Over time these small pieces of information were collated and passed to those planning attacks. This virtual hostile reconnaissance provided insider data illustrating how it was no longer necessary for terrorists to conduct physical reconnaissance if relevant information can be pieced together from the internet. Police investigations subsequently revealed that Tsouli had €2.5million worth of fraudulent transactions passing through his accounts which he used to support and finance terrorist activity. Pleading guilty to charges of incitement to commit acts of terrorism Tsouli received a 16-year custodial sentence to be served at Belmarsh High Security Prison in London where, perhaps unsurprisingly, he has been denied access to the internet. The then National Coordinator of Terrorist Investigations, Deputy Assistant Commissioner Peter Clarke, said that Tsouli 'provided a link to core al Qaida, to the heart of al Qaida and the wider network that he was linking into through the internet', going on to say 'what it did show us was the extent to which they could conduct operational planning on the internet. It was the first virtual conspiracy to murder that we had seen.'

SLIDE 9 – Part 2: Online Terrorist Activity



PART 2 - Online terrorist activity: As an example of extent of online terrorist activity, during 2022, Tech Against Terrorism published a report on The Threat of Terrorist and Violent Extremist Operated Websites which found that terrorist and violent extremist actors were running at least 198 websites on the surface web. Further in-depth analysis of 33 of the most prominent websites – run by actors such as IS Al Qaeda, Atomwaffen Division, and the Taliban – confirmed that these sites had 1.54 million monthly visitors, with the majority of visits coming from Algeria, Pakistan, United States, and the UK.

The scale of the threat from websites operated by terrorists and extremists reported by Tech Against Terrorism is shocking and demonstrates the scale of the security challenge for all in authority engaged in counter terrorism across the world. Adam Hadley, Founder and Director of Tech Against Terrorism stated: "The fact that terrorists and violent extremists are able to operate hundreds of websites attracting millions of views with impunity is a failure on behalf of the global online counter terrorism sector. Terrorist operated websites is the key strategic threat with regards to terrorist use of the internet. It is clear that policymakers need to devote more political capital towards identifying practical and policy-oriented solutions to this challenge."

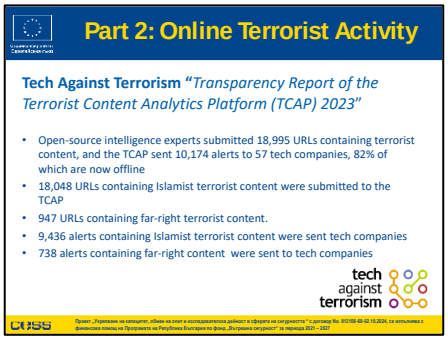
Since January 2021, Tech Against Terrorism has conducted open-source intelligence (OSINT) research into the threat of terrorism and violent extremist operated websites. Their methodology comprised of keyword searches across several mainstream and niche social media and messaging apps, as well as search engines and bespoke apps, mostly conducting searches in English and Arabic, though also in Dari, Pashto and Russian. Tech Against Terrorism also identified terrorist and violent extremist operated websites through daily monitoring of online terrorist spaces that were likely to promote such sites, such as social media platforms and messaging platforms.

The daily monitoring encompassed both mainstream and niche social media, video sharing platforms, and messaging platforms. The 198 websites identified by Tech Against Terrorism included sites which promoted violent extremist ideologies such as Neo-Nazism, violent insurrectionary accelerationism, Salafi-Jihadism, and Incel ideology. Analysis of these sites found that: 101 websites were operated by far-right violent extremist or terrorist groups; 79 websites were operated by violent Sunni Islamist extremist or terrorist groups; and 18 websites were operated by violent Shia Islamist extremist or terrorist groups. A sample analysis of 33 of these websites – run by groups such as ISIS, Al

Qaeda, Atomwaffen Division, Combat 18, and the Taliban – found that they had a total of 1.54 million monthly visits with 91% displaying audio and visual propaganda. Moreover, the sample analysis revealed that 73% contained an archive of historic terrorist content and 57% included a contact address form.

The Tech Against Terrorism report indicates that terrorist operated websites constitute a key propaganda organ for terrorist and violent extremist groups which allows groups to disseminate recruitment material without disruption. The rise in prominence of terrorist operated websites is likely the result of improved removal campaigns across other parts of the tech industry, including on larger social media platforms.

SLIDE 10 – Part 2: Online Terrorist Activity



The second Transparency Report of the Terrorist Content Analytics Platform (TCAP) published in 2023 by Tech Against Terrorism, outlined the progress of the world's largest alert platform for verified terrorist content, collected in real time. The Platform notifies technology companies of the presence of such content on their platforms. The Transparency Report detailed the extent and scale of terrorist content discovered by Tech Against Terrorism's Terrorist Content Analytics Platform and how the data gathered is utilised to disrupt and understand terrorist and violent exploitation of the internet. The report found that between 1 December 2021 and 30 November 2022:

- Open-source intelligence experts submitted 18,995 URLs containing terrorist content, and the TCAP sent 10,174 alerts to 57 tech companies, 82% of which are now offline. In total, 150 tech companies are registered and able to receive alerts as soon as we detect terrorist content on their platforms. We have increased the number of platforms we can alert from 114 in Year 1.
- Most of the content we have alerted has been related to Islamist terrorist entities (92% of alerts in Year 2). This is compared to 98% of alerts containing Islamist terrorist content in Year 1 of the TCAP.
- Because of alerts from the TCAP, an average of 84% of Islamist terrorist content was removed, whilst an average 61% of far-right terrorist content was removed. Compared to our previous Transparency Report, the takedown rate for Islamist terrorist content has decreased from 94% but has increased from 50% for far-right terrorist content.
- 18,048 URLs containing Islamist terrorist content were submitted to the TCAP, compared to 947 URLs containing far-right terrorist content. 9,436 alerts containing Islamist terrorist content were sent, whilst 738 alerts containing far-right terrorist content have been sent to tech companies. The discrepancy in numbers is due to the different propaganda

dissemination techniques employed by far-right and Islamist terrorist groups. However, we have begun to close the gap between Islamist and far-right terrorist content submissions and alerts and this difference is smaller than in Year 1.

The analyses conducted by Tech Against Terrorism concludes that there is currently no unified global approach against terrorist operated websites, and their recommendation is that governments should step in and create a strategy to disrupt terrorist operated websites based on collaborative engagement with web infrastructure providers and on human rights safeguards. What is clear from the findings in the Tech Against Terrorism report is that responses to terrorist and violent extremist operated websites can be severe in that they often constitute the removal or blocking of entire websites. There are therefore several ethical challenges posed by tackling websites to ensure firm but fair responses are put in place and tighter regulation may be preferrable to more anti-terror legislation which, if used disproportionately, can have potential long-term damaging consequences on fundamental human rights.

SLIDE 11 – Part 3: Countermeasures



PART 3 – Countermeasures - What can we do to counter this online terror threat? While citizens in western nations have enjoyed protection from terrorism and violent extremism under the aegis of various departments and agencies across the landscape of government, critical to the future success of contemporary counter terrorism and violent extremism is the cooperation between law enforcement and social media platforms. This collaboration between very different emanations of state power and private enterprise is now considered essential to keep citizens safe. And while their cultures and operating practices are very different and not without them imperfections, they must now seek to identify ways in which to meld and amplify their approach to tackle terrorist online content for mutual benefit. There have been recent developments providing encouragement and evidence that law enforcement and social media
platforms are now beginning to work together but these efforts are isolated cases, and cooperation remains fractured and in its infancy.

A truly cooperative and interoperable approach, where law enforcement and social media bring their expertise to bear in concert with one another to tackle online terrorist content as part of their operating cultures and practices has yet to be fully achieved. There are impediments to close cooperation between police authorities and the private sector. Tech companies and law enforcement have very different cultures and operating practices. There have been high-profile instances of non-cooperation. Concerns have also been raised about the informality of existing collaborations.

To guard against the possibility of censorship, mission creep and a lack of accountability and oversight, there have been calls for all requests submitted to tech companies from state authorities to be subjected to rigorous scrutiny, accompanied by detailed reporting requirements to ensure transparency. The policy challenge is to address the impediments to cooperation between law enforcement and the tech sector in order to achieve the collaboration that is widely accepted as necessary to tackle online terrorist content, while ensuring that such cooperation meets the demands of due process and accountability

SLIDE 12 – Part 3: Countermeasures



In 2023, the Global Network on Extremism and technology (GNET),published a report 'Tackling Online Terrorist Content Together: Cooperation between Counterterrorism Law Enforcement and Technology Companies'. The findings of this research provide unique insights into the context and operating environment of members of law enforcement and tech companies engaged in the highly specialised counterterrorism field of online terrorist content removal.

From a law enforcement perspective, it is clear that the rapid pace of social and technical innovation has resulted in an increasingly interconnected and interdependent world, in which many new hazards have a transnational dimension. This has necessitated a significant shift in approach to counterterrorism. Tech companies are the driving force behind this dynamic change in society, sometimes with unintended consequences for safety and security. But while the tendency has been to highlight the differences between tech companies and law enforcement agencies, this research report provides evidence of an understanding of the common vision shared by both sides to keep people safe online.

The processes and professional partnerships that have been developed are, in part, the product of tech companies' investment in establishing dedicated teams to remove terrorist content. This investment has included the recruitment and buy-in of much needed knowledge and expertise, including hiring personnel with law enforcement backgrounds. The establishment of these teams, coupled with the development and delivery of bespoke training, has led to an improved understanding of each other's roles.

The findings also reveal positive working practices of tech companies providing direct and fast access to data at times of critical threat, as well as making personnel available to work within and alongside police counterterrorism operations in response to major terrorist events. These developments provide evidence of a real commitment to tackle terrorism and reveal existing models of cooperation upon which future collaboration can be founded.

It is noteworthy that the research findings did not contain any demands from law enforcement for a more robust regulatory or legislative framework for the removal of online terrorist

content. On the contrary, what emerged was a more nuanced, practical and pragmatic approach by police officers who have invested time and resources into developing positive relations with individual tech companies.

The law enforcement interviewees expressed concerns about the utility of new legislation, particularly at a national level, with the most common concern being that such legislation could impede voluntary cooperation and mark a return to the "transactional" relationship of the past. Perhaps it is unsurprising that police officers wish to protect the professional partnerships that they have built over time with their counterparts in tech companies.

Nonetheless, the only justification that the law enforcement interviewees offered for new legislation was that it might increase public confidence in how this issue is being tackled. In contrast, it was the tech sector participants who had misgivings about the informality of the existing referral process, citing concerns about mission creep and transparency.

From their perspective, response times can be slowed as a result of insufficient information being provided and because some requests are not terrorism-related and so have to be redirected within the organisation. There was also a sense that the tech sector's improvements in transparency reporting should be mirrored by state authorities requesting takedowns or shutdowns. This has particular force where an informal referral process is utilised in preference to a formal statutory procedure for content takedown, such as in the UK.

While the cultures and operating practices of law enforcement and tech companies are very different, strides have been made towards an increasingly open and cooperative relationship in recent years. Nonetheless, such cooperation remains in its infancy and tensions remain.

From a policy perspective, the challenge is to resolve these tensions, given the value of cooperation to tackling online terrorist content, while simultaneously addressing the concerns about due process and accountability that stem from the informality of current arrangements. The following recommendations are highlighted and offered in an attempt to meet this policy challenge with measures that can be implemented with immediate effect:

- The development of an ***experience exchange programme*** affording the opportunity for identified personnel within counterterrorism policing and tech companies to be embedded within each other's counterterrorism operational functions.
- The implementation of a ***takedown-shutdown counterterrorism*** policing protocol, providing clarity following review of current practices for content takedown and account shutdown referrals.
- The development of a ***joint upstreaming programme***, which seeks to deliver a fundamental shift in emphasis from the removal of terrorist content online to preventing its initial publication.
- The development of ***joint strategic research requirements***, identifying and prioritising areas of mutual concern for further development and investigation through research.

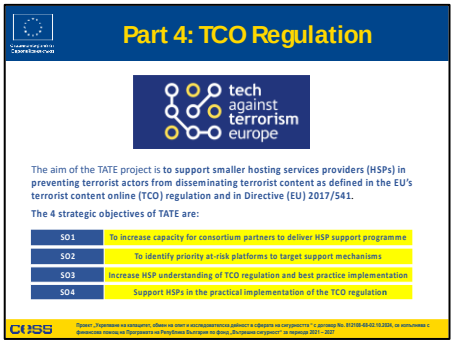
The research report concludes that as the sustained threat from terrorism in all its forms persists, a more progressive, cooperative and collaborative partnership between law enforcement agencies and tech companies must be encouraged. Adopting these recommendations will support transforming this partnership.

SLIDE 13 – Part 4: TCO Regulation



PART 4 - TCO Regulation: Social media platforms and host service providers (HSPs) are now subject to increased regulation in the global effort to tackle harmful terrorist online. The EU's Terrorist Content Online (TCO) regulation addressing the dissemination of terrorist content entered into application on 7 June 2022. These regulations were brought forward because of a series of critical factors, which included the high volume of hostile content that overwhelms all government agencies capacity and capability to prevent it and keep the public safe online. Despite voluntary measures and non-binding recommendations which bore fruit to reduce the availability of terrorist content online, limitations including the small number of HSPs adopting voluntary mechanisms, as well as the fragmentation of procedural rules across EU Member States, limited the effectiveness and the efficiency of cooperation among Member States and HSPs making it necessary to establish regulatory measures. Therefore, the effective application of the TCO Regulation is key to address the dissemination of terrorist content online across Europe, and the European Commission has proactively supported national competent authorities in this process to enforce the regulations, but a recent report published by Tech Against Terrorism Europe (TATE) suggests more needs to be done.

SLIDE 14 – Part 4: TCO Regulation



Introduce TATE, partners, aims and objectives: Recognising the challenge for HSPs, the TATE initiative, supported by the EU's Internal Security Fund (ISF), has recently published a study which aimed to speak to small and micro HSPs to understand what they regard as the main obstacles they face in implementing and complying with the requirements of the EU's TCO. In total, 49 HSPs were invited to participate in the study, and these invitations yielded 15 interviews with participants based in six different countries. The findings of the study will be of interest to police counter terrorism units engaged in internet referrals in the UK, across the

EU, and beyond EU borders, as well as those police personnel and partners engaged in the prevention of terrorism and violent extremism online.

Interviewees identified a number of challenges that small and micro platforms face in complying with the TCO Regulation, as many may lack the necessary expertise, both in terms of the legal knowledge required to navigate multiple regulatory regimes and their terminology, and the subject-matter understanding needed to identify terrorist content correctly. One specific challenge that interviewees faced was to define what content is 'terrorist'. While some companies chose to sidestep this task – simply using the term 'terrorism' without defining it – most had either developed a list of designated organisations or adopted a generic, dictionary-style definition.

One issue common to both of these approaches was the difficulty choosing between different official designation lists and definitions. Interestingly, none of the interviewees in the study said that they had adopted the TCO Regulation's definition of terrorist content, though they felt it is broadly similar to the definition they have chosen to use. The TCO Regulation's one-hour removal window was a cause of grave concern to small and micro HSPs.

Interviewees described it as a source of significant anxiety, even stating that the pressure it places on a small team has had a significant impact on their wellbeing. Some interviewees were also concerned about the possibility of receiving bogus removal orders and called for a mechanism by which the validity of any order received could be verified.

For all of these reasons, interviewees felt that some companies might choose not to engage with the TCO Regulation – particularly if they have never been contacted by a competent authority and believe they are under-the-radar. On the other hand, they identified several reasons for seeking to comply, including the business' reputation and long-term prospects for success and the intrinsic desire to combat terrorism online.

Various coping strategies have been adopted by companies that are motivated to comply, but struggle with resource limitations. Some have developed organisational practices that ensure someone is always on duty, in case a removal order should arrive. Other strategies were to simply defer to those referring the content and to outsource content moderation to Trust and Safety vendors (although some concerns were raised here about these vendors' lack of transparency).

The TATE study reveals that there is an ongoing need to raise awareness and understanding of the TCO Regulation and recommends that it would be desirable to ensure that each Member State has a national clearinghouse, that is able to provide advice and support to companies in their native language. The study also suggests that competent authorities should avoid an enforcement-led approach if a company is engaging with the TCO Regulation and striving to remove terrorist content from its platform promptly. Some understanding of the difficulty in always responding to a removal order within one hour should be shown where small HSPs are making a concerted effort to comply with the TCO Regulation's requirements but where platforms are non-responsive or uncooperative, the study is robust in its recommendation that enforcement action is taken – even if this is likely to prove time-consuming and resource intensive.

SLIDE 15 – Part 4: TCO Regulation



Introduce the TCO Cluster projects of TATE, FRISOC and ALLIES.

SLIDE 16 – Conclusions & Key Takeaways



The EU IRU detects and investigates malicious content on the internet and in social media and recognises that terrorists' use of the internet and social media has increased enormously over the course of recent years. The EU IRU reveal that Jihadist groups, have demonstrated a sophisticated understanding of how social networks operate and have launched highly sophisticated, concerted social media campaigns to recruit followers and to promote or glorify acts of terrorism and violent extremism. The EU IRU comprises of a team of experts with multiple and diverse knowledge and skills, ranging from experts in religiously inspired terrorism, translators, information and communications technology developers and law enforcement experts in counter terrorism.

Since it was set up, the EU IRU has assessed in total 42 066 pieces of content, which triggered 40 714 decisions for referral across over 80 platforms in more than 10 languages. On average, the content flagged for referrals has been removed in 86% of the cases. Responding to the threat of terrorist-operated websites is a crucial part of the EU IRU's ongoing work, which serve as key platforms for the dissemination of violent ideologies.

These websites enable terrorist organisations and violent extremists to bypass the enhanced moderation and content removal efforts of mainstream online service providers, allowing them to maintain a persistent online presence. Identifying, flagging, investigating and disrupting these websites has become a key function of the EU IRU.

The TCO Regulation, which came into effect from June 2022, provides a legal framework to ensure that hosting service providers are obliged to remove terrorist content within one hour of receiving a removal order from Member State authorities. The Regulation applies to all

hosting service providers offering services within the EU, including providers of social media, video, image and audio-sharing services.

The new legal and regulatory provisions to tackle online terrorist content provides the effective tools for Europol to carry out their mission which is reinforced through the regulation which now amplifies the mandate of Europol as the European criminal police agency, expanding its capability to tackle online terrorist content.

SLIDE 17 – Any Questions?



Question and answer session, thank you and close.

8. Topic content

8.1 Introduction

Modern terrorism has rapidly evolved becoming increasingly non-physical, with vulnerable 'home grown' citizens being recruited, radicalised, trained and tasked online. It would be unwise to underestimate how the internet has rapidly changed – and continues to change – the very nature of terrorism. The internet is well suited to the nature of terrorism and the psyche of the terrorist. In particular, the ability to remain anonymous makes the deep and darkest corners of the internet attractive to the terrorist plotter.

The dissemination of propaganda online is a strategic priority for terrorist groups. Terrorist groups and their sympathisers post an enormous volume of content, such that in the year up to September 2022 Facebook had removed a total of 54 million items of terrorist content. In the same period, YouTube removed 273,016 videos that promoted violence and violent extremism, while in 2021 Twitter suspended a total of 112,360 accounts for the same reason. The dissemination of terrorist content is not confined to the biggest platforms nor is terrorist exploitation of online platforms limited to social media. A variety of other services are also exploited. For example, from December 2020 to November 2021, Tech Against Terrorism alerted 65 different tech companies to terrorist content on their platforms. These spanned 13 different service types, including file-sharing, archiving, link shortening, book subscriptions and web hosting.

For more than a decade, stakeholders have emphasised the importance of public-private partnership in tackling terrorists' use of the Internet, particularly cooperation with tech

companies. Tech companies have publicly stated their commitment to cooperation with law enforcement and vice versa. Law enforcement in several countries has established specialist units, who work to identify online terrorist content and refer it to the host platform for removal. The UK's Counter-Terrorism Internet Referral Unit (CTIRU), established by the UK Metropolitan Police in 2010, contributed to the removal of 310,000 pieces of content during its first eight years. Following the CTIRU model, the EU's Internet Referral Unit (EU IRU) was established in 2015 within Europol who believe cooperation with tech companies is a strategic priority, the aim being to exchange best practices and specific measures to improve the referral process and content moderation to better tackle online terrorist content.

8.2 Online terror threats

The Internet has revolutionized terrorism in many ways. For example, activities that were once conducted face-to-face, such as fundraising or training, are now conducted through websites and virtual training camps. Geospatial imagery, such as Google Earth, can be used to study locations and plan potential attacks. Hacking and cyber-attacks present the possibility that great harm can be done to a country's infrastructure from a computer halfway across the world. Likewise, the Internet has emerged as a dangerous tool for terrorist propaganda and recruitment purposes. There are at least nine key ways that the Internet has changed the way that terrorists use propaganda.

8.2.1 Limitless content

First, social media allows terrorist groups to provide limitless content directly to numerous websites or individuals, without having to go through a third party. Traditionally, the media had a monopoly on covering and interpreting terrorist incidents. Now, terrorists have the ability to instantly convey their messages directly to their target audience. The terrorists can also tailor their recruiting pitch, sending different messages to individuals based on their age, gender, location, or other factors. For example, ISIS sends starkly different messages to Muslims in the West than those closer to the Middle East. The messages to English speakers tend to highlight jihad as a means of personal fulfilment and tend to be softer in nature than the messages in Arabic, and the Arabic media messages tend to focus on jihad as a duty for all Muslims.

8.2.2 Efficient recruitment

Social media provides terrorist organizations with an efficient way to recruit new members, spread propaganda, and spread their ideology to a large audience with minimal effort. Physical geography is no barrier to communications between potential recruits and terrorists. Terrorists can create any number of account names on social media platforms, making communication cheap, easy, and almost impossible to stop. Twitter and other social media platforms have attempted to thwart terrorist groups by suspending ISIS-supporting Twitter accounts, only to find that the accounts are replaced quickly by other ISIS- supporting accounts. Like the mythical Hydra, the suspension of an ISIS- supporting Twitter account seems to yield two more ISIS-supporting accounts in its place.

8.2.3 Low barrier of access

Third, social media “lowers the barrier of access” to terrorist propaganda. Social media platforms provide individuals with ways to easily reach terrorist propaganda and terrorist users. Unlike terrorist websites, which typically require individuals to intentionally locate the specific site, individuals may also stumble across terrorist social media accidently. For example, an individual may click on a link posted by a friend and unintentionally land on a jihadist forum. Furthermore, smart phones have made it possible for individuals to constantly have access to the Internet at almost all times and places. Thus, physical location and time are no longer relevant constraints on an individual’s ability to access terrorist information.

8.2.4 Unregulated domain

Internet postings are not regulated as sources of news, and thus terrorists can post inaccurate information with almost no oversight or regulation. The Internet removes the ability to effectively pre-screen content by allowing for instantaneous broadcast of terrorist messages. Readers might con- sider terrorist Internet postings to be factually correct, and the stories may go unchecked.

8.2.5 Anonymity

Terrorists can use anonymity on the Internet to their advantage. The anonymity of the Internet has been found to foster higher levels of violence in people. Terrorists can encourage feelings of violence, drawing people to their cause. Anonymity also allows the terrorists to evade detection by law enforcement. Previously, if terrorists communicated by electronics, they were limited to using telephones or radios, which were at risk of being monitored by electronic surveillance tools such as wiretaps. Now, individuals can make countless usernames that mask their true identities on numerous platforms.

8.2.6 Expert knowledge

Terrorists can gain knowledge about social media in order to distort the prevalence and ranking of their messages on search results. Social media, in particular Twitter, allows terrorists to amplify their messages by posting links to their propaganda and “hashtags” at an unnaturally fast pace, causing the postings to place higher in search results and in content aggregated by third parties. ISIS and al Qaeda reportedly both use “bots,” which are computer- controlled Twitter accounts that automatically send out content in a similar manner.

8.2.7 Multidirectional communications

The Internet allows for multidirectional communication between the terrorists and the potential recruits. Individual communication allows terrorists to craft propaganda specifically tailored for certain types of individuals. Further- more, interactive participation can foster a sense of cohesion and generate a sort of virtual community between the terrorists and potential recruits, thereby creating a sense of unity.

8.2.8 Targeting the vulnerable

Terrorist groups can use social media to search for and target individuals who might be particularly vulnerable to their ideology. For example, ISIS utilizes social media platforms that are popular with teenagers to attract and recruit young people, who are more susceptible to its propaganda. Terrorists can craft their propaganda to appeal to certain vulnerable populations by portraying their organization as the solution to individuals' problems. Furthermore, terrorists can weed out less susceptible populations by blocking apparent nonbelievers from their communications.

8.9 Encryption privacy

Encryption allows terrorists to maintain private networks of communication without law enforcement oversight. Encrypted communications cannot be easily accessed by law enforcement, and as such, recruitment efforts and other terrorist activities can take place in relative secrecy. As more websites and smartphone applications turn to encryption, its ability to hide such communications and actions will likely be a growing concern. In September 2014, Apple and Google announced plans to strengthen encryption of data stored on smart- phones using their operating systems. Two encrypted messaging applications, WhatsApp and Kik, have been especially popular with ISIS. These applications make it much more difficult for law enforcement to intercept communications than would otherwise be possible on Twitter or Facebook.

8.10 Cyber terrorist case study

An early of example of the terrorist's creative use of the Internet is the case of Younes Tsouli. When police officers raided a flat in West London during October 2005, they arrested a young man, Younes Tsouli. The significance of this arrest was not immediately clear, but investigations soon revealed that the Moroccan born Tsouli was the world's most wanted 'cyber-terrorist'. In his activities Tsouli adopted the username 'Irhabi 007', (Irhabi meaning 'terrorist' in Arabic), and his activities grew from posting advice on the internet on how to hack into mainframe computer systems to assisting those in planning terrorist attacks. Tsouli trawled the internet searching for home movies made by US soldiers that would reveal the inside of US military bases. Over time these small pieces of information were collated and passed to those planning attacks. This virtual hostile reconnaissance provided insider data illustrating how it was no longer necessary for terrorists to conduct physical reconnaissance if relevant information can be pieced together from the internet.

Police investigations subsequently revealed that Tsouli had €2.5million worth of fraudulent transactions passing through his accounts which he used to support and finance terrorist activity. Pleading guilty to charges of incitement to commit acts of terrorism Tsouli received a 16-year custodial sentence to be served at Belmarsh High Security Prison in London where, perhaps unsurprisingly, he has been denied access to the internet. The then National Coordinator of Terrorist Investigations, Deputy Assistant Commissioner Peter Clarke, said that Tsouli 'provided a link to core al Qaida, to the heart of al Qaida and the wider network that he was linking into through the internet', going on to say 'what it did show us was the extent to which they could conduct operational planning on the internet. It was the first virtual conspiracy to murder that we had seen.'

8.3. Online terrorist activity

As an example of extent of online terrorist activity, during 2022, Tech Against Terrorism published a report on The Threat of Terrorist and Violent Extremist Operated Websites which found that terrorist and violent extremist actors were running at least 198 websites on the surface web. Further in-depth analysis of 33 of the most prominent websites – run by actors such as IS Al Qaeda, Atomwaffen Division, and the Taliban – confirmed that these sites had 1.54 million monthly visitors, with the majority of visits coming from Algeria, Pakistan, United States, and the UK. The scale of the threat from websites operated by terrorists and extremists reported by Tech Against Terrorism is shocking and demonstrates the scale of the security challenge for all in authority engaged in counter terrorism across the world. Adam Hadley, Founder and Director of Tech Against Terrorism stated: "The fact that terrorists and violent extremists are able to operate hundreds of websites attracting millions of views with impunity is a failure on behalf of the global online counter terrorism sector. Terrorist operated websites is the key strategic threat with regards to terrorist use of the internet. It is clear that policymakers need to devote more political capital towards identifying practical and policy-oriented solutions to this challenge."

Since January 2021, Tech Against Terrorism has conducted open-source intelligence (OSINT) research into the threat of terrorism and violent extremist operated websites. Their methodology comprised of keyword searches across several mainstream and niche social media and messaging apps, as well as search engines and bespoke apps, mostly conducting searches in English and Arabic, though also in Dari, Pashto and Russian. Tech Against Terrorism also identified terrorist and violent extremist operated websites through daily monitoring of online terrorist spaces that were likely to promote such sites, such as social media platforms and messaging platforms. The daily monitoring encompassed both mainstream and niche social media, video sharing platforms, and messaging platforms. The 198 websites identified by Tech Against Terrorism included sites which promoted violent extremist ideologies such as Neo-Nazism, violent insurrectionary accelerationism, Salafi-Jihadism, and Incel ideology. Analysis of these sites found that: 101 websites were operated by far-right violent extremist or terrorist groups; 79 websites were operated by violent Sunni Islamist extremist or terrorist groups; and 18 websites were operated by violent Shia Islamist extremist or terrorist groups. A sample analysis of 33 of these websites – run by groups such as ISIS, Al Qaeda, Atomwaffen Division, Combat 18, and the Taliban – found that they had a total of 1.54 million monthly visits with 91% displaying audio and visual propaganda. Moreover, the sample analysis revealed that 73% contained an archive of historic terrorist content and 57% included a contact address form.

The Tech Against Terrorism report indicates that terrorist operated websites constitute a key propaganda organ for terrorist and violent extremist groups which allows groups to disseminate recruitment material without disruption. The rise in prominence of terrorist operated websites is likely the result of improved removal campaigns across other parts of the tech industry, including on larger social media platforms.

The second Transparency Report of the Terrorist Content Analytics Platform (TCAP) published in 2023 by Tech Against Terrorism, outlined the progress of the world's largest alert platform for verified terrorist content, collected in real time. The Platform notifies technology

companies of the presence of such content on their platforms. The Transparency Report detailed the extent and scale of terrorist content discovered by Tech Against Terrorism's Terrorist Content Analytics Platform and how the data gathered is utilised to disrupt and understand terrorist and violent exploitation of the internet. The report found that between 1 December 2021 and 30 November 2022:

- Open-source intelligence experts submitted 18,995 URLs containing terrorist content, and the TCAP sent 10,174 alerts to 57 tech companies, 82% of which are now offline. In total, 150 tech companies are registered and able to receive alerts as soon as we detect terrorist content on their platforms. We have increased the number of platforms we can alert from 114 in Year 1.
- Most of the content we have alerted has been related to Islamist terrorist entities (92% of alerts in Year 2). This is compared to 98% of alerts containing Islamist terrorist content in Year 1 of the TCAP.
- Because of alerts from the TCAP, an average of 84% of Islamist terrorist content was removed, whilst an average 61% of far-right terrorist content was removed. Compared to our previous Transparency Report, the takedown rate for Islamist terrorist content has decreased from 94% but has increased from 50% for far-right terrorist content.
- 18,048 URLs containing Islamist terrorist content were submitted to the TCAP, compared to 947 URLs containing far-right terrorist content. 9,436 alerts containing Islamist terrorist content were sent, whilst 738 alerts containing far-right terrorist content have been sent to tech companies. The discrepancy in numbers is due to the different propaganda dissemination techniques employed by far-right and Islamist terrorist groups. However, we have begun to close the gap between Islamist and far-right terrorist content submissions and alerts and this difference is smaller than in Year 1.

The analyses conducted by Tech Against Terrorism concludes that there is currently no unified global approach against terrorist operated websites, and their recommendation is that governments should step in and create a strategy to disrupt terrorist operated websites based on collaborative engagement with web infrastructure providers and on human rights safeguards. What is clear from the findings in the Tech Against Terrorism report is that responses to terrorist and violent extremist operated websites can be severe in that they often constitute the removal or blocking of entire websites. There are therefore several ethical challenges posed by tackling websites to ensure firm but fair responses are put in place and tighter regulation may be preferrable to more anti-terror legislation which, if used disproportionately, can have potential long-term damaging consequences on fundamental human rights.

8.4. Countermeasures

While citizens in western nations have enjoyed protection from terrorism and violent extremism under the aegis of various departments and agencies across the landscape of government, critical to the future success of contemporary counter terrorism and violent extremism is the cooperation between law enforcement and social media platforms. This collaboration between very different emanations of state power and private enterprise is now considered essential to keep citizens safe. And while their cultures and operating practices are very different and not without them imperfections, they must now seek to identify ways in

which to meld and amplify their approach to tackle terrorist online content for mutual benefit. There have been recent developments providing encouragement and evidence that law enforcement and social media platforms are now beginning to work together but these efforts are isolated cases, and cooperation remains fractured and in its infancy. A truly cooperative and interoperable approach, where law enforcement and social media bring their expertise to bear in concert with one another to tackle online terrorist content as part of their operating cultures and practices has yet to be fully achieved.

There are impediments to close cooperation between police authorities and the private sector. Tech companies and law enforcement have very different cultures and operating practices. There have been high-profile instances of non-cooperation. Concerns have also been raised about the informality of existing collaborations. To guard against the possibility of censorship, mission creep and a lack of accountability and oversight, there have been calls for all requests submitted to tech companies from state authorities to be subjected to rigorous scrutiny, accompanied by detailed reporting requirements to ensure transparency. The policy challenge is to address the impediments to cooperation between law enforcement and the tech sector in order to achieve the collaboration that is widely accepted as necessary to tackle online terrorist content, while ensuring that such cooperation meets the demands of due process and accountability.

In 2023, the Global Network on Extremism and technology (GNET),published a report 'Tackling Online Terrorist Content Together: Cooperation between Counterterrorism Law Enforcement and Technology Companies'. The findings of this research provide unique insights into the context and operating environment of members of law enforcement and tech companies engaged in the highly specialised counterterrorism field of online terrorist content removal. From a law enforcement perspective, it is clear that the rapid pace of social and technical innovation has resulted in an increasingly interconnected and interdependent world, in which many new hazards have a transnational dimension. This has necessitated a significant shift in approach to counterterrorism. Tech companies are the driving force behind this dynamic change in society, sometimes with unintended consequences for safety and security. But while the tendency has been to highlight the differences between tech companies and law enforcement agencies, this research report provides evidence of an understanding of the common vision shared by both sides to keep people safe online.

The processes and professional partnerships that have been developed are, in part, the product of tech companies' investment in establishing dedicated teams to remove terrorist content. This investment has included the recruitment and buy-in of much needed knowledge and expertise, including hiring personnel with law enforcement backgrounds. The establishment of these teams, coupled with the development and delivery of bespoke training, has led to an improved understanding of each other's roles. The findings also reveal positive working practices of tech companies providing direct and fast access to data at times of critical threat, as well as making personnel available to work within and alongside police counterterrorism operations in response to major terrorist events. These developments provide evidence of a real commitment to tackle terrorism and reveal existing models of cooperation upon which future collaboration can be founded. It is noteworthy that the research findings did not contain any demands from law enforcement for a more robust

regulatory or legislative framework for the removal of online terrorist content. On the contrary, what emerged was a more nuanced, practical and pragmatic approach by police officers who have invested time and resources into developing positive relations with individual tech companies.

The law enforcement interviewees expressed concerns about the utility of new legislation, particularly at a national level, with the most common concern being that such legislation could impede voluntary cooperation and mark a return to the "transactional" relationship of the past. Perhaps it is unsurprising that police officers wish to protect the professional partnerships that they have built over time with their counterparts in tech companies. Nonetheless, the only justification that the law enforcement interviewees offered for new legislation was that it might increase public confidence in how this issue is being tackled. In contrast, it was the tech sector participants who had misgivings about the informality of the existing referral process, citing concerns about mission creep and transparency. From their perspective, response times can be slowed as a result of insufficient information being provided and because some requests are not terrorism-related and so have to be redirected within the organisation. There was also a sense that the tech sector's improvements in transparency reporting should be mirrored by state authorities requesting takedowns or shutdowns. This has particular force where an informal referral process is utilised in preference to a formal statutory procedure for content takedown, such as in the UK.

While the cultures and operating practices of law enforcement and tech companies are very different, strides have been made towards an increasingly open and cooperative relationship in recent years. Nonetheless, such cooperation remains in its infancy and tensions remain. From a policy perspective, the challenge is to resolve these tensions, given the value of cooperation to tackling online terrorist content, while simultaneously addressing the concerns about due process and accountability that stem from the informality of current arrangements. The following recommendations are highlighted and offered in an attempt to meet this policy challenge with measures that can be implemented with immediate effect:

- The development of an *experience exchange programme* affording the opportunity for identified personnel within counterterrorism policing and tech companies to be embedded within each other's counterterrorism operational functions. The purpose of the exchange is to fully embed, immerse and expose personnel with the required security vetting and clearances to the operating cultures and practices of each other's organisations, serving to share knowledge, expertise and opportunities to identify better alignment of priorities and more productive ways of working together.

- The implementation of a *takedown-shutdown counterterrorism* policing protocol, providing clarity following review of current practices for content takedown and account shutdown referrals. The protocol will reset and reform current practices with the primary purpose of achieving greater transparency between counterterrorism policing and tech companies, including clearly defined referral parameters and the introduction of independent oversight for takedown and shutdown requests. The protocol serves to ensure counterterrorism powers and partnerships are used only for

counterterrorism purposes, while protecting policing from determining legality without independent oversight of takedown and shutdown referrals.

- The development of a *joint upstreaming programme*, which seeks to deliver a fundamental shift in emphasis from the removal of terrorist content online to preventing its initial publication. The upstreaming is founded upon a proactive preventative ethos. This must include increased access and visibility of each other's threat assessments, intelligence insights and future risk forecasting, including meaningful briefings of operational value that offer far greater granularity of detail.

- The development of *joint strategic research requirements*, identifying and prioritising areas of mutual concern for further development and investigation through research. The research requirements can then be made available to the research and innovation community, offering a unique opportunity to design, develop and deliver research meeting the identified needs of tech companies and counterterrorism agencies better to tackle online terrorist content. These research requirements may include the provision of new AI tools, techniques and technologies, and in-depth analysis providing an evidence base to inform policy, practice and procedure directly.

The research report concludes that as the sustained threat from terrorism in all its forms persists, a more progressive, cooperative and collaborative partnership between law enforcement agencies and tech companies must be encouraged. Adopting these recommendations will support transforming this partnership.

8.5. Terrorist Content Online Regulation

Social media platforms and host service providers (HSPs) are now subject to increased regulation in the global effort to tackle harmful terrorist online. The EU's Terrorist Content Online (TCO) regulation addressing the dissemination of terrorist content entered into application on 7 June 2022. According to the EU, This Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society, by addressing the misuse of hosting services for terrorist purposes and contributing to public security across the Union. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers and users' trust in the online environment, as well as by strengthening safeguards to the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media.

Regulatory measures to address the dissemination of terrorist content online should be complemented by Member State strategies to address terrorism, including the strengthening of media literacy and critical thinking, the development of alternative and counter narratives, and other initiatives to reduce the impact of and vulnerability to terrorist content online, as well as investment in social work, deradicalisation initiatives and engagement with affected communities, in order to achieve the sustained prevention of radicalisation in society. Addressing terrorist content online, which is part of a broader problem of illegal content online, requires a combination of legislative, non-legislative and voluntary measures based

on collaboration between authorities and hosting service providers, in a manner that fully respects fundamental rights.

Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, the services of hosting service providers are in certain cases abused by third parties for the purpose of carrying out illegal activities online. Of particular concern is the misuse of those services by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity. While not the only factor, the presence of terrorist content online has proven to be a catalyst for the radicalisation of individuals which can lead to terrorist acts, and therefore has serious negative consequences for users, citizens and society at large as well as for the online service providers hosting such content, since it undermines the trust of their users and damages their business models. In light of their central role and the technological means and capabilities associated with the services they provide, hosting service providers have particular societal responsibilities to protect their services from misuse by terrorists and to help address terrorist content disseminated through their services online, while taking into account the fundamental importance of the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society.

Efforts at EU level to counter terrorist content online commenced in 2015 through a framework of voluntary cooperation between Member States and hosting service providers. Those efforts need to be complemented by a clear legislative framework in order to further reduce the accessibility of terrorist content online and adequately address a rapidly evolving problem. The legislative framework seeks to build on voluntary efforts, which were reinforced by Commission Recommendation (EU) 2018/334, and responds to calls made by the European Parliament to strengthen measures to address illegal and harmful content online in line with the horizontal framework established by Directive 2000/31/EC of the European Parliament and of the Council, as well as by the European Council to improve the detection and removal of content online that incites terrorist activity.

The EU TCO Regulation provides a legal framework to ensure that hosting service providers, that make content available to the public, address the misuse of their services for the dissemination of terrorist content online. Online platforms will be obliged to remove terrorist content upon receiving a removal order from Member States' authorities within one hour and to take measures when their platforms are exposed to terrorist content. The Regulation applies to all hosting service providers offering services within the EU, insofar as they disseminate information to the public. These are types of online platforms that include: providers of social media, video, image and audio-sharing services.

The definition of terrorist content for the operational purposes of the EU TCO is aligned with the definition of terrorist offences set out in the Directive on combating terrorism and applies to material that:

- Solicits someone to commit or to contribute to terrorist offences, or to participate in activities of a terrorist group,
- Incites or advocates terrorist offences, such as by glorification of terrorist acts.
- Provides instruction on how to conduct attacks.
- Such material includes text, images, sound recordings and videos, as well as live transmissions of terrorist offences that cause a danger of further such offences being committed.

Terrorist content is most harmful in the first hours after its appearance. The new Regulation obliges online platforms to stop the dissemination of such content as early as possible. The competent authority of each Member State can issue a removal order to any online platform established in the EU, requiring them to remove or to disable access to terrorist content in all Member States. Removal orders must contain justifications as to why the material is considered to be terrorist content, including detailed information on how to challenge the removal order. Online platforms must take proactive measures when they are exposed to terrorist content. The measures they take will depend on the level of exposure and their size and capabilities as well as resources. The measures must be applied with effective safeguards to protect fundamental rights, in particular freedom of speech. There is no obligation to use automated tools to identify or remove content. Where platforms choose to use such tools, they need to ensure human oversight and publicly report on their functioning. Moreover, the following safeguards have been built into the EU TCO Regulation to protect fundamental rights as follows:

- Strong safeguards are put in place to ensure that freedom of speech is protected: Both Member States and hosting services providers will have to issue annual transparency reports on the measures taken to remove terrorist content, and on any erroneous removals of legitimate speech online.
- Where content is removed, the user will be informed and provided with information to contest the removal.
- Complaint mechanisms to ensure that content that has been removed erroneously can be reinstated as soon as possible
- Content providers and online platforms can request a review of the removal order before the relevant authorities or seek judicial redress in courts in the respective Member States.
- Content disseminated for educational, journalistic, artistic or research purposes is exempted. The exemption will also apply to content disseminated to raise awareness against terrorist activity.

Sanctions of non-compliance will depend on the nature and size of the platforms to ensure penalties for small, medium and micro enterprises are proportionate. Financial penalties can be up to 4% of the platform's turnover.

The EU TCO Regulations were brought forward because of the series of critical factors stated above, and which also included the high volume of hostile content that overwhelms all government agencies capacity and capability to prevent it and keep the public safe online. Despite voluntary measures and non-binding recommendations which bore fruit to reduce the availability of terrorist content online, limitations including the small number of HSPs adopting voluntary mechanisms, as well as the fragmentation of procedural rules across EU

Member States, limited the effectiveness and the efficiency of cooperation among Member States and HSPs making it necessary to establish regulatory measures. Therefore, the effective application of the TCO Regulation is key to address the dissemination of terrorist content online across Europe, and the European Commission has proactively supported national competent authorities in this process to enforce the regulations, but a recent report published by Tech Against Terrorism Europe (TATE) suggests more needs to be done.

Recognising the challenge for HSPs, the TATE initiative, supported by the EU's Internal Security Fund (ISF), has recently published a study which aimed to speak to small and micro HSPs to understand what they regard as the main obstacles they face in implementing and complying with the requirements of the EU's TCO. In total, 49 HSPs were invited to participate in the study, and these invitations yielded 15 interviews with participants based in six different countries. The findings of the study will be of interest to police counter terrorism units engaged in internet referrals in the UK, across the EU, and beyond EU borders, as well as those police personnel and partners engaged in the prevention of terrorism and violent extremism online.

The study reveals that the interviewees reported first hearing about the TCO Regulation from various sources, including via already- existing connections with organisations such as the Global Internet Forum to Counter Terrorism (GIFCT) or Tech Against Terrorism (TaT), legal advice, media coverage, networking events and even conversations with friends. The general feeling was that there is a lack of awareness of the TCO Regulation within the tech sector, particularly in comparison to other relevant legislation such as the Digital Services Act (DSA). Several interviewees felt that there could have been a more effective awareness-raising campaign prior to the TCO Regulation's implementation.

Interviewees identified a number of challenges that small and micro platforms face in complying with the TCO Regulation, as many may lack the necessary expertise, both in terms of the legal knowledge required to navigate multiple regulatory regimes and their terminology, and the subject-matter understanding needed to identify terrorist content correctly. One specific challenge that interviewees faced was to define what content is 'terrorist'. While some companies chose to sidestep this task – simply using the term 'terrorism' without defining it – most had either developed a list of designated organisations or adopted a generic, dictionary-style definition. One issue common to both of these approaches was the difficulty choosing between different official designation lists and definitions. Interestingly, none of the interviewees in the study said that they had adopted the TCO Regulation's definition of terrorist content, though they felt it is broadly similar to the definition they have chosen to use. The TCO Regulation's one-hour removal window was a cause of grave concern to small and micro HSPs. Interviewees described it as a source of significant anxiety, even stating that the pressure it places on a small team has had a significant impact on their wellbeing. Some interviewees were also concerned about the possibility of receiving bogus removal orders and called for a mechanism by which the validity of any order received could be verified.

For all of these reasons, interviewees felt that some companies might choose not to engage with the TCO Regulation – particularly if they have never been contacted by a competent

authority and believe they are under-the-radar. On the other hand, they identified several reasons for seeking to comply, including the business' reputation and long-term prospects for success and the intrinsic desire to combat terrorism online. Various coping strategies have been adopted by companies that are motivated to comply, but struggle with resource limitations. Some have developed organisational practices that ensure someone is always on duty, in case a removal order should arrive. Other strategies were to simply defer to those referring the content and to outsource content moderation to Trust and Safety vendors (although some concerns were raised here about these vendors' lack of transparency).

The TATE study reveals that there is an ongoing need to raise awareness and understanding of the TCO Regulation and recommends that it would be desirable to ensure that each Member State has a national clearinghouse, that is able to provide advice and support to companies in their native language. The study also suggests that competent authorities should avoid an enforcement-led approach if a company is engaging with the TCO Regulation and striving to remove terrorist content from its platform promptly. Some understanding of the difficulty in always responding to a removal order within one hour should be shown where small HSPs are making a concerted effort to comply with the TCO Regulation's requirements but where platforms are non-responsive or uncooperative, the study is robust in its recommendation that enforcement action is taken – even if this is likely to prove time-consuming and resource intensive.

During February 2023, the European Commission issued its report on the implementation of the Terrorist Content Online (TCO) Regulation. The key findings reveal that as of 31 December 2023, at least 349 removal orders sent to Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net and Catbox by the competent authorities of Spain, Romania, France, Germany, Austria and Czechia. Sixty-two removal orders have been sent by the Spanish competent authority - CITCO (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado), while the Romanian competent authority (ANCOM – Autoritatea Națională pentru Administrare și Reglementare în Comunicații) sent two removal orders and the French competent authority (OCLCTIC – L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) sent twenty-six removal orders. Since the terrorist attack perpetrated by Hamas against Israel, the German competent authority (BKA – Bundeskriminalamt) has sent 249 removal orders.

The Spanish competent authority has transmitted sixty-two removal orders: eighteen before the launch of PERCI and fourty-four through PERCI. It provided a detailed description of the transmission of and follow-up to the first removal orders issued, which is very relevant to better understand the implications and effects of the Regulation. The two first removal orders were issued by the Spanish competent authority on 24 April 2023. They were related to two pieces of terrorist content, one concerning right-wing terrorism and the other one concerning jihadism. The content that was subject to the first removal order was a PDF document posted on Telegram with unlimited access, which advocated for terrorist violence and glorified right-wing terrorist attacks. The piece of terrorist content subject to the second removal order was a video featuring images of jihadists from the so-called Islamic State terrorist organisation in combat uploaded on Internet Archive. These two pieces of content were removed from both

platforms in less than one hour, thus in compliance with Article 3(3) of the Regulation. In the assessment provided by the Spanish competent authority it was explained that they had opted for a removal order rather than a referral for two main reasons: compliance with the requirements in the Regulation on removal orders and urgency. The Spanish competent authority then sent further removal orders. The Spanish authority highlighted challenges related to the use of a webform by one hosting service provider (Meta) to receive removal orders instead of providing a direct contact point. This webform also led to problems to communicate with the competent authority of the Member State where the hosting service provider's main establishment is located. The French competent authority issued their first removal order on 13 July 2023 to a sharing platform (Justpaste.it), which removed the terrorist content within one hour. The targeted content was propaganda from Al Qaeda, more specifically from the media body Rikan Ka Mimber of its Indian branch Al Qaeda Indian Sub-continent (AQIS). The full removal of the content was confirmed in Europol's platform PERCI. The German competent authority issued six, sixteen and five removal orders on 16, 18 and 24 October 2023 respectively targeting propaganda from Hamas and Palestinian Islamic Jihad. Access to the content was blocked in the EU in compliance with Article 3(3) of the Regulation. The German competent authority had first sent referrals and subsequently issued removal orders as these referrals were not acted upon. Following Hamas' attack on 7 October 2023, the German competent authority has sent 249 removal orders, mostly to Telegram. The Czech competent authority and the Austrian competent authority issued 2 and 8 removal orders, to X and Telegram respectively.

As regards the use of a webform to receive removal orders by one hosting service provider, Spanish authorities indicated two issues: 1) in the context of Article 3(2) of the Regulation, a webform does not allow Member States' competent authorities to send information on the applicable procedures and deadlines before issuing the first removal order to the hosting service provider; 2) in the context of Article 4(1), a webform does not allow to submit a copy of the removal order simultaneously to the competent authority of the Member State where the hosting service provider has its main establishment and to the hosting service provider's legal representative. For the two first removal orders issued in April 2023, the Spanish competent authority could not send copies to the authority of the Member State where the hosting service provider had its main establishment or its legal representative, as none of the two hosting service providers had, at the time, their main establishment or designated a legal representative in the EU. For the subsequent removal orders, the Spanish competent authority sent copies to the competent authority of the Member State where the hosting service provider had its main establishment or had designated its legal representative.

Transmitting removal orders to hosting service providers based in third countries that have not yet fulfilled their obligation of appointing a legal representation in the EU was reported as a challenge by Member States. In this context, the Commission supported Member States to ensure that hosting service providers comply with their obligation to appoint a legal representative in the EU and to provide a contact point (Article 15(1) of the Regulation), such as an email address, to ensure immediate action. Furthermore, the Commission has reminded hosting service providers of their obligations in different fora, including in the EU Internet Forum. According to the information available to the Commission, no competent authority of the Member State in which the hosting service provider has its main establishment has so far

scrutinised a removal order pursuant to Article 4 of the Regulation to determine whether it seriously or manifestly violated the Regulation or fundamental rights and freedoms as there has been no reasoned request for scrutiny submitted yet. As a consequence, up to now, no authority has found that any removal order infringed this Regulation or fundamental rights in that manner.

No hosting service provider has so far reinstated the content (or access thereto) which had been subject to a removal order pursuant to scrutiny in accordance with Article 4 of the Regulation, because such scrutiny and requests for reinstatement have not yet taken place. Hence, there is no information available on how long it usually takes to reinstate content or access to it, or the "necessary measures" taken by the hosting service providers to reinstate the content or access to the content. Despite the European Commission assessing that the application of the TCO Regulation has had a positive impact in limiting the spread of terrorist content online, all engaged in countering terrorism recognise that more must be done to tackle the persistence of online terror threat vectors. The regulatory framework to address illegal content online has been further strengthened with the entry into force of the Digital Services Act (DSA) on 16 November 2022. The DSA regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with content, services, and goods, thereby better protecting users online and contributing to a safer online environment. The DSA enables the tackling of all forms of illegal content, allowing the European Commission to challenge platforms to provide data to demonstrate that they are living up to their own commitments on content removal.

8.6. Conclusions

Despite the European Commission assessing that the application of the EU TCO Regulation has had a positive impact in limiting the spread of terrorist content online, all engaged in countering terrorism recognise that more must be done to tackle the persistence of online terror threat vectors. Last month judicial and law enforcement authorities across Europe and in the United States dismantled critical online infrastructure in a large-scale operation to disrupt platforms and websites for terrorist communications and propaganda. In a concerted major action, servers were taken down in Germany, the Netherlands, United States and Iceland, with the Spanish authorities arresting nine radicalised individuals. The servers supported multiple media outlets linked to the so-called Islamic State. They were used to disseminate worldwide propaganda and messages capable of inciting terrorism in at least thirty languages. Europol coordinated and supported the joint operations which were part of ongoing efforts and constant vigilance to tackle online terrorist propaganda and communications, including through social media.

Investigations and the continuous monitoring of online activities of terrorist organisations, led by the Spanish Civil Guard in 2022 gave insight to the communications of media linked to the Islamic State. The traceability was complex, as they operated new and sophisticated technological infrastructures. The websites and communication channels, such as radio stations, a news agency and social media content, had a global reach. They communicated directives and slogans of Islamic State in over thirty languages, including Spanish, Arabic, English, French, German, Danish, Turkish, Russian, Indonesian and Pashto. Several terabytes

of information were uncovered and marked an important achievement for Europol in tackling online terrorism. Europol's European Counter Terrorism Centre made its full range of services and expertise available to the investigation. Since the launch of investigative activities, Europol has provided intelligence packages mapping the web infrastructure of the targeted online assets through forensic analysis of the servers. Europol's expertise on the terrorist propaganda landscape was instrumental in informing judicial proceedings.

Following the success of the operation, law enforcement authorities from Albania, Bosnia and Herzegovina, Denmark, Germany, Iceland, Moldova, Romania, the Slovak Republic, Ukraine and the United Kingdom, joined forces with the European Union Internet Referral Unit (EU IRU), located within Europol's European Counter Terrorism Centre to further disrupt the online terrorist content. Under Operation HOPPER II, authorities targeted key assets in the online dissemination of terrorist propaganda, including those of the Islamic State, al-Qaeda and its affiliates, and Hayat Tahrir al-Sham. The EU IRU referred a total of 13 websites spreading terrorist propaganda to hosting service providers for removal, following the seizure of four servers in Romania, Ukraine and Iceland over the course of the investigation and the removal of associated websites. The EU IRU detects and investigates malicious content on the internet and in social media and recognises that terrorists' use of the internet and social media has increased enormously over the course of recent years. The EU IRU reveal that Jihadist groups, have demonstrated a sophisticated understanding of how social networks operate and have launched highly sophisticated, concerted social media campaigns to recruit followers and to promote or glorify acts of terrorism and violent extremism. The EU IRU comprises of a team of experts with multiple and diverse knowledge and skills, ranging from experts in religiously inspired terrorism, translators, information and communications technology developers and law enforcement experts in counter terrorism.

Since it was set up, the EU IRU has assessed in total 42 066 pieces of content, which triggered 40 714 decisions for referral across over 80 platforms in more than 10 languages. On average, the content flagged for referrals has been removed in 86% of the cases. Responding to the threat of terrorist-operated websites is a crucial part of the EU IRU's ongoing work, which serve as key platforms for the dissemination of violent ideologies. These websites enable terrorist organisations and violent extremists to bypass the enhanced moderation and content removal efforts of mainstream online service providers, allowing them to maintain a persistent online presence. Identifying, flagging, investigating and disrupting these websites has become a key function of the EU IRU through the technical solution Europol developed in-house – the EU Platform on illicit content online (PERCI). PERCI provides a single system to facilitate referrals and removal orders and was developed as a technical solution to support the facilitation of the implementation of the Terrorist Content Online Regulation (TCO Regulation - (EU) 2021/784) by EU Member States.

The TCO Regulation, which came into effect from June 2022, provides a legal framework to ensure that hosting service providers are obliged to remove terrorist content within one hour of receiving a removal order from Member State authorities. The Regulation applies to all hosting service providers offering services within the EU, including providers of social media, video, image and audio-sharing services. The new legal and regulatory provisions to tackle online terrorist content provides the effective tools for Europol to carry out their mission

which is reinforced through the regulation which now amplifies the mandate of Europol as the European criminal police agency, expanding its capability to tackle online terrorist content.

9. Sources of information

The following sources of information were used to inform and create the content for the topic of *Online Radicalisation*:-

1. European Union, ***Counter Terrorism Agenda 2020*** (9/12/2020) Available online at: https://home-affairs.ec.europa.eu/document/download/9b54c533-139a-4662-99cf-b5f72220bb18_en?filename=09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf
2. Tech Against Terrorism, ***Transparency Report of the Terrorist Content Analytics Platform*** (22 August 2023) Available online at: https://techagainstterrorism.org/news/terrorist-content-analytics-platform-second-annual-transparency-report
3. Staniforth, A ***Stronger together: Tackling online terrorist*** **content** (5/4/2023) Policing Insight, Available online at: https://policinginsight.com/feature/analysis/stronger-together-tackling-online-terrorist-content/
4. Tech Against Terrorism, ***Patterns of Online Terrorist Exploitation*** (28 April 2023) Available online at: https://techagainstterrorism.org/news/patterns-of-online-terrorist-exploitation
5. Tech Against Terrorism Europe, ***The challenges that small and micro host service providers face in implementing the TCO Regulation*** (September 2024) Available online at: https://tate.techagainstterrorism.org/news/report-the-challenges-that-small-and-micro-hsps-face-in-implementing-the-tco-regulation
6. Tech Against Terrorism, ***Mapping Far-Right Terrorist Propaganda Online*** (20 May 2024) Available online at: https://techagainstterrorism.org/news/report-mapping-far-right-terrorist-propaganda-online
7. Staniforth, A ***One-year on: Examining new powers to tackle terrorist content*** (7/6/2023) Policing Insight, Available online at: https://policinginsight.com/feature/innovation/one-year-on-examining-new-powers-to-tackle-terrorist-content-online/
8. European Commission, ***Report on the operation of the Terrorist Content Online Regulation*** (February 2023) Available online at: https://home-affairs.ec.europa.eu/document/download/506de61d-c53f-489f-a9e3-e16e78793e81_en?filename=202104_terrorist-content-online_en.pdf
9. European Commission, ***An Introduction to the Terrorist Content Online Regulation*** (April 2021) Available online at: https://home-affairs.ec.europa.eu/document/download/506de61d-c53f-489f-a9e3-e16e78793e81_en?filename=202104_terrorist-content-online_en.pdf

10. Staniforth, A ***Combatting terrorist content online: Proactive AI detection*** (4/1/2024) Policing Insight, Available online at: https://policinginsight.com/feature/innovation/combatting-terrorist-content-online-proactive-ai-detection/
11. Europol, ***European Union Terrorism Situation and Trends Report 2024*** (16 December 2024) Available online at: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat
12. Staniforth, A ***Tackling terrorist content online: A new paradigm for security research*** (19/10/2023) Policing Insight, Available online at: https://policinginsight.com/feature/innovation/tackling-terrorist-content-online-a-new-paradigm-for-security-research/
13. Macdonald, A & Staniforth, A ***Tackling Online Terrorist Content Together – Cooperation Between Counter Terrorism Law Enforcement and Technology Companies*** (24 January 2023) Global Network on Extremism & Technology (GNET) Available online at: https://gnet-research.org/2023/01/24/tackling-online-terrorist-content-together-cooperation-between-counterterrorism-law-enforcement-and-technology-companies/
14. Staniforth, A. ***Mission critical: The crucial role of the UK's counter-terror policing*** (17/7/2024) Policing Insight, Available online at: https://policinginsight.com/feature/mission-critical-the-crucial-role-of-the-uks-counter-terror-policing/
15. Bindner, L ***Violent extremists are agile, they are alert, and they are constantly ready to adapt*** (16/10/2024) Policing Insight, Available online at: https://policinginsight.com/feature/interview/laurence-bindner-violent-extremists-are-agile-they-are-on-alert-and-they-are-constantly-ready-to-adapt/
16. Staniforth, A ***Posting propaganda: Compliance checks for online content*** (24/2/2024) Policing Insight, Available online at: https://policinginsight.com/feature/innovation/posting-propaganda-compliance-checks-for-online-content/
17. Staniforth, A ***TCO regulation report: Tackling online terror content*** (28/2/2024) Policing Insight, Available online at: https://policinginsight.com/feature/analysis/tco-regulation-report-tackling-online-terror-content/
18. Staniforth, A ***Tacking terror online: Europol takes executive action*** (11/7/2024) Policing Insight, Available online at: https://policinginsight.com/feature/analysis/tackling-terror-online-europol-takes-executive-action/
19. Hamid, N, & Ariza, C ***Offline versus online radicalisation – Which is the bigger threat?*** (21 February 2022) Global Network on Extremism & Technology (GNET) Available online at: https://gnet-research.org/2022/02/21/offline-versus-online-radicalisation-which-is-the-bigger-threat/
20. Mathieson, N ***User journeys in Online Extremist Groups*** (24 July 2024) Global Network on Extremism & Technology (GNET) Available online at: https://gnet-research.org/2024/07/24/user-journeys-in-online-extremist-groups/
21. Staniforth, A ***Regulation risk: The challenges facing smaller service providers in tackling terror*** **online** (25/10/2024) Policing Insight, Available online

at: https://policinginsight.com/feature/innovation/regulation-risk-the-challenges-facing-smaller-service-providers-in-tackling-terror-online/

22. Ragandang, P ***Young people challenging violent extremism online: Insights from Asia*** (27 August 2024) Global Network on Extremism & Technology (GNET) Available online at: https://gnet-research.org/2024/08/27/young-people-challenging-violent-extremism-online-insights-from-asia/

Този обучителен материал е създаден в рамките на проект „Укрепване на капацитет, обмен на опит и изследователска дейност в сферата на сигурността“, с номер BG65ISPR001-3.004-0002, по договор № 812108-68-02.10.2024, финансиран по Програмата на Република България по фонд „Вътрешна сигурност“ за периода 2021 – 2027 г. Цялата отговорност за съдържанието на материала е на неговия автор и фондация „Европейски институт“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на ЕС и Отговорния управляващ орган.