FRISCO

Fighting Terrorist Content Online

FRISCO INSIGHTS

The EU Regulation on Terrorist Content Online: are European platforms ready?

In 2023, the FRISCO Team conducted a study (available in full-length here) to assess the readiness of small European online platforms (i.e. 'Hosting Service Providers') regarding the provisions of the EU Regulation on Terrorist Content Online. We gathered their insights and identified the most common challenges they face. In this article series, we offer a comprehensive breakdown of our findings. Having already examined the reasons why terrorists use the Internet, today we will focus on their online behaviour and the types of platforms they exploit (2/3).

In 2021, Pharos[1] has dealt with more than 263,000 report forms of which 7,894 were terrorism-related[2]. Nevertheless, available figures usually face several structural problems which makes it difficult to accurately assess the extent of terrorist content online. For example, we can assume that reported content only represents a tiny fraction of all terrorist content published online. Most of these figures also exclude private channels of communication, password-protected websites, deep and dark webs, and honeypots. In a first article, we have showed that the exploitation of the Internet by terrorists serves a variety of purposes, such as disseminating propaganda, financing activities, or providing training. A series of questions then logically arise: *How do they proceed? How do they behave online? Which types of platforms do they use?* Beyond figures and their shortcomings, looking at trends, relating for instance at the types of platforms exploited, can help us answer these questions and refine our understanding of the phenomenon.

Virtual dead drop platforms

To begin with, we are seeing a lasting reliance on 'dead drop' platforms. A physical 'dead drop' is a technique used in espionage to "*secretly pass information items using a clandestine local for interim storage*[3]". In recent years, terrorists, and especially jihadist groups, have transformed the later physical dead drops into virtual ones, using anonymous sharing portals and cloud services to do so[4]. Least sophisticated ways of virtual 'dead dropping' are known since the early 2000s, for instance 'foldering'. Foldering is the process of communication via unsent messages, stored in

[1] Pharos is the French Law Enforcement Agency in charge of illegal content monitoring and reporting.

[2] Assemblée Nationale (2022) - Compte rendu n°47 de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 9 février 2022. Available here.

[3] Weimann, G. and Vellante, A. (2021), "The Dead Drops of Online Terrorism". *Perspectives on Terrorism*, August 2021, Vol. 15, No. 4, pp. 39-40. Available here.

[4] Weimann, G. and Vellante, A. (2021), *op.cit.*, p.40.

'draft' folders of online email accounts (such as Google Mail for instance), thus accessible anywhere by anyone in possession of the relevant password[5]. Regarding anonymous sharing portals, much ink has been spilled about Telegra.ph (developed by the instant messaging app Telegram) and JustPaste.It. Alongside other platforms, such as Sendvid.com and Dump.to, they became "*some of the most used sites by ISIS and other extremist groups*[6]". Cloud-sharing platforms are not spared either, with a lot of them being invested by terrorists, for instance: files.fm, Pixeldrain, Mediafire, OneDrive, CloudShare, Nextcloud, Cloudflare, Mixdrop, 4shared, Cloudmail, Top4top, pCloud, UsersDrive, Dropapk[7], etc.

Decentralised web and platforms

The decentralised web, also known as the 'Dweb', works in the same way as the web we use daily, except it does not rely on centralised operators like Google and Facebook. In fact, the Dweb is "*built on network infrastructure that is more resilient against censorship and surveillance and poses additional challenges to law enforcement agencies, restricting their ability to remove content*[8]". The growing exploitation of the Dweb and related centralised platforms by terrorists and extremists[9] can be traced back to 2018 and 2019, following the major purges of Telegram accounts. Consequently, ISIS and terrorist groups were pushed to search for alternatives, namely Rocket.Chat, ZeroNet and Riot. These platforms offer various advantages for terrorists and "*have proved attractive for IS media operatives, as the developers of those platforms have no way of acting against content that is stored on user-operated serves or dispersed across the user community*", which is a major difference with "*social media giant like Facebook and Twitter and messaging apps like Telegram – all with centralised data stores*[10]". Despite collaboration with authorities from platforms like Rocket.Chat, the removal of terrorist servers is (almost) impossible [11]. Independent from any intermediary, these services represent a major threat. Since 2019, other decentralised platforms like Mastodon and Odysee have attracted the attention of Law Enforcement Agencies (LEAs).

'Unmoderated' platforms

Terrorists also seek platforms with weak content moderation policies and capacities. The reasons explaining poor content moderation are diverse (e.g., available capacities, internal policies, recent market entry, risk perception, etc.) but small players are more likely to be concerned. This was already pointed out by the European Commission in 2018 during the preparatory works of the TCO Regulation:

[5] United Nations Office on Drugs and Crime (2012), The use of Internet for terrorist purposes, New York, p.10. Available here.
[6] Weimann, G. and Vellante, A. (2021), *op.cit.,* p.40.
[7] *Ibid.*, p.46.
[8] King, P. (2019), "Islamic State group's experiments with the decentralised web". Europol, ECTC Advisory Network Conference, p.4. Available here.
[9] Bodo, L. and Trauthig, I. K. (2022), "Emergent Technologies and Extremists: The DWeb as a New Internet Reality?", *Global Network on Extremism*. Available here.
[10] King, P. (2019), *op. cit.,* p.4.
[11] "*Rocket.Chat provides a blueprint of the software that anyone can install on their own servers, without us, as a company, being able to access those private servers*". From: "Rocket.Chat Announces Internal Task Force to Prevent Future Platform Use by Terrorist Groups", *Rocket Chat*, 26 March 2021. Available here.

"*SMEs [⋯] are particularly vulnerable to exploitation for illegal activities, not least since they tend to have limited capacity to deploy state-of-the-art content moderation tools or specialised staff*[12]".

Apart from the size of the platform itself, the type of services offered may also be in cause. For instance, a greater exploitation of platforms offering audio-sharing services, like Clubhouse or Spotify, has been witnessed in recent years "*due to their insufficient content moderation guidelines, personnel, and tools*[13]". The policies enforced by LEAs and tech companies also create a 'push-and-pull effect' that may lead individuals and groups to turn themselves towards formerly used platforms and techniques, *"such as email newsletter services (e.g, Substack)*[14]". Similarly, there has been a resurgence of Terrorist Operated Websites (TOW), which is "*likely a side-effect of broad improvements in social media platforms' content moderation efforts*[15]".

Uses and behavioural characteristics

Opportunism and flexibility might be the watchwords of terrorists. They are constantly adapting to digital trends and regulatory blind spots, switching to new, trendy, or unmonitored platforms. Stable patterns can be identified, but behaviours can change overnight. We have also seen that the implementation of countermeasures pushes them to search for alternative means of communication and content sharing. Terrorists demonstrate remarkable ingenuity when it comes to leverage online resources to their advantage and bypass surveillance. They are versatile and use different types of platforms, relying on different types of technologies. In line with the typology produced by the *Global Internet Forum to Counter Terrorism* (GIFCT)[16], these platforms can be distinguished according to their usages and functions for terrorists:

- Beacons. Beacons are platforms used by terrorists to advertise and redirect the public. As such, beacons act "*both as a centrally located lighthouse and a signpost to where the content can be found*[17]". The aim is to ensure high visibility and attract attention, with a view to effectively conveying a message to as wide an audience as possible. Facebook, Telegram, Discord or BitChute are examples of beacons.

- Content stores. Terrorists need to store their propaganda materials online (e.g., texts, videos, audio files, etc.), while increasing anonymity and accessibility. Platforms offering content storage, archiving, or pasting services are exploited for this purpose. Websites such as the JustPaste.It or Internet Archive play the role of 'virtual libraries'.

[12] European Commission (2018), Commission Staff Working Document - Impact Assessment - Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. Available here.
[13] Radicalisation Awareness Network Policy Support (2021), *Violent Extremism and Terrorism Online in 2021. The year in review*, Luxembourg:Publications Office of the European Union, 2021, p.46. Available here.
[14] *Ibidem*.
[15] Tech Against Terrorism (2021),"Trends in Terrorist and Violent Extremist Use of the Internet I Q1-Q2 2021", July 2021, p.5. Available here.
[16] GIFCT - Tech Against Terrorism (2021), "GIFCT Technical Approaches Working Group Gap Analysis and Recommendations for deploying technical solutions to tackle the terrorist use of the internet", July 2021, pp.14-16. Available here.
[17] GIFCT – Tech Against Terrorism (2021), *op. cit.*, p.15.

- Aggregators. Aggregators are platforms used to centralise and facilitate the diffusion of content. The removal of terrorist content by authorities and companies initiates a cat-and-mouse game, prompting terrorists to seek alternative avenues for (re)posting or (re)sharing their materials. In that regard, aggregators (e.g., 1fichier.com or Vkontatke) prove to be very useful: terrorists compile there "*a wide range of URLs to content hosting platforms*", meaning that if "*one link is taken down, [they] can easily find an alternative*[18]".

- Circumventors. Finally, circumventors are platforms used by terrorists to bypass "*content moderation and deplatforming measures* [19] ". Examples include the aforementioned decentralised platforms (the 'Dweb'), very handy to avoid takedowns, as well as Virtual Private Networks (VPN). The latter enable terrorists "*to access content that has been blocked in specific countries*[20]". For instance, before its dismantling, DoubleVPN "*was heavily advertised on both Russian and English-speaking underground cybercrime forums as a means to mask the location and identities of ransomware operators and phishing fraudsters* [21] " offering multiple layers of protection. Of course, this type of tool is also very useful for terrorism-related activities.

Targeting small platforms

What about small platforms? Unfortunately, recent data has confirmed that micro and small platforms are targeted by terrorists. In 2019, our partners from Tech Against Terrorism showed that "*smaller platforms [were] heavily targeted by ISIS*" thanks to an analysis "*of more than 45,000 URLs since 2014 across more than 330 platforms*[22]". But if smaller are platforms are targeted, some are more than others. For instance, in 2021, an analysis of the URL alerts received on the Terrorist Content Analytics Platform (TCAP) showed "*that more than 80% of all content discovered on smaller platforms (100+ platforms) is shared on the top 20% of these platforms (22 out of 115)*[23]*".*

This asymmetry of exploitation can be explained by the types of services offered, as some are more likely to attract terrorists than others, namely file storage and sharing services, archiving services, and link shortener services. According to the 2022 Transparency Report of the TCAP, of 19,000 URLs analysed, 78% concerned file sharing services, 12% archiving services, 5% link shortener services, the others accounting for very small numbers [24] . Terrorists certainly face a dilemma and must choose between using large-scale platforms with massive audiences but an increased likelihood of suppression and investigation or using smaller platforms with more limited audiences but increased discretion and risk limitation.

[18] *Ibidem.*
[19] *Ibidem.*
[20] *Ibidem.*
[21] "Coordinated action cuts off access to VPN service used by ransomware groups", *Europol*, 30 June 2021. Available here.

[22] Tech against Terrorism (2019), "Analysis: ISIS use of smaller platforms and the Dweb to share terrorist content", April 2019. Available here.
[23] GIFCT - Tech Against Terrorism (2021), *op. cit.,* p.9.
[24] Tech against Terrorism (2022), "Transparency Report. Terrorist Content Analytics Platform. Year One: 1 December 2020 - 30 November 2021", March 2022, p.13. Available here.

To sum-up, all platforms that enable the sharing of user-generated content are at risk to be affected. This includes but is not limited to services such as: file sharing, file storage, social media, archiving, link-shortening, content-pasting, emailing, messaging, video sharing. Furthermore, with weak content moderation, due to available capacities or internal policies, the likelihood to be affected increases. In consequence, smaller platforms, and the ones that just entered the market, might be more exposed than other platforms because they struggle with limited capacities, capabilities, and subject matter knowledge. What is certain is that terrorist content is available online, on the clear web, on European platforms and for European users. It has been estimated that "*at any point, there are 250-500 platforms used by designated terrorist organisations to disseminate content*[25]".

Phenomena to watch

Beyond the trends in the types of platforms exploited, we wanted to conclude this article by outlining some of the main emerging threats in the field of terrorism and violent extremism online. Most of them have been identified in various reports since 2021, for instance by the Radicalisation Awareness Network (RAN)[26].

- A growing relationship between online **gaming** and (violent) extremism and the parallel rise of **gamification dynamics** (i.e., "*the application of gaming and game-design principles within non-gaming environments*[27]").

- The spread of **borderline content** ('awful but lawful'), especially coming from "*cyberfascist*[28]" communities, challenging moderation policies, regulations, and countermeasures – so to say, "*content that is legal, but widely considered to be morally reprehensible or offensive*", such as "*racist comments, […], offensive memes, or harmful disinformation*[29]".

- An increasing tendency to **ideological and aesthetic crossovers** (e.g., incels - extreme right or extreme right – Salafis, etc.) and the rise of hybrid ideologies – for instance, a 2021 study showed how "*Gen-Z Salafis are adopting, altering and amplifying chan communities, alt-right and far-right narratives, and in some cases glorifying Nazism*[30]".

- The identification of "**anti-government extremism**[31]", mainly right-wing oriented, as a rising threat – this type of extremism is fuelled by conspiracy theories and narratives (e.g., Covid-19 pandemic, deep state, Eurabia, etc.), blurs the lines between different violent phenomena and affects vulnerabilities to radicalisation.

[25] GIFCT - Tech Against Terrorism (2021), *op cit.*, pp.6-7.
[26] Radicalisation Awareness Network Policy Support (2021), *op. cit.*
[27] Radicalisation Awareness Network (2021), "The gamification of violent extremism & lessons for P/CVE", Luxembourg: Publications Office of the European Union, 2021, p.5. Available here.
[28] Thorleifsson, C. (2022), "From cyberfascism to terrorism: on 4chan/pol/culture and the transnational production of memetic violence". *Nations and Nationalism*, 28, pp.286-301. Available here.
[29] Deedman, J. (2023). "The Internet Consortium for Online Safety: How Collaborative Tech, Not Legislation, Could Prevent Harmful Content Proliferation". *Global Network on Extremism and Technology*, 2023. Available here.
[30] Ayad, M. (2021). "Islamogram: Salafism and Alt-Right Online Subcultures". *Institute for Strategic Dialogue*, 2021, p.5. Available here.
[31] Bjørgo, T., & Braddock, K. (2022). "Anti-Government Extremism: A New Threat?" *Perspectives on Terrorism*, 16(6), 2–8. Available here.

- The emerging risks posed by **'ill-defined' content** and misuses or innovative technologies (e.g., metaverse or generative AI).
- The mobilisation of **propaganda tactics** such as targeted disinformation or slight modification of already flagged content (i.e., to try tricking perceptual hashing procedures and related databases).

Adeline KUGLER

Pierre SIVIGNON

About FRISCO

FRISCO ("Fighting Terrorist Content Online") is an EU-funded project implemented by a team of 7 partners across Europe. Our main objective is to raise awareness among small tech companies and online platforms and to help them comply with the EU Regulation on Terrorist Content Online (TCO). By supporting the fight against terrorist content in Europe, we are helping to prevent and counter violent extremism online and to create a safer online environment.