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. Today, we will first see why terrorists use the Internet and online platforms (1/3).

Since the late 1990s, the Internet and the growing number of online communication tools have become increasingly pervasive in our lives. Unsurprisingly, the ability to reach massive audiences has attracted individuals and groups wishing to engage in illegal, and sometimes terrorist, activities. With its 450 million inhabitants and 92,5% of households with Internet access[1], the European Union is a clear target for terrorists willing to spread their ideologies and recruit new followers. The Internet is an easy, cheap, and convenient way for terrorists to engage in a wide variety of activities, across borders and (almost) anonymously. But what about the actual purposes of these activities?

Terrorist Propaganda

Propaganda materials are the core of publicly available terrorist content online and their dissemination represents a strategic priority for terrorist groups, regardless of their ideologies. Usually, this online propaganda consists of "*multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities*[2]". It can take many forms: messages, books, magazines, audio files, video files, video games, etc. When disseminating propaganda online, we consider that terrorists pursue three objectives, either separately or jointly: radicalisation, recruitment, and incitement to terrorism. Their methods can be particularly effective, and the messages conveyed very convincing. For instance, Roshonara Choudhry is a singular (and extreme) case of 'solitary online radicalisation': in 2010, the 21-year-old British student with "*no known connection to any Islamist groups*[3]" attempted to kill the Labour Member of Parliament Stephen Timms, an act described as the

[1] Insee (Institut national de la statistique et des études économiques) (2023), "Accès et utilisation de l'Internet dans l'Union Européenne. Données annuelles 2003 à 2022". Available here.

[2] United Nations Office on Drugs and Crime (2012), *The use of Internet for terrorist purposes*, New York, p.3. Available here.

[3] "Profile: Roshonara Choudhry", *The Guardian*, 2 November 2010. Available here.

result of the young woman's self-indoctrination. It was later found that she had watched and downloaded hours of sermons given by cleric Anwar al-Awlaki's, available on Youtube.

Terrorist Financing

The Internet provides numerous tools and opportunities for terrorist groups to finance their activities and attacks, a phenomenon fostered by the growing integration of financial flows and the ingenuity of terrorists when it comes to exploiting loopholes in the system[4]. For instance, they can make purchases, as well as raise, collect and move funds using different techniques such as direct solicitation, e-commerce, 'fake' charitable organisations, exploitation of online payment tools[5], etc. A recent research paper, focused on a sample of 231 individuals that acted on behalf of the Islamic State in the US between 2012-2020, identified 224 instances of money being moved totalling $480,000 and 319 of goods and services being purchased for a sum of $96,980[6]. Cryptocurrencies such as Bitcoin are increasingly appealing to terrorists due to their decentralisation and anonymity features.

Online Training

The Internet is also "*an alternative training ground*[7]" and a 'knowledge-sharing hub' for confirmed and would-be terrorists, given the number of training materials disseminated online (manuals, information, audio, and video files, etc.). The methods to share such training materials, as well as the platforms used, are profuse and the topics covered range from 'how to join terrorist organisations' to 'how to construct explosives and weapons', passing by 'how to carry out an attack'. For instance, Internet Archive has been abundantly used by terrorist organisations to store and disseminate training manuals: in 2021, "*researchers discovered a large cache of explosive manuals on the Internet Archive, finding 37 different manuals totalling more than 1,000 pages. The collection had been online for five years and received more than 10,000 views before it was removed*[8]". The profusion of free training materials available can be particularly useful for potential lone-wolf terrorists, thus able to find any information in just a few clicks.

Planning and Coordinating Attacks

The Internet can also be used by terrorists to plan and coordinate specific attacks. For instance, we know that 9/11 attacks relied on the Internet for planning and coordination. In Europe, allegations have been made as to whether terrorists could have exploited PS4 features to plan the 2015 Paris attacks. While it is unclear if such tools were effectively used, because of a lack of evidence[9], "*there are a few options, from sending messages through the PlayStation Network (PSN) online*

[4] European Council - Council of the European Union (2023), "Fight against money laundering and terrorist financing". Available here.
[5] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.7.
[6] Whittaker, J. (2022), "The Role of Financial Technologies in US-Based ISIS Terror Plots". *Studies in Conflict & Terrorism*, pp.1-26. Available here.
[7] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.8.
[8] Weimann, G. and Vellante, A. (2021), "The Dead Drops of Online Terrorism". *Perspectives on Terrorism*, August 2021, Vol. 15, No. 4, p. 40. Available here.
[9] "Did Paris terrorists really use Playstation 4 to plan attacks?", *The Telegraph*, 16 November 2015. Available here.

gaming service and voice-chatting to even communicating through a specific game[10]*"*. This explains how these features could have been used. Another example is Brenton Tarrant, the perpetrator of the 2019 Christchurch Mosque shootings, who mobilised many resources to plan and perpetrate the massacre, including online ones[11]. Simple means of remote communication can be used to plan attacks, thus falling into this category.

Cyberterrorism: Myth or Reality?

Finally, the Internet and related technologies can (or rather could) be used by terrorists to launch cyberattacks. Here we enter the realm of fully-fledged cyberterrorism, a phenomenon that has generated a lot of angst in the late 1990s and in the aftermath of 9/11, but whose risk was greatly overestimated at the time[12]. Where do we stand 20 years later? Is cyber-terror a "*looming threat or [a] phantom menace*"[13]? If some incidents (might) have been labelled as cyberterrorism, the phenomenon is still marginal or at least difficult to identify. Indeed, it should not be confused with other phenomena such as cyberattacks, cyberwarfare, hacktivism, or general uses of the Internet by terrorists. There is no doubt that capabilities have increased in parallel with the development of ever-sophisticated technologies but the "*most immediate online threat from non-state terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit supporters rather than engage in cyberterrorism*[14]".

Online vs. Offline?

The terrorists use Internet and online platforms with great adaptability and ingenuity, their activities serving different purposes. Of course, complementary activities or subcategories can also be identified: OSINT-like activities, virtual community building, risk mitigation, execution, psychological warfare, publicity, data mining, mobilisation, networking, etc. As shown in this article the spread of terrorist content online has real world impact. However, what should be really highlighted is the intertwined nature of both spheres: the dichotomy between offline and online is a myth or a misconception, both regarding radicalisation processes and attack planning, as terrorists and violent extremists usually engage in activities in both spheres. In short, the Internet operates as a facilitative tool, used for instrumental purposes[15].

Adeline KUGLER

Pierre SIVIGNON

[10] "How ISIS Terrorists May Have Used Playstation 4 to Discuss and Plan Attacks", *Forbes*, 14 November 2015. Available here.
[11] Veilleux-Lepage, Y., Daymon, C. and Amarasingam, A. (2020), "The Christchurch Attack Report: Key Takeaways on Tarrant's Radicalization and Attack Planing". *International Center for Counter-Terrorism* (ICCT Perspective), December 2020, p.3. Available here.
[12] Weimann, G. (2004), "Cyberterrorism. How real is the threat?". *United States Institute of Peace*, Special Report 119, December 2004, p.1. Available here.
[13] Dunn Cavelty, M. (2008), "Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate". *Journal of Information Technology & Politics*, 4:1, pp.19-36. Available here.
[14] Kenney, M. (2015), "Cyber-Terrorism in a Post-Stuxnet World". *Orbis*, 59, Winter 2015, p.111. Available here.
[15] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J. (2017), "Terrorist Use of the Internet by the Numbers". *Criminology & Public Policy*, 16, p.101. Available here.

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.