FR!SCO

Fighting Terrorist Content Online

D2.1: Mapping Report on needs and barriers for compliance

Understanding small and micro HSPs' needs and awareness in relation to implementing the TCO Regulation requirements

Grant Agreement ID	101080100	**Acronym**	FRISCO
Project Title	Fighting teRrorISt Content Online		
Start Date	15/11/2022	**Duration**	24 Months
Project URL	https://friscoproject.eu/		
Contractual due date	14/05/2023	**Actual submission date**	15/05/2023
Nature	R = Document, report	**Dissemination Level**	PU = Public
Author(s)	Pal Boza (Tremau), Noah Douglas (Tremau), Pierre Sivignon (Civipol)		

This project has received funding from the European Union's Internal Security Fund (ISF) programme under Grant Agreement No 101080100. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Contributor(s)	Elena Galifianaki (NCSR-D), Charalampos Mavrikas (NCSR-D), Martina Manfredda (D-Learn), Tamas Berecz (INACH), Charlotte Devinat (INACH), Adinde Schoorl (INACH), Klara Heilingbrunner (IVSZ), Zsuzsa Lovas (IVSZ), Louis-Victor de Franssu (Tremau), Agne Kaarlep (Tremau), Arwa Ben Ahmed (VPN), Rositsa Dzhekova (VPN)
Reviewer(s)	Vangelis Karkaletsis (NCSR-D), Panagiotis Krokidas (NCSR-D)

Document Revision History *(including peer reviewing & quality control)*

Version	Date	Changes	Contributor(s)
1.0	15/05/2023	Final	All

Executive Summary

The objective of the *Fighting Terrorist Content Online* (FRISCO) project is to inform and support Hosting Service Providers (HSPs) to comply with the Regulation (EU) 2021/784, addressing the dissemination of terrorist content online (TCO Regulation), which entered into force on the 7th of June 2021.

Conducted over a six-month period ending in May 2023, the present mapping report reflects on the needs of European micro and small HSPs, gathering their insights to identify challenges and gaps in relation to the TCO Regulation. Three main methods were employed by the FRISCO team to gather the information necessary for this report: (1) semi-structured interviews with target group representatives and key stakeholders; (2) online survey disseminated among European HSPs; and (3) comprehensive desk research.

Based on institutional data and most recent scientific papers, the result of our desk research efforts helped us to circumscribe our subject and guide our investigations. We showed that terrorist uses of the Internet were mainly articulated around five standard activities (propaganda, financing, training, planning, cyberattacks), with a constant intertwining between online and offline realms. Facing the difficulty to obtain precise figures on the spread of terrorist content online, we focused on trends, identifying three major ones regarding the type of platforms used: a lasting reliance on online dead drops, the recent rise of decentralised platforms and the search for (smaller) platforms with weak content moderation. Finally, we were able to assess an increasing exposure of smaller European HSPs to terrorist content, especially regarding certain types of platforms and services.

Regarding our findings, one of the key takeaways of this report is that micro and small HSPs tend to have a very limited awareness and knowledge of the TCO Regulation. As a comparison, we found that HSPs are clearly more aware of the Digital Services Act (DSA) than the TCO Regulation. However, despite the lack of awareness and preparedness a large majority of HSPs perceive themselves as at low risk for terrorist content.

In general several stakeholders have also pointed out the lack of resources that micro and small HSPs are facing. This also affects their willingness to invest in developing the right processes and implementing efficient tools not only to be compliant with new regulations but also to serve their own business needs. This would only be changed in case an imminent manifestation of a (terrorist) threat would push them to do so, otherwise these investments would be likely to be postponed for as long as possible.

Furthermore, micro and small HSPs fundamentally lack the tools but even more importantly the processes to efficiently implement the provisions of the TCO Regulation. A large majority of the responding HSPs have not set-up the tools and processes in relation to be compliant with the TCO Regulation. This is to some extent reflected by the fact that only about 20% of the HSPs responding to our online survey moderate all content generated by users in their services.

Providing support for HSPs would help to clear the current lack of information that has left many HSPs unaware of both their requirements as well as how to reach these requirements. Participation in FRISCO's training and awareness activities may help bridge this knowledge gap and improve HSPs' ability to effectively address terrorist content on their platforms. In addition, FRISCO’s products focused on fostering knowledge exchange and providing guidance on good practices and available tools is likely to directly address HSPs needs of practical know-how when implementing the TCO Regulation.

Table of Contents

1. Introduction **8**
1.1 The FRISCO project - presentation 8
1.2 The report's objective - purpose and scope 8
1.3 Approach for Work Package and Relation to other Work Packages and Deliverables 10
1.4 Methodology and structure of the report 10
2. Terrorism in the digital EU - trends and challenges **13**
2.1 Defining terrorism and terrorist content online 13
2.2 Overview of the terrorist threat in the European Union 15
2.3 Understanding the terrorist (mis)uses of the Internet 16
2.4 Identifying trends in the spread of terrorist content online 21
2.5 Assessing the exposure of smaller platforms 27
2.6 Stressing the measures imposed by the TCO Regulation 31
3. Findings **34**
3.1 Key takeaways from our investigations 34
3.2 Hosting service providers 34
3.3 Law enforcement agencies National & Competent Authorities 41
4. Conclusions **43**
5. Appendices **46**
5.1 Overview of the terrorist threat in the European Union 46
5.2 Features attractive to terrorist groups for internal and external communications 51
6. References **52**

List of Figures and Tables

Figure 1 - Typology of platforms used by terrorists (by technology types and practical uses)
Figure 2 - Intervention logic behind the TCO Regulation (2018)
Figure 3 - TCO Regulation overview
Figure 4 - Q1/ User base size
Figure 5 - Q2/ Moderation of user-generated content
Figure 6 - Q3/ Awareness regarding the TCO Regulation
Figure 7 - Q4/ Awareness regarding the DSA
Figure 8 - Q5/ Definition of terrorist content
Figure 9 - Q6/ Exposure to terrorist content
Figure 10 - Q7/ Perceived risk of being affected by terrorist content
Figure 11 - Q8 / Implementation of a single Point of Contact
Figure 12 - Q9/ Implementation of a complaint mechanism
Figure 13 - Q10/ Implementation of automated measures
Figure 14 - Q11/ Implementation of transparency measures
Figure 15 - Q12/ Communication with LEAs
Figure 16 - Q13/ Potential help areas
Figure 17 - Terrorist attacks in the EU between 2010 and 2011
Figure 18 - Terrorism-related arrests in the EU between 2010 and 2011
Figure 19 - Terrorist attacks and arrests in the EU between 2019 and 2021
Figure 20 - Global deaths from terrorism by regions (1970-2020)
Figure 21 - Terrorism death in Western Europe (1970-2017)

Figure 22 - Features attractive to terrorist groups for internal and external communications

List of Terms & Abbreviations

Abbreviation	Definition
CSAM	Child Sexual Abuse Material
DSA	Digital Services Act
EU	European Union
EU IRU	EU Internet Referral Unit
FRISCO	Fighting teRrorISt Content Online
GDPR	General Data Protection Regulation
GIFCT	Global Internet Forum to Counter Terrorism
HSP	Hosting Service Provider
IRMA	Internet Referral Management Application
LEA	Law Enforcement Agency
NCA	National Competent Authority
OSINT	Open Source Intelligence
PERCI	*Plateforme Européenne de Retraits de Contenus Illégaux sur Internet*
RAN	Radicalisation Awareness Network
SMEs	Small and medium-sized enterprises
TaT	Tech against Terrorism
TCAP	Terrorist Content Analytics Platform
TCO	Terrorist Content Online
TE-SAT	Terrorism Situation and Trend Report
TOW	Terrorist Operated Website
T/VEOW	Terrorist / Violent Extremist Operated Website
WP	Work Package

1. Introduction

1.1 The FRISCO project - presentation

Terrorist and other illegal content online is an increasing issue both from a security and public policy perspective. In today's complex, interconnected world, countering the spread of terrorist content online requires a multifaceted approach. One which recognizes the interdependence of global and digital phenomena and requires a combination of legislative, non-legislative and voluntary measures based on collaboration between authorities and Hosting Service Providers (HSPs).

The Regulation (EU) 2021/784, addressing the dissemination of terrorist content online (TCO Regulation), entered into force in this context on the 7th of June 2021 and is applicable as of the 7th of June 2022 and sets out several specific measures that hosting service providers exposed to TCO Regulation must implement to address the misuse of their services.

In this context, the objective of the *Fighting Terrorist Content Online* (FRISCO) project is to support HSPs to comply with the TCO Regulation, through:

(1) Informing HSPs and increasing their awareness of the Regulation and their related obligations.

(2) Developing and validating tools, frameworks, and mechanisms to support HSPs in the implementation of the Regulation.

(3) Sharing experiences, best practices and tools to support its implementation.

The project has received funding from the European Commission – Internal Security Fund under Grant agreement No 101080100 and will be realised between November 2022 and November 2024. The consortium realising the project is composed of 8 beneficiaries from 6 different European countries, involving NCSR-D (Greece), the French Ministry of Interior (France), Tremau (France), Civipol (France), Violence Prevention Network (Germany), IVSZ (Hungary), D-Learn (Italy) and INACH (Netherlands).

1.2 The report’s objective - purpose and scope

The current report has been produced to map the needs and barriers for compliance, as well as general awareness, of micro and small HSPs in relation to the TCO Regulation. It presents the results of Task 2.1 (*Mapping of need and barriers for compliance*), conducted over a six-month period (14th of November 2022 – 14th of May 2023) by the FRISCO consortium with the participation of all consortium members. The mapping exercise aims to reflect on the needs of European micro and small HSPs, gathering their experiences and insights to identify challenges and needs in relation to the TCO Regulation. The objective of this study is to map the needs and barriers for compliance with the TCO Regulation to provide a better understanding concerning small HSP’s technical resources and processes human competences knowledge and skills general level of awareness concerning the TCO Regulation.

Understanding the needs of micro and small providers requires examining the relationships, experiences, and requirements of various actors. Hence solely focusing on micro and small HSPs would have limited our understanding of the complex ecosystem impacted by the TCO Regulation. To address this, we engaged also several different stakeholders in the space, such as Law Enforcement Agencies (LEAs), larger (including medium-sized) HSPs, Professional Associations of HSPs and other key stakeholders (such as Europol, the European Commission and experts), and reached out to them in order to broaden our knowledge base and inform our research.

The definition of 'Hosting Service Provider' given by the TCO Regulation is the following: "*a provider of services as defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council (14), consisting of the storage of information provided by and at the request of a content provider*", a content provider meaning "*a user that has provided information that is, or that has been, stored and disseminated to the public by a hosting service provider*[1]". To be exhaustive, the EU Directive 2015/1535 to which the TCO Regulation refers to, states at the mentioned article that service means "*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*[2]".

To further specify which services fall under TCO Regulation, two specific notions need to be addressed, those of 'storing' and 'disseminating to the public', which are key factors for understanding what constitutes a HSP under the regulation.

Definitions are provided, with "*the concept of 'storage' [is] understood as holding data in the memory of a physical or virtual server*[3]". This therefore means that *"Providers of 'mere conduit' or 'caching' services, [...] which do not involve storage, such as registries and registrars, as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services*[4]" fall outside of the scope of TCO Regulation.

Dissemination to the public is clarified as "*making the information easily accessible to users in general, without requiring further action by the content provider, irrespective of whether those persons actually access the information in question*[5]". Information in this case should be understood to include 'user-generated-content'. Therefore we can understand that "*providers of social media, video, image and audio-sharing services, as well as file-sharing services and other cloud services, insofar as those services are used to make the stored information available to the public*[6]" all fall under the scope of the regulation; while it can be understood that "*providers of services, such as*

[1] REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online, p.89. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN

[2] DIRECTIVE (EU) 2015/1535 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), p.3. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN

[3] REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online, p.81. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN

[4] *Ibidem.*

[5] *Ibidem*.

[6] *Ibid.*, p.82.

cloud infrastructure, which are provided at the request of parties, other than the content providers[7]" and "*emails or private messaging services*[8]" do not fall under the scope of HSP's under the TCO Regulation.

To ensure the integrity of our research process and to encourage open and honest communication, we implemented the following measures:

- *Anonymization*: in compliance with GDPR, all participants were assured that their responses and all personal information would be anonymized in the final report.
- *Chatham House Rule*: after obtaining consent to use the information gathered from interviews, we adhered to the Chatham House Rule, ensuring that the identification of the speakers remained confidential.

1.3 Approach for Work Package and Relation to other Work Packages and Deliverables

The project is delivered through five Working Packages (WP). WP1 will manage and coordinate day-to-day management activities of the project. WP2 is dedicated to the development of relevant tools. WP3 aims to create a training program and to develop e-training modules, while WP4 helps raise awareness of HSPs. WP5 is dedicated to the dissemination and exploitation of results.

The present mapping report is realised within the framework of WP2, task 2.1. The aim of task 2.1 is to provide a clear understanding of the needs of small and micro HSPs in the context of the TCO Regulation. To support this, a methodology will be developed at the start of WP2 with input from all partners, outlining how the target group will be reached (incl. through the multipliers - HSP associations) and methods for data collection, including an online survey among small HSPs across the EU. A mapping report with results and recommendations will be the basis for subsequent tool development, capacity building and training curriculum, best practice sharing and awareness raising activities (WP2, WP3 and WP4). In task 2.2 - based on the results of task 2.1 - technical tools, frameworks and mechanisms will be developed to decrease small and micro HSPs' barriers for compliance which will be tested in task 2.3.

1.4 Methodology and structure of the report

Methodology. Three main methods were employed by the FRISCO team to gather the information necessary for this report: (1) semi-structured interviews with target group representatives and key stakeholders; (2) online survey disseminated among European HSPs; and (3) comprehensive desk research.

[7] *Ibidem.*

[8] *Ibid.*, p.81.

- ***Semi-structured interviews***. During the six-month mapping exercise, we organised 36 interviews with mainly micro and small but also with medium HSPs, LEAs, Associations of HSPs and other stakeholders. The process involved 4 steps: (1) developing and testing a tailored set of questions, differentiated by the type of actor being interviewed ; (2) identifying and reaching out to appropriate interviewees ; (3) conducting the interviews ; (4) recording the minutes, extracting key information, and analysing it. The interviews generally lasted for at least one hour.
- ***Online survey***. To engage with a broader range of stakeholders, we created an online survey for HSPs to gauge their awareness of the TCO Regulation and assess the industry preparedness. FRISCO partners distributed the survey to HSPs, and HSP umbrella organisations in their respective countries through internally compiled email lists and industry networks. This helped gather quantitative data to complement the more qualitative insights from interviews.
- ***Desk research***. We conducted extensive desk research to collect additional information and to corroborate the findings from the interviews and the online survey. This involved reviewing existing literature, legislation, and relevant publications to gain a comprehensive understanding of the challenges posed by terrorist content online, the regulatory environment, and the general impact of TCO Regulation on the ecosystem.

Challenges and Limits to the findings. Despite our comprehensive methodology and approach, there were certain challenges and limitations to the findings of our study, which are important to acknowledge:

- ***Limited sample size***. Although we conducted a relatively large number of interviews, the sample size may not fully represent the entire European ecosystem. In total, our team has gathered the feedback of 48 European HSPs, 33 answers through our online survey and 15 through interviews.
- ***Non-response bias***. Despite reaching out to a large number of HSPs with our survey, the number of responses was rather limited. Indeed, the online survey has been sent: directly to more than 2000 HSPs ; indirectly through LEAs and associations of HSPs to more than 4000 HSPs.
- ***Subjectivity of qualitative data***. While the interviews provided us with valuable qualitative data, such data is often subject to interpretation and may be influenced by individual perspectives and biases, which could affect the overall analysis.

The report is structured into 4 main Sections :

1. Section 1 (*Introduction*) presents as an introduction the FRISCO project, details its objectives and target group and describes the used methodology.

2. Section 2 (*Terrorism in the digital EU - trends and challenges*) provides the results of our desk research, giving an overview of the general trends in relation to the spread of terrorism content online. It also presents details about how terrorists use the Internet for their purposes and assesses the exposure of smaller platforms to terrorist content.

3. Section 3 (*Findings*) presents the findings from the interviews and online survey…

4. …while Section 4 (*Conclusions*) summarises the key takeaways in relation to HSPs and LEAs.

2. Terrorism in the digital EU - trends and challenges

2.1 Defining terrorism and terrorist content online

Due to the complexity and richness of the broader topics we are dealing with in this report, as a first step we provide a description of the key concepts. These will be used throughout the report and rely on EU legal texts and the wider scholarly debate.

Terrorism. *"While 'terrorism' is one of the most widely used terms in adversarial political discourse, there is still no international consensus about its exact meaning*[9]". Defining terrorism is a challenge in itself, to the point that legal and academic definitions cannot be precisely counted. Indeed, despite the existence of legal definition(s), on which European LEAs act, even the most trained actors or organisms may encounter challenges when trying to identify terrorism, terrorists, terrorist acts or terrorist content.

In defining 'terrorism' for our report, we referred to EU regulations. However, EU law does not define 'terrorism' itself, but rather 'terrorist offences'. This approach is both convenient and operative, as terrorism is typically addressed within Member States under penal law and criminal jurisdiction. By defining offences instead of the concept itself, the EU avoids potential pitfalls and maintains a practical focus. Based on elements highlighted by the EU Directive 2017/541 on combating terrorism, transposed into Member States' national legislation in 2018 and cited by the TCO Regulation, "*terrorist attacks are criminal offences carried out with the purpose of intimidating a population or trying to coerce a government or international organisation, seriously destabilising or destroying fundamental political, constitutional, economic or social structures of a country or an international organisation*[10]".

Furthermore, the EU Directive 2017/541 also identifies several offences related to terrorist activities, which relate to the issue of terrorist content online : "*public provocation to commit a terrorist offence ; recruitment for terrorism ; providing training for terrorism ; receiving training for terrorism ; travelling for the purpose of terrorism ; organising or otherwise facilitating travelling for the purpose of terrorism ; terrorist financing*[11]". We also draw attention to the EU terrorist list, which makes it easier to identify previously listed terrorist persons and entities.

Before going further, we should also stress that terrorism is often linked to another phenomenon, 'violent extremism', especially regarding right-wing / left-wing extremist ideologies and their online manifestations, making it more difficult to identify and distinguish related content or activities. As both phenomena communicate with each other and are often treated together in institutional reports and scientific articles, we will sometimes refer to 'violent extremism' in this report.

[9] Schmid, A. P. (2023), "Defining terrorism". *International Center for Counter-Terrorism* (ICCT Report), March 2023, p.2. URL : https://www.icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf

[10] Europol (2022), *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg, p.6. URL : https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

[11] DIRECTIVE (EU) 2017/541 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, pp.14-15. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN

Terrorist offences as defined by Article 3 of the EU Directive 2017/541 on combating terrorism[12]

1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences were committed with one of the aims listed in paragraph 2:
(a) attacks upon a person's life which may cause death;
(b) attacks upon the physical integrity of a person;
(c) kidnapping or hostage-taking;
(d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
(e) seizure of aircraft, ships or other means of public or goods transport;
(f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;
(g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (1) in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies;
(j) threatening to commit any of the acts listed in points (a) to (i).

2. The aims referred to in paragraph 1 are:
(a) seriously intimidating a population;
(b) unduly compelling a government or an international organisation to perform or abstain from performing any act;
(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

Terrorist content online. In our hyperconnected world, terrorists have leveraged internet and communication technologies for their purposes. In this task, we relied on EU Regulations for clear standards and definitions. The TCO Regulation's definition of 'terrorist content' is based on the terrorist offences outlined in EU Directive 2017/541. Terrorist content consists of *"text, images, audios or videos used to incite terrorist acts, give instructions on how to commit offences and/or solicit participation in terrorist groups*[13]*"*. Thereby, different types of online behaviours and content can be labelled as terrorist within the framework of the TCO Regulation, such as propaganda, recruitment, training etc. Nevertheless, the content provider and the context should not be disregarded : "*[m]aterial disseminated for educational, journalistic, artistic or research purposes or*

[12] *Ibid.*, p.13.
[13] See : European Council - Council of the European Union (2022), "*Infographic - Addressing the dissemination of terrorist content online*". URL : https://www.consilium.europa.eu/en/infographics/terrorist-content-online/

for awareness-raising purposes against terrorist activity should not be considered to be terrorist content[14]". For instance, a newspaper sharing a Daesh video for information purposes is not producing the same type of content as a fully-fledged Daesh member.

Terrorist content as defined by Article 2 of the Regulation 2021/784 on addressing the dissemination of terrorist content online (TCO Regulation) (p.90)

(7) 'terrorist content' means one or more of the following types of material, namely material that:

(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;

(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;

(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

2.2 Overview of the terrorist threat in the European Union

In 2023, terrorism remains a key threat to the European Union's internal security and citizens. But beyond quantifiable aspects, such as attacks, arrests and sentences, it remains a difficult phenomenon to measure or assess, especially regarding online terrorist activities. As online and offline interactions often go hand in hand, separating both realms is a conceptual pitfall we wish to avoid in this report : indeed, there is no "*digital dualism*" in our contemporary societies, online and offline activities relating to terrorism are thus constantly intertwined[15]. To assess the threat caused by the spread of terrorist content online in the EU, we first need to understand the broader context in which it takes place.

For more information on this subject, the reader is referred to Appendix 5.1. We chose to present these data in the Appendices' part to focus on our main subject, the spread of terrorist content online. As shown in Appendix 5.1, there are two key takeaways from a short overview of the terrorist threat in the European Union : first and foremost, Western Europe is far from being the region the most affected by terrorism on a global scale (if we take into account attacks, arrests and deaths) ; second, terrorism is not on the rise in Western Europe, if we compare the current situation with the 70s and the 80s, which implies a probable distortion of the threat perception.

[14] REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online, p.81. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN

[15] Whittaker, J. (2022), "Rethinking online radicalization". Perspectives on Terrorism, August 2022, Vol. 16, No. 4, p.30. URL : https://www.jstor.org/stable/10.2307/27158150

Nevertheless, it should be stressed that terrorism remains a deadly threat in the European Union. For instance, the "*proliferation of terrorist online postings and their documented impact on recruitment of fighters and activation of lone-wolf operations*[16]" is a major concern, lone actors being "*the primary perpetrators of terrorist and violent extremist attacks in Europe*[17]". Furthermore, although these terrorists are described as lone-wolves, they do not necessarily "*act in complete isolation*" because "*[o]nline community building often plays a key role, as it connects peers virtually on a global scale*" : this phenomenon "*drives radicalisation and provides access to terrorist propaganda, instructional material and opportunities for procurement of weapons and explosives precursors*[18]". This dialectic between online community building and actualisation of lone-wolves radicals is particularly true for both jihadist and right-wing terrorisms.

2.3 Understanding the terrorist (mis)uses of the Internet

With approximately 5,3 billion regular users[19], the Internet and the ever-sophisticated communication tools it provides have become increasingly pervasive in our lives since the early 1990s. It has "*created a network with a truly global reach, and relatively low barriers to entry*" making it easier and cheaper "*for an individual to communicate with relative anonymity, quickly and effectively across borders, to an almost limitless audience*[20]". The later development of social media, as well as new technologies such as instant messaging, end-to-end encryption or cloud-sharing, has offered further opportunities for individuals and groups to communicate and disseminate content. Unsurprisingly, "*the ability to reach such a large audience with minimum cost also attracts individuals who want to use the Internet for illegal [or terrorist] purposes*[21]" - and this is precisely what terrorists have been doing since the late 1990s, at least[22]. The Internet can be used for both internal (e.g. communicating and planning) and external purposes (e.g. publicising activities and recruitment of new members for instance). Thus, terrorist content targets different audiences that can be divided into three main categories : "*current and potential supporters*", "*international public opinion*" and "*enemy publics*[23]".

[16] Weimann, G. and Vellante, A. (2021), "The Dead Drops of Online Terrorism". *Perspectives on Terrorism*, August 2021, Vol. 15, No. 4, p. 39. URL: https://www.jstor.org/stable/10.2307/27044234

[17] Europol (2022), *op. cit.*, p.4

[18] *Ibidem*.

[19] "Un tiers de la population mondiale n'a toujours pas accès à Internet", *Les Echos*, 16 Septembre 2022. URL : https://www.lesechos.fr/tech-medias/medias/un-tiers-de-la-population-mondiale-na-toujours-pas-acces-a-internet-1788569

[20] United Nations Office on Drugs and Crime (2012), *The use of Internet for terrorist purposes*, New York, p.3. URL : https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf

[21] 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*, p.3. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0408

[22] See : Google Books Ngram Viewer - "Terrorism Online" (1975-2019).
URL : https://books.google.com/ngrams/graph?content=terrorism+online&year_start=1975&year_end=2019&corpus=en-2019&smoothing=3

[23] Weimann, G. (2004), "How modern terrorism uses the Internet". United States Institute of Peace, Special Report 116, March 2004, pp. 4-5. URL : https://www.usip.org/sites/default/files/sr116.pdf

With its 450 million inhabitants and 92.5% of households with Internet access[24], the European Union is a 'market to conquer' for terrorists, a major audience/recruitment pool. Concerning the online behaviour and practices of its citizens, almost 70% are regular users of social media, a similar share watch videos or live-streamings, 47% use file storage or sharing services and 51% read blogs, comment on articles or news websites[25]. Why is the Internet used by terrorists is thus a self-explanatory statement : it is an easy, cheap and convenient way to communicate, build a community, plan actions and share content across borders, all this anonymously and with the prospect of reaching a massive audience. The uses of the Internet by terrorist individuals and groups serve a number of purposes that fall into five major categories, similar to the ones the UNODC identified back in 2012[26] : propaganda, financing, training, planning, and cyberattacks. Terrorist propaganda itself responds to at least 3 objectives (or sub-categories) : recruitment, incitement to terrorism and radicalisation. Of course, complementary activities or subcategories can also be identified, such as OSINT-like activities, virtual community building, risk mitigation[27], execution[28], psychological warfare, publicity, data mining, mobilisation or networking[29], but we will only cover the aforementioned ones for the sake of clarity and conciseness.

Propaganda. Terrorists, regardless of their ideology, use the Internet as a platform to disseminate propaganda. This online propaganda "*generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities*" and "*may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organisations or sympathisers*[30]". For instance, *Internet Archive* has been widely used in recent years by terrorist groups, especially jihadist[31], to disseminate terrorist propaganda (and avoid removal) : *"a wide variety of terrorist groups such as ISIS, al-Qaeda, and the banned British neo-Nazi group National Action are storing on Internet Archive instructions like bomb-making videos, beheading clips, seductive calls to commit terrorist attacks and attempts to recruit new members and followers*[32]*"*. This brings us to our three subcategories as online propaganda "*aimed at potential or actual supporters may be focused on recruitment, radicalization and incitement to terrorism, through messages conveying pride, accomplishment and dedication to an extremist goal*[33]". An example of how terrorist propaganda can drive people to action is the one of Roshonara Choudhry, a 21-year-old British student and first Al-Qaeda sympathiser to attempt an assassination in Britain. After attempting to murder the Labour MP Stephen Timms in 2010, by stabbing him, she stated that she had been influenced by online sermons of cleric Anwar al-Awlaki she had watched on Youtube and "*that made her understand that 'even women are supposed to*

[24] See : 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".
URL : https://www.insee.fr/fr/statistiques/2385835#:~:text=Lecture%20%3A%20en%202022%2C%2092%2C,de%2016%20%C3%A0%2074%20ans

[25] European Commission (2018), *op. cit.*, p.3.

[26] United Nations Office on Drugs and Crime (2012), *op. cit.*, pp.3-12.

[27] 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. URL : https://onlinelibrary.wiley.com/doi/epdf/10.1111/1745-9133.12249

[28] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.11.

[29] Weimann, G. (2004), *op. cit.*, pp.5-9.

[30] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.3.

[31] "Jihadist content targeted on Internet Archive platform", Europol, 16 July 2021.
URL : https://www.europol.europa.eu/media-press/newsroom/news/jihadist-content-targeted-internet-archive-platform

[32] Weimann, G. and Vellante, A. (2021), *op.cit*., p.41.

[33] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.4

fight' and that she had an obligation to engage in violence[34]". Terrorist propaganda is really the core of publicly available terrorist content online, and probably the main challenge for European HSPs.

Financing. The Internet provides tools and opportunities for terrorist groups to finance their activities and attacks, a phenomenon fostered by "*the increasing integration of financial flow*", "*the global nature of terrorist organisations*" and "*the ingenuity of criminals to exploit gaps or loopholes in the system*[35]". As stated by the UNODC, "*[t]he manner in which terrorists use the Internet to raise and collect funds and resources may be classified into four general categories: direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations*[36]". The Internet and financial technologies are also used by terrorists to move their own funds and make purchases[37]. A recent research paper, focused on a sample of 231 individuals that acted on behalf of the Islamic State in US between 2012-2020, identified 224 instances of money being moved totalling $480,000 and 319 of goods and services being purchased for a total of $96,980[38]. Further, the scientific literature tends to show that Bitcoin and other cryptocurrencies "*may be used to finance terrorism*", because their decentralisation and anonymity features makes them difficult to regulate : thus, "*Bitcoin is often associated with criminal activities, including money laundering and the financing of terrorism*[39]".

Training. The Internet also is "*an alternative training ground*[40]" and a 'knowledge-sharing hub' for confirmed and would-be terrorists. It is hosting a "*growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice*[41]". 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, the aforementioned *Internet Archive* has been abundantly abused 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 totaling more than 1,000 pages. The collection had been online for five years and received more than 10,000 views before it was removed by the Internet Archive*[42]". The profusion of free training materials available can be particularly useful for would-be lone-wolf terrorists, thus able to find any information in just a few clicks. During the 2010s, the *Inspire* magazine case[43], allegedly published by Al-Qaeda in the Arabian Peninsula

[34] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J. (2017), *op. cit.*, p.108.

[35] See : European Council - Council of the European Union (2023), "*Fight against money laundering and terrorist financing*". URL : https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/

[36] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.7.

[37] Whittaker, J. (2022), "How do terrorists use financial technologies?", International Center for Counter-Terrorism, 9 November 2022. URL : https://www.icct.nl/publication/how-do-terrorists-use-financial-technologies

[38] Whittaker, J. (2022), "The Role of Financial Technologies in US-Based ISIS Terror Plots". *Studies in Conflict & Terrorism*, pp.1-26. URL : https://www.tandfonline.com/doi/epdf/10.1080/1057610X.2022.2133345?needAccess=true&role=button

[39] Song, Y., Chen, B., & Wang, X. Y. (2023). "Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related?". *Financial innovation*, *9*(1), 29. URL : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9860235/#CR50

[40] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.8.

[41] *Ibidem*.

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

[43] Lemieux, A., Brachman, J. M., Levitt, J., and Wood, J. (2014), ""*Inspire* Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model." *Terrorism and Political Violence* 26 (January), pp. 354-371. URL : https://www.tandfonline.com/doi/abs/10.1080/09546553.2013.828604#.Uu-nW_vWS_A&nbsp

(AQAP) "*with the stated objective of enabling Muslims to train for jihad from home*[44]", has been much talked about. Recently, similar "*pro-IS publications [focusing] on the South Asian region*" have been disseminated online, providing propaganda and training materials, such as "*Sawt-al-Hind (Voice of India) [...] ; the Urdu online magazine Yalghar launched in April 2021; and an IS-KP [Islamic State – Khorasan Province] magazine Voice of Khurasan in February 2022*[45]". Most of these magazines are available online with a single click, shared and stored on platforms such as *Internet Archive*, *NextCloud* or *RocketChat*[46].

Planning. As online and offline activities often go hand in hand, located somewhere on the same continuum and overlapping constantly, it is no surprise that "*criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology*[47]". Thus, the Internet can also be used by terrorists to plan and coordinate specific attacks. For instance, "*Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks*" as "*[t]housands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks*[48]". In Europe, allegations have been made as to whether terrorists could have used PS4 facilities to plan for the 2015 Paris attacks[49] - if it is unclear if such tools were effectively used, because of a lack of evidence[50], "*there are a few options, from sending messages through the PlayStation Network (PSN) online gaming service and voice-chatting to even communicating through a specific game*[51]". Simple means of remote communication can indeed be used to plan attacks and thus fall under this category of terrorist uses of the Internet. A last example, investigations showed that Brenton Tarrant, the 2019 Christchurch mosque attacker, mobilised "*significant planning and resources*" to perpetrate the massacre, including online ones[52].

Cyberattacks. Finally, the Internet and related technologies can be used by terrorists to launch cyberattacks, which refer to "*the deliberate exploitation of computer networks as a means to launch an attack [...] typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, phlooding or other means of unauthorized or malicious access*[53]". With this category, we enter in the realm of fully-fledged 'cyber-terrorism', a phenomenon that has generated a lot of angst in the late 1990s and in the aftermath of 9/11. As stated in 2004 by

[44] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.8.

[45] Europol (2022), *op. cit.*, p.34

[46] "Extremist Content Online: Pro-ISIS Propaganda Site Reemerges One Month After Takedowns", *Counter Extremism Project*, 28 April 2020. URL : https://www.counterextremism.com/press/extremist-content-online-pro-isis-propaganda-site-reemerges-one-month-after-takedowns

[47] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.8.

[48] Weimann, G. (2004), *op. cit.*, p.10.

[49] "How ISIS Terrorists May Have Used Playstation 4 to Discuss and Plan Attacks'', *Forbes*, 14 November 2015. URL : https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/

[50] "Did Paris terrorists really use Playstation 4 to plan attacks?", The Telegraph, 16 November 2015, URL : https://www.telegraph.co.uk/technology/video-games/playstation/11997952/paris-attacks-playstation-4.html

[51] "How ISIS Terrorists May Have Used Playstation 4 to Discuss and Plan Attacks'', *Forbes*, 14 November 2015. URL : https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/

[52] 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. URL :https://www.icct.nl/sites/default/files/2022-12/Christchurch-report-Dec-2020_Spelling-fixed.pdf

[53] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.11.

Gabriel Weimann : "*Many of these fears […] are exaggerated : not a single case of cyberterrorism has yet been recorded, hackers are regularly mistaken for terrorists, and cyberdefenses are more robust than is commonly supposed. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the danger without inflating or manipulating it*[54]". Where do we stand 20 years later ? Is cyber-terror "*a looming threat*" or a "*phantom menace*"[55]? If some incidents (might) have been labelled as 'cyberterrorism' - such as the 2007 cyberattacks on Estonia, the disclosure of 20 000 Israeli's credit card details in 2012[56] or "*ideologically motivated cyberattacks*[57]" performed by far-left groups for instance[58] - cyber-terrorism is still marginal, or at least difficult to identify. Indeed 'cyber-terrorism' *per se* "*differs from cyber-attacks, cyber-warfare, hacktivism and terrorists' use of the Internet*" ; sure, capabilities have increased in parallel with the development of ever-sophisticated technologies, but "*[t]he 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 cyber-terrorism*[59]".

As shown through the various examples, the spread of terrorism and terrorist content online, or 'in cyberspace', do have multiple impacts offline, in the real world. But what recent scientific literature highlights is the intertwined nature of both realms : the dichotomy between offline and online is a myth or a misconception, both regarding radicalisation processes and attack planning, as fully-fledged terrorists or violent extremists usually engage in activities in both realms. The Internet is often used as a facilitative tool, for instrumental purposes, it is "*a facilitator, rather than a driver of terrorist behaviours*[60]". A study conducted in 2017 on a set of 223 convicted United Kingdom-based terrorists on their online activities and behaviours[61], came to the following conclusion : "*Violent radicalization should […] be framed as cyber-enabled rather than as cyber-dependent while underlining that enabling factors differ from case to case depending on need (i.e., who or what to attack and what tactics to use) and circumstance (i.e., availability of co-offenders, expertise, and ideology). The use of the Internet was largely for instrumental purposes whether it was pre-attack (e.g., surveillance, learning, practice, or communication) or post-attack (e.g., disseminating propaganda). There is little evidence to suggest that the Internet was the sole explanation prompting actors to decide to engage in a violent act*[62]". To conclude on this issue, the

[54] Weimann, G. (2004), "Cyberterrorism. How real is the threat?". United States Institute of Peace, Special Report 119, December 2004, p.1. URL : https://www.usip.org/sites/default/files/sr119.pdf

[55] 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. URL : https://www.tandfonline.com/action/showCitFormats?doi=10.1300%2FJ516v04n01_03

[56] "Cyberattack exposes 20,000 Israeli Credit Card Numbers and Details about Users", *The New York Times*, 6 January 2012. URL : https://www.nytimes.com/2012/01/07/world/middleeast/cyberattack-exposes-20000-israeli-credit-card-numbers.html

[57] Holt, J. T., Lee, J. R., Freilich, J. D., Chemark, S. M., Bauer, M. J., Shillair, R. and Ross, A. (2002), "An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks". *Terrorism and Political Violence*, 34:7, pp.1305-1320. URL : https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F09546553.2020.1777987

[58] Holt, J. T., Stonhouse, M., Freilich, J. and Chermak, S. M. (2021), "Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups, Terrorism and Political Violence". *Terrorism and Political Violence*, 33:3, pp.527-548. URL : https://www.tandfonline.com/doi/abs/10.1080/09546553.2018.1551213?journalCode=ftpv20

[59] Kenney, M. (2015), "Cyber-Terrorism in a Post-Stuxnet World". *Orbis*, 59, Winter 2015, p.111. URL : https://www.researchgate.net/publication/270914520_Cyber-Terrorism_in_a_Post-Stuxnet_World

[60] Whittaker, J. (2022), "How do terrorists use financial technologies?", International Center for Counter-Terrorism, 9 November 2022. URL : https://www.icct.nl/publication/how-do-terrorists-use-financial-technologies

[61] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J. (2017), *op. cit.*

[62] *Ibid.*, p.114.

same study also identified profiles among terrorists that were more likely to learn online than others : extreme-right wing individuals; attack planners; perpetrators of lethal attacks; committers of improvised explosive device and/or armed assaults; members of terrorist cells; individuals engaged in recruitment tentatives, nonvirtual network activities and place interactions[63]. These findings are completed by relevant figures regarding the convicted terrorists' online activities and behaviours[64] :

- 76% used Internet to learn about one several aspect of their (intended) activities
- 61% had an online activity related to their radicalisation journey or attack planning
- 44% downloaded extremist media, 30% accessed extremist ideological content online
- 32% used online resources to prepare for their attacks
- 29% communicated with other terrorists (emails, online discussion forums, chat rooms)
- 15% disseminated terrorist propaganda online themselves
- 14% were inspired to commit violent acts after witnessing something online
- 9% tried to recruit other persons online

2.4 Identifying trends in the spread of terrorist content online

Given the objective of our report and project, a pivotal question remains unanswered so far : what is the extent of the spread of terrorist content online? Regarding available figures, some European LEAs entitled to report or remove content do publish data about their activities. For instance, the French LEA in charge of illegal content monitoring and reporting, Pharos, has dealt with 263,825 content in 2021 of which 7,894 were terrorist[65]. Nevertheless, during our interviews with them, other European LEAs have given figures far superior or inferior, ranging from 600,000 to 40 (all illegal content together). This huge gap can be explained by differences in internal capacities and/or domestic policies. Furthermore, this kind of data is facing several structural issues. First, we can assume that the reported terrorist content might just be 'the tip of the iceberg', accounting for a (small?) part of the total terrorist content published on the clear, deep and dark webs. Second, only looking at the publicly available content, as it is the case with TCO-like legislations, excludes *de facto* private channels of communication (e.g. instant messaging apps) or 'private content' (e.g. protected by passwords) from any quantitative analysis. Finally, some elements are likely to distort figures, such as VPNs, making the geolocation of data complex, or potential 'honeypots' created by LEAs to attract and trace terrorists, which may result in the manufacturing of "fake" terrorist content for investigation or monitoring purposes. To be complete on this issue and look further than European LEAs, we should also mention that interesting figures can be found in the *2022 Transparency Report*

[63] *Ibid.*, p.99
[64] *Ibid.*, pp.107-108
[65] 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. URL : https://www.assemblee-nationale.fr/dyn/opendata/CRCANR5L15S2022PO59051N047.html

of the TCAP (*Terrorist Content Analytics Platform*), launched in 2020 by *Tech against Terrorism* (TaT) and described as the "*world's largest database of verified terrorist content, collected in real time from verified terrorist channels on messaging platforms and apps*[66]". In a one-year-long reporting period (December 2020-November), 18,958 URLs containing terrorist content were thus identified by open-source intelligence experts and automated scrapers[67]. Nevertheless, as stated by the European Commission *2018 Impact Assessment* relating to TCO Regulation preparatory works, "*[g]iven its illegal nature but also the lack of systematic reporting on terrorist content identified online, comprehensive and fully reliable numbers of illegal content available online cannot be established*", even if "*reports on the amount of content removed by certain companies, the number of pieces of content referred by public authorities or figures produced by research can give an indication of the size of the problem*[68]" .

Thinking in terms of numbers therefore seems at best incomplete, at worst ineffective. However, what can be done to assess the extent of terrorism (and violent extremism) online is looking at trends, which can be more easily identified, especially regarding the type of platforms used by terrorists. This is of particular relevance for our project, focused on the needs of micro and small HSPs. Before detailing these trends, it is important to recall that terrorists, as all individuals or groups engaging in illegal activities, are by nature opportunist : they are constantly adapting to legislations' impediment and loopholes, switching to new (trendy or unmonitored) platforms and mobilising the ever-sophisticated tools available. The main common trends among terrorists is thus to adapt, with flexibility and agility, to the current digital trends and regulatory blind spots. The implementation of countermeasures by Member States and LEAs also push terrorists to search for alternative means of communication and content sharing : "*[t]hese measures - such as 'deplatforming' or removal of terrorist content online, suspension of social media accounts, and pressuring social media companies to remove terrorist propaganda - have led terrorists to seek new alternatives*[69]*'*". As pointed out by the LEAs we have interviewed as part of our mapping exercise, behaviours and platforms can change overnight, even if stable and lasting patterns can be identified.

We have chosen to present three relevant trends below : the lasting reliance on dead drops platforms ; the rise of decentralised web and platforms ; the search for (smaller) platforms with weak content moderation. Thus, the following information does not intend to constitute an exhaustive account of terrorism and violent extremism online, as some topics will not be covered *in extenso* because of our focus on the platforms used and the related behaviours, rather than on phenomena such as the pandemic impact, the potential misuse of the metaverse[70], the intersection

[66] Tech against Terrorism (2022), "Transparency Report. Terrorist Content Analytics Platform. Year One : 1 December 2020 - 30 November 2021", March 2022, p.2. URL : https://www.techagainstterrorism.org/wp-content/uploads/2022/03/Tech-Against-Terrorism-TCAP-Report-March-2022_v6.pdf

[67] *Ibidem.*

[68] 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*, p.7. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0408

[69] Weimann, G. and Vellante, A. (2021), *op.cit.*, p.39.

[70] Europol (2022), "Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab", Publications Office of the European Union, Luxembourg, 2022. https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf

between terrorism and online gaming[71], the mechanics of gamification[72][73], the spread of '*awful but lawful*' content, violent right-wing extremism and "*cyberfascism*[74]", etc. For instance, we witnessed a clear impact of the COVID-19 pandemic on both behaviours and themes mobilised by terrorists and violent (right-wing[75]) extremists online, as on the one hand "*terrorist propaganda disseminated online in 2021 has continued to reflect themes related to COVID-19*", and, on the other hand, "*[v]iolent anti-COVID-19 and anti-government extremism, which is not affiliated with traditional violent extremist and terrorist activities, emerged in some Member States and non-EU countries*[76]". These interconnections with and/or between other phenomena such as disinformation, conspiracy theories[77] and anti-government extremism[78][79], especially since the pandemic, are making it even more difficult to differentiate terrorist and other violent content, including incitement to violence, while affecting vulnerabilities to radicalisation, opening up new pathways. Furthermore, regarding similar dynamics, recent years have seen a rise of hybrid ideologies and ideological cross-overs[80], for instance between neo-nazism and salafi-jihadism[81].

Returning to platforms themselves, and before presenting the three trends aforementioned, TaT, in a 2021 report published for the *Global Internet Forum to Counter Terrorism* (GIFCT)[82], has built a particularly interesting typology, distinguishing platforms by technology types and their uses by terrorists and violent extremists. We will not rely on it entirely for part 2.4, as some may not be HSPs and/or do not fall under TCO Regulation scope. Nevertheless, this typology functions as a good summary of how given platforms, services and technologies can be misused by individuals and groups and thus understand how trends develop. Regarding the technology types, platforms used by terrorists can be divided in seven categories : social media platforms, messaging apps, alt-tech platforms, video-sharing platforms, file hosting platforms, gaming-related platforms and Terrorist Operated Websites (TOWs)[83]. Then, this time regarding the practical uses, online platforms are mainly used, according to TaT, as "*beacons*" (redirecting the target audience), "*content stores*"

[71] United Nations Counter-Terrorism Centre (2022), "Examining the Intersection Between Gaming and Violent Extremism", United Nations Office of Counter-Terrorism (UNCCT), Global Programme on Preventing and Countering Violent Extremism and Special Projects and Innovation Branch, 2022. URL : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf

[72] Lakhani, S. and Wiedlitzka, S. (2022), "Press F to Pay Respects": An Empirical Exploration of the Mechanics of Gamification in Relation to the Christchurch Attack", *Terrorism and Political Violence*. URL : https://www.tandfonline.com/doi/full/10.1080/09546553.2022.2064746

[73] Radicalisation Awareness Network (2021), " The gamification of violent extremism & lessons for P/CVE", Luxembourg: Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2021-03/ran_ad-hoc_pap_gamification_20210215_en.pdf

[74] Thorleifsson, C. (2022), *op. cit.*

[75] Radicalisation Awareness Network Practitioners (2021), "Capitalising on Crises How VRWEs Exploit the COVID-19 Pandemic and Lessons for P/CVE", Luxembourg : Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2022-02/ran_capitalising_crises_how_vrwe_exploit_covid-19_pandemic_082021_en.pdf

[76] Europol (2022), *op. cit.*, p.5.

[77] Radicalisation Awareness Network (2021), "Conspiracy theories and right-wing extremism – Insights and recommendations for P/CVE", Luxembourg : Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2021-04/ran_conspiracy_theories_and_right-wing_2021_en.pdf

[78] Jackson, S. (2022). What Is Anti-Government Extremism? *Perspectives on Terrorism*, *16*(6), 9–18. URL : https://www.jstor.org/stable/27185088

[79] Bjørgo, T., & Braddock, K. (2022). Anti-Government Extremism: A New Threat? *Perspectives on Terrorism*, *16*(6), 2–8. URL : https://www.jstor.org/stable/27185087

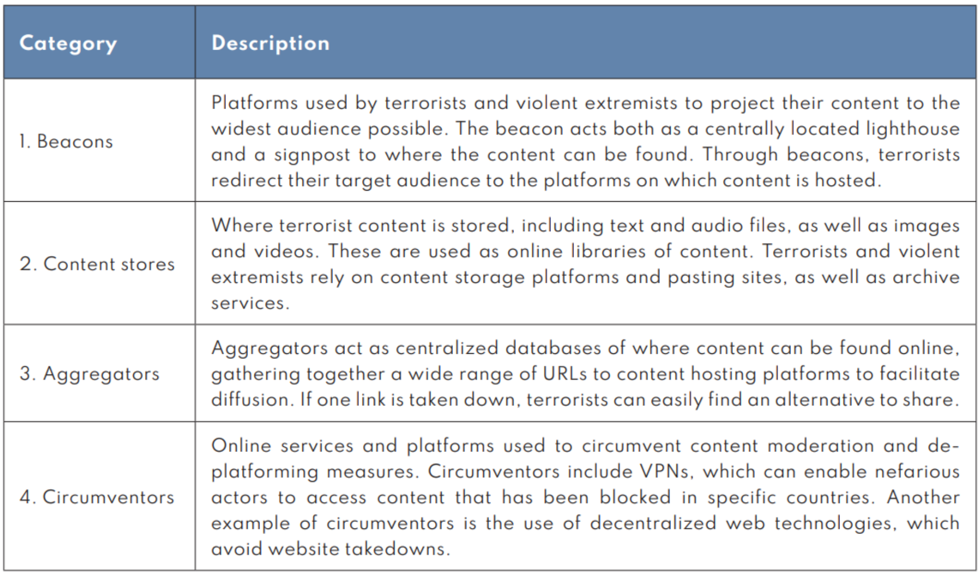
[80] Radicalisation Awareness Network Policy Support (2021), *Violent Extremism and Terrorism Online in 2021. The year in review*, Luxembourg: Publications Office of the European Union, 2021, p.46. URL : https://cronfa.swan.ac.uk/Record/cronfa62902

[81] "Connecting the Fringes: Neo-Nazi Glorification of Salafi-Jihadi Representations Online", Global Network on Extremism and Technology, 24 August 2021. URL : https://gnet-research.org/2021/08/24/connecting-the-fringes-neo-nazi-glorification-of-salafi-jihadi-representations-online/

[82] 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. URL : https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf

[83] *Ibid.*, pp.14-15.

(storing the relevant content), "*aggregators*" (centralising and facilitating its diffusion) and "*circumventors*[84]" (circumventing the countermeasures). Last point, if virtually all online platforms offering such possibilities may be invested by terrorists, some features, relating to "*security*", "*stability*", "*audience reach*" an "*usability*[85]", make them more or less attractive for internal and external communication purposes. For more information on the attractive features of given platforms, see Appendix 5.2.



Category	Description
1. Beacons	Platforms used by terrorists and violent extremists to project their content to the widest audience possible. The beacon acts both as a centrally located lighthouse and a signpost to where the content can be found. Through beacons, terrorists redirect their target audience to the platforms on which content is hosted.
2. Content stores	Where terrorist content is stored, including text and audio files, as well as images and videos. These are used as online libraries of content. Terrorists and violent extremists rely on content storage platforms and pasting sites, as well as archive services.
3. Aggregators	Aggregators act as centralized databases of where content can be found online, gathering together a wide range of URLs to content hosting platforms to facilitate diffusion. If one link is taken down, terrorists can easily find an alternative to share.
4. Circumventors	Online services and platforms used to circumvent content moderation and de-platforming measures. Circumventors include VPNs, which can enable nefarious actors to access content that has been blocked in specific countries. Another example of circumventors is the use of decentralized web technologies, which avoid website takedowns.

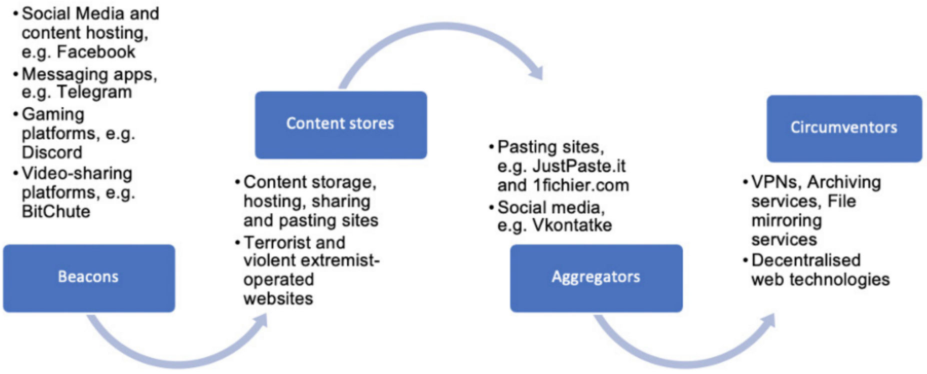

• Social Media and content hosting, e.g. Facebook
• Messaging apps, e.g. Telegram
• Gaming platforms, e.g. Discord
• Video-sharing platforms, e.g. BitChute
Beacons
Content stores
• Content storage, hosting, sharing and pasting sites
• Terrorist and violent extremist-operated websites
• Pasting sites, e.g. JustPaste.it and 1fichier.com
• Social media, e.g. Vkontatke
Aggregators
Circumventors
• VPNs, Archiving services, File mirroring services
• Decentralised web technologies

Figure 1 - Typology of platforms used by terrorists (by technology types and practical uses)
Source : GIFCT - Tech Against Terrorism (2021), *op. cit.*, pp.15-16.

[84] *Ibid.*, p.15.
[85] *Ibid.*, p.33.

A lasting reliance on virtual dead drops platforms. A physical “dead drop” is a technique used in espionage to “*secretly pass information items using a clandestine location for interim storage[86]*”. In recent years, terrorists, and especially jihadist groups, have transformed the later physical dead drops into virtual ones, using to do so anonymous sharing portals[87] and cloud services*[88]*. Least sophisticated ways of virtual ‘dead dropping’ are known since more than ten years with, for instance, the use of online email-account to write draft and unsent messages, accessible anywhere by anyone having the relevant password[89]. Regarding anonymous sharing portals, much ink has been spilled about *Telegra.ph* (developed by the well-known instant messaging app *Telegram*) and *JustPaste.It*: alongside other platforms such as *Sendvid.com* and *Dump.to*, they have become “*some of the most-used sites by ISIS and other terrorist and extremist groups*[90]”, *JustPaste.It* being described as soon as 2014 as an “*ISIS propaganda tool[91]*”. The case of *JustPaste.It* is particularly interesting, in a TCO perspective, as we have a micro HSP, an independent platform owned and operated by a single man, whose free service has been widely used for terrorist purposes, in spite of himself and efforts to collaborate with LEAs and curb the phenomenon. Regarding cloud-sharing services, we can cite the following websites : *files.fm*, *Pixeldrain*, *Mediafire*, *OneDrive*, *CloudShare*, *Nextcloud*, *Cloudflare*, *Yandex.Disk*, *Mixdrop*, *4shared*, *Cloudmail*, *Top4top*, *pCloud*, *UsersDrive*, and *Dropapk[92]*. Thus small HSPs offering these types of services are particularly at risk of being affected by terrorist content.

A rise of decentralised web and platforms. Another major trend is the growing exploitation of the decentralised web and platforms by terrorists and extremists[93]. The decentralised web, also known as ‘Dweb’, works in the same way as the web we use everyday, but does not rely on centralised operators, “*the big Internet gatekeepers like Google and Facebook*” : 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[94]*”. We can trace this growing exploitation of the Dweb and decentralised platforms back to 2018 and 2019, where coordinated action from Telegram and Europol led to major purges of accounts on the app and forced ISIS and terrorist groups to search for alternatives[95][96][97], namely *Rocket.Chat*, *ZeroNet* and *Riot*. The decentralised platforms like *Rocket.Chat* and *ZeroNet* 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 servers or dispersed across*

[86] Weimann, G. and Vellante, A. (2021), *op.cit*., p.39-40

[87] Weimann, G. and Vellante, A. (2021), *op.cit*., p.40 : “*online sites that are openly available, have no login requirement and thus provide anonymity and allow for sharing links of which content is to be collected, shared and mass distributed*”.

[88] Weimann, G. and Vellante, A. (2021), *op.cit*., p.46.

[89] United Nations Office on Drugs and Crime (2012), *op. cit.*, p.10.

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

[91] “How a Polish student’s website became an Isis propaganda tool”, The Guardian, 15 August 2012 URL: https://www.theguardian.com/world/2014/aug/15/-sp-polish-man-website-isis-propaganda-tool

[92] Weimann, G. and Vellante, A. (2021), *op.cit*., p.46.

[93] Bodo, L. and Trauthig, I. K. (2022), “Emergent Technologies and Extremists: The DWeb as a New Internet Reality?”, Global Network on Extremism and Technology, 2022. URL : https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf

[94] King, P. (2019), “Islamic State group’s experiments with the decentralised web”. Europol, ECTC Advisory Network Conference, p.4. URL: https://www.europol.europa.eu/sites/default/files/documents/islamic_state_group_experiments_with_the_decentralised_web_-_p.king_.pdf

[95] “Referral Action Day against Islamic State online terrorist propaganda”, Europol, 22 November 2019. URL: https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda

[96] “Europol disrupts Islamic State propaganda machine”, BBC, 25 November 2019. URL : https://www.bbc.com/news/world-middle-east-50545816

[97] King, P. (2019), *op. cit.*

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*[98]". Despite collaboration with authorities from platforms like *Rocket.Chat*, the removal of terrorist servers is impossible : "*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*[99]". As stated by TaT in 2019 in a study dedicated to ISIS use of smaller platforms and the Dweb, "*[i]f implemented successfully and accepted by the wider pro-ISIS audience, it will become difficult – if not impossible – to tackle ISIS presence on these decentralised services [...] because these services are independent from any intermediary or 'middle man' for receiving and sending messages*[100]". Since, other decentralised platforms have attracted the attention of LEAs, practitioners and researchers, for instance *Mastodon*[101] and *Odysee*[102].

Seeking (smaller) platforms with weak content moderation. Another commontrend for terrorists is to seek platforms with weak content moderation, which induces a greater likelihood of content persistence. The origins of such an insufficient content moderation can be diverse (e.g. available capacities, internal policies, recent market entry, etc.) but smaller platforms are more likely to be concerned. Available figures reflect the higher exposure of micro, small and unregistered hosting service providers within the European Union : "*[w]hilst the percentage of referrals sent to micro, small and unregistered companies only amounted to 7% in 2015 (when the EU IRU was first set up), they amount to 68% today [i.e. 2018]*[103]". Apart from the size of the platform itself, the weakness of the content moderation may also result from the type of services it is actually offering. For instance, a greater reliance on platforms offering audio-sharing services (e.g. *Clubhouse* or *Spotify*) by extremists and terrorists has been witnessed in recent years "*due to their insufficient content moderation guidelines, personnel and tools*[104]". The policies led by LEAs and public authorities regarding the fight against terrorist content online also creates a 'push-and-pull effect' that may lead individuals and groups to turn themselves towards 'old' or formerly-used platforms or techniques: "*[s]imilarly to websites, an increasing reliance on resurfaced 'old' technology, such as email newsletter services (e.g., Substack), by extremists and terrorists due, again, to these services relative inattention to content moderation*[105]". In the same vein, recent years witnessed the resurgence of TOWs, which is "*likely a side-effect of broad improvements in social media platforms' content moderation efforts*[106]" : for instance, between January 2021 and January 2022, TaT identified no less than 198 T/VEOWs (Terrosist and Violent Extremist Operated Websites)[107].

[98] King, P. (2019), *op. cit.*, p.4.

[99] "Rocket.Chat Announces Internal Task Force to Prevent Future Platform Use by Terrorist Groups", Rocket Chat, 26 March 2021. URL : https://www.rocket.chat/press-releases/rocket-chat-announces-internal-task-force-to-prevent-future-platform-use-by-terrorist-groups

[100] Tech against Terrorism (2019), "Analysis : ISIS use of smaller platforms and the Dweb to share terrorist content", April 2019. URL : https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/

[101] Mastodon is free and open-source software for running self-hosted social networking services, with microblogging features similar to Twitter.

[102] Odyssey is a video hosting platform based on the LBRY protocol, decentralised through peer-to-peer broadcasting : created by a libertarian, the Youtube-like platform has become a QAnon, conspiracy theorists and violent extremists favourite.

[103] European Commission (2018), *op. cit.*, p.6.

[104] Radicalisation Awareness Network Policy Support (2021), *op. cit.*, p.46.

[105] *Ibidem.*

[106] Tech Against Terrorism (2021),"Trends in Terrorist and Violent Extremist Use of the Internet l Q1-Q2 2021", July 2021, p.5. URL : https://www.techagainstterrorism.org/2021/07/30/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/

[107] Tech Against Terrorism (2022), "The Threat of Terrorist and Violent Extremist Operated Websites", January 2022, p.3. URL : https://www.techagainstterrorism.org/wp-content/uploads/2022/02/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022.pdf

To conclude on the current trends of terrorism online, the *Radicalisation Awareness Network* (RAN), in a 2021 report dedicated to violent extremism and terrorism online, identified 12 issues or phenomena to watch in 2022, that we reproduced below[108]. It completes the overview focused on platforms we have given in this part.

Online Extremism and Terrorism: What to Watch for in 2022[109]

- Continued extreme right exploitation of COVID-19, including online to offline trajectories;
- Increasing online and 'real world' ideological and aesthetic crossover, both between ideological 'sets' (e.g., incels-extreme right, QAnon-extreme right, ecology-extreme right) and across ideologies (e.g., far-right-Salafis);
- Continued targeting of women (e.g., QAnon via beauty and wellness online influencers and communities) and youth (e.g., via gaming and adjacent platforms);
- More reliance on audio (e.g., Clubhouse, Spotify, Twitter) by extremists and terrorists due to their insufficient content moderation guidelines, personnel, and tools;
- Similarly to websites, an increasing reliance on resurfaced 'old' technology, such as email newsletter services (e.g., Substack), by extremists and terrorists due, again, to these services relative inattention to content moderation;
- The emergence of new online platforms and services attractive to extremists and terrorists but with no strategies in place to deal with these—and other—harms;
- Increasing exploitation of the federated or decentralised web (i.e., the 'Dweb');
- Continued financial profiting by, especially, extreme right influencers from their online activity;
- Increasing reliance on, especially privacy-preserving, cryptocurrency and other online payment mechanisms for fundraising, donations, and payments;
- The implementation of relevant new legislation, especially the EU's TCO Regulation;
- The progress of relevant measures already-in-train through the legislative process, especially the EU's Digital Services Act (DSA);
- The tabling of relevant new regulatory measures globally, including outside of the Western democratic sphere (e.g., India)

2.5 Assessing the exposure of smaller platforms

As we have seen, virtually "*all platforms that enable the sharing of user-generated conten*t", for communication or content-sharing purposes, are at risk to find themselves used one day by terrorist individuals or groups - this includes but "*is not limited to file sharing, file storage, social media, archiving, link-shortening, content-pasting, email, messaging, video sharing, and blogging platforms*[110]". With weak content moderation, due to available capacities (technological, financial or human) and/or internal policies (Dweb and alt-tech platforms notably), we can assume that the likelihood to be affected by terrorist content significantly increases. Smaller platforms 'ticking all the boxes', and usually characterised by lesser capacities and capabilities, thus "*have a significantly greater need for support*[111]". Indeed, there is an obvious asymmetry of resources between the Internet giants (Big Tech companies and other large-scale online platforms) and the Small and

[108] Radicalisation Awareness Network Policy Support (2021), *op. cit.*, p.46.

[109] *Ibidem.*

[110] GIFCT - Tech Against Terrorism (2021), *op. cit.*, p.6.

[111] *Ibid.*, p.20.

Medium Enterprises (SME) providing hosting services and/or offering the possibility for users to generate content (so to say micro, small and medium HSPs). Based on these premises, we can argue that such SMEs are likely more at risk for becoming a hub for the dissemination of terrorist propaganda, as pointed out by the European Commission in 2018 during the preparatory works of the TCO Regulation : "*SMEs offering hosting services are particularly vulnerable to exploitation for illegal activities, not at least since they tend to have limited capacity to deploy state-of-the-art content moderation tools or specalised*[112]". But can we confirm these premises and assess precisely the exposure to terrorist content of these smaller European platforms ?

To do so, we first need to have a look at the European HSPs' ecosystem. Once again, giving a precise estimation of the number of active HSPs in Europe is a wager. In 2018, the European Commission gave the following figures, which can not be taken for granted as they relied on the *Dealroom* database : 10,500 HSPs established in Europe, of which 9,700 SMEs, and 20,000 established both in Europe and in the US and Canada[113]. A quick research on *Crunchbase*, using 'EU' for headquarters location and 'Internet services' for industry, gives 26,225 results as of May 2023, a figure that should not be taken for granted either (all of these companies are not hosting service providers and some are not active anymore). In the absence of more robust data, we can only assume that several thousands of companies can be qualified as European HSPs and may be affected by terrorist content, while falling under TCO scope. Theses European HSPs offer a wide range of services, and the ones in the scope of TCO can be divided into three main categories[114]:

1. Online storage and distribution (i.e "*services allowing their users to store content online*[115]") : web hosting (e.g. *Leaseweb*, *WIX.com*, *Vautron Rechenzentrum AG*, etc.), online media sharing platforms (e.g. *Youtube*, *Vimeo*, *Photobucket*, *Soundcloud*, *Bandcamp*, *Medium*, *Wordpress*, etc.), file storage and sharing (e.g. *Dropbox*, *box.com*, *WeTransfer*, etc.) and IaaS/Paas (e.g. *AWS*, *Google Cloud*, *Microsoft Azure*, etc.).

2. Networking, collaborative production and matchmaking (i.e. "*the central function of the platform is not (merely) to store content online, even though this always remains a part of the service, but to connect producers and users around more complex sets of networked interactions, such as an online debate and discussions, market transactions or the collaborative production of documents and other media*[116]"): social networking and discussion forums (e.g. *Facebook*, *Linkedin*, *Twitter*, etc.), collaborative production (e.g. *Wikipedia*, *Google Docs, Office*, etc.), online marketplaces (e.g. *eBay*, *Marktplaats*, *eBid*, *Craigslist*, etc.), collaborative economy (e.g. *Lyft*, *BlaBlaCar*, *Twizzi*, *Airbnb*, *Homestay*, *Kickstarter*, etc.), and online games (e.g. *Xbox Live*, *World of Warcraft*, etc.).

[112] European Commission (2018), *op. cit.*, p.6.

[113] *Ibidem.*

[114] European Commission (2019), Directorate-General for Communications Networks, Content and Technology, Hoboken, J., Quintais, J., Poort, J., et al., *Hosting intermediary services and illegal content online : an analysis of the scope of article 14 ECD in light of developments in the online service landscape : final report*, Publications Office, 2019, pp.12-14. URL : https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content

[115] European Commission (2019), *op. cit.*, p.12.

[116] *Ibidem*.

3. Selection and referencing (i.e. "*intermediaries that help provide further value, organisation and structure to available offerings online*[117]"): for example rating and reviews (e.g. *Yelp*).

As stated in the European Commission *2018 Impact Assessment* relating to TCO Regulation preparatory works, two major problems can be identified regarding the HSPs exposure to terrorist content online: "(1) *hosting services providers are abused for the dissemination of terrorist content online, affecting the business models and users' trust in the digital single market* ; (2) *terrorist content is accessible online, reappears, and spreads across service providers posing security challenge"*[118]. Indeed, because of the 'offline impact' we have discussed in the previous section, the dissemination of illegal and terrorist content online is a major concern for all European stakeholders (i.e. users, citizens, companies, public authorities…). For instance, 61% of the respondents to the *Flash Eurobarometer 469 on illegal content (2018)*[119] claimed "*to have seen online some type of illegal content*", while "*6% […]claimed to have seen terrorist content online"*, with a higher reported exposure for younger people aged 15-24 (11%)[120]. Furthermore, 65% of the respondents labelled the Internet as "*not safe*" for its users, 90% agreed that measures should be implemented to limit the spread of illegal content online and only 44% considered HSPs effective in tackling illegal content[121]. The dissemination of terrorist content online also jeopardises HSPs private interests, creating "*reputational damage on companies*[122]" which can affect business models, relations with users and advertisers and ultimately global turnovers and companies' viability. To give an example, *Youtube* underwent a massive backlash in 2017 after companies found their advertisements associated with terrorist or extremist videos[123].

Based on the formulation of these two problems and our subsequent findings, we can argue further : first, that smaller platforms are indeed exposed to terrorist content and that this exposure is uneven based on the type of services offered (1) ; second, that the availability and the ubiquity are two main issues regarding the spread of terrorist content via (smaller) HSPs (2).

(1) Smaller platforms are exposed, but this exposure is uneven based on services offered

Recent data tend to show that smaller platforms / HSPs are increasingly targeted by terrorist groups and individuals to communicate and share content. In 2019, "*[a]nalysis of more than 45,000 URLs [by TaT] since 2014 across more than 330 platforms show that smaller platforms are heavily targeted by ISIS and that 49% of all URLs were found on just eight of these platforms*[124]", thus also confirming the existence of 'trendy' platforms and overarching trends. As a result of *Telegram*'s purges in 2018 and 2019, ISIS / Daesh started a major "*experimentation with small media*

[117] *Ibidem*.

[118] European Commission (2018), *op. cit.*, pp.6-8.

[119] "Flash Eurobarometer on illegal content", European Commission, 12 September 2018. URL: https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content

[120] European Commission (2018), *op. cit.*, p.7.

[121] "Flash Eurobarometer on illegal content", European Commission, 12 September 2018. URL: https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content

[122] European Commission (2018), *op. cit.*, p.6.

[123] "Google's bad week : Youtube loses millions as advertising row reaches US", *The Guardian*, 25 March 2017. URL : https://www.theguardian.com/technology/2017/mar/25/google-youtube-advertising-extremist-content-att-verizon

[124] Tech against Terrorism (2019), "Analysis : ISIS use of smaller platforms and the Dweb to share terrorist content", April 2019. URL : https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/

platform[s][125]", such as *Koonekti* for instance, and also mobilised Dweb-related tools and platforms. This was not the first occurrence of reliance on medium - small - micro platforms by ISIS : "*[w]hen looking at past attempts, a pattern emerges, namely the use of small-to medium-sized apps, platforms and services*" such as "*Baaz, Viber, Kik, Ask.fm, Discord and others, including micro-platforms run by a single individual*[126]" (e.g. *JustPaste.It*). Accounts from 2021 and 2022 also confirm these findings. In 2021, TaT through GIFCT showed that "*while terrorist use of the internet is still prevalent on smaller platforms, in general the absolute volume of content is low*", stressing that "*[a]nalysis of TCAP URL alerts since November 2020 shows that more than 80% of all content discovered on all smaller platforms (100+ platforms) is shared on the top 20% of these platforms (22 out of 115)*[127]". Even more recently, the Transparency Report of the TCAP also assessed that "*terrorist and violent extremist use of the internet is increasingly concentrated on smaller platforms, who struggle to action extremist content due to limitations of capacity, capability, and subject matter knowledge*[128]".

Furthermore, regarding the type of services offered by these platforms, some seem more likely to be affected than others, as already evoked in previous parts. On a set of 150 companies identified by Europol as hosting terrorist content between 2017 and 2018[129]: over 50% offered file storage and sharing services, most of which being SMEs with a limited audience ("*median of 20 000 views per month, with a first quartile including below 1000 views*[130]") ; around 20% were online media sharing services, "*half of which have a limited audience in Europe (average number of monthly views below 25 000)*[131]" ; just under 10% offered web hosting services or were networking and discussion forums, half of the latter category having less than 150,000 views.

As shown by this sample, and also by findings from the literature[132], some types of services are more likely to be exploited by terrorists (e.g. file storage and sharing services, online media sharing services, networking and discussion forums). Findings extracted from the 2022 Transparency Report of the TCAP, based on the 18,957 URLs containing terrorist content submitted on the platform by OSINT analysts and automated scrapers between December 2020 and November 2021, also tend to confirm this uneven exposure of platforms depending on the type of services offered : on the 18,957 alerts, 78% concerned platforms offering file sharing services, 12% archiving services, 5% link shortener services, the other ones accounting for very small numbers[133]. We can also assume that, depending on the type of audience they wish to target, terrorists thus face a common dilemma : using large-scale platforms with large audiences, but with clear preparedness, high monitoring and moderation capabilities (e.g. AI tools, large moderation and specialised investigation teams) and extensive awareness of both regulations in force and trends in illegal content spreading ; investing in smaller HSPs, with limited audiences, but with weaker preparedness, moderation and

[125] *Ibidem.*
[126] *Ibidem.*
[127] GIFCT - Tech Against Terrorism (2021), *op. cit.*, p.9.
[128] Tech against Terrorism (2022), *op. cit.*, p.21.
[129] European Commission (2018), *op. cit.*, pp.6-7.
[130] *Ibid.*, p.6.
[131] *Ibidem*.
[132] See : Weimann, G. and Vellante, A. (2021), *op.cit*. ; Radicalisation Awareness Network Policy Support (2021), *op. cit. ;* King, P. (2019), *op. cit.* ; etc.
[133] Tech against Terrorism (2022), *op. cit*., p.13.

awareness. The dilemma is therefore a choice between, on the one hand, a large audience but an increased likelihood of suppression or investigation, and, on the other, a more limited audience but increased discretion and risk limitation. For more information on the attractive features of given platforms, see Appendix 5.2.

(2) Two major issues with terrorist content shared via HSPs are availability and ubiquity

As it has been shown throughout this report, giving precise and/or exhaustive figures on the extent of terrorism and violent extremism online is a wager, maybe impossible. Nevertheless, one thing remains certain : terrorist content is available online, on the clear web, on European platforms or for European users. Quick research done by the FRISCO team showed that, for instance, getting hold of the terrorist magazines mentioned in part 2.3 only took an Internet connection and a few seconds. Reminding the aforementioned TCAP's results, almost 19,000 URLs were identified by TaT's OSINT analysts and automated scrappers as containing terrorist content in a very short period of 12 months. Likewise, between July 2015 and September 2018, Europol's Internet Referral Unit (EU IRU) *"has made over 50,000 decisions for referrals to service providers about terrorist content in their platforms"* while the *"UK's Internet Referral Unit [...] identified 300,000 pieces of terrorist content between 2010 and 2019*[134]*"*. Thus, all the figures given throughout the report, even incomplete, tend to show the availability of terrorist content online. A related problem is the ubiquity of terrorist content online, as materials tend to spread quickly and to reappear on different platforms - this was confirmed during our discussions with LEAs, stating that they were sometimes confronted with the same piece of content dozens of times. For instance, platforms used as 'aggregators', so to say as centralised databases, usually redirect the individuals to several other platforms where the same content is displayed to avoid total deletion. To conclude on this issue, regarding the overall number of platforms exposed to terrorist content, it has been estimated that *"at any one point there are 250-500 platforms used by designated terrorist organisations to disseminate content*[135]*"*.

2.6 Stressing the measures imposed by the TCO Regulation

According to the *European Commission 2018 Impact Assessment*, four drivers were associated with the two problems aforementioned: *"hosting service providers face legal fragmentation and uncertainty* (1) ; *Member States face obstacles in intervening against terrorist content online* (2) ; *measures to detect, remove and prevent the dissemination of terrorist content are not effectively or evenly implemented by hosting services* (3) ; *hosting services providers' policies to detect, assess and remove content are not transparent for users and public authorities to monitor companies' action against terrorist content* (4)[136]*"*. The intervention logic behind the TCO Regulation implementation and subsequent measures thus aims at curbing both problems and their drivers, as shown below.

[134] European Commission (2018), *op. cit.*, p.7.

[135] GIFCT - Tech Against Terrorism (2021), *op. cit.*, pp.6-7.

[136] European Commission (2018), *op. cit*., pp.9-16.

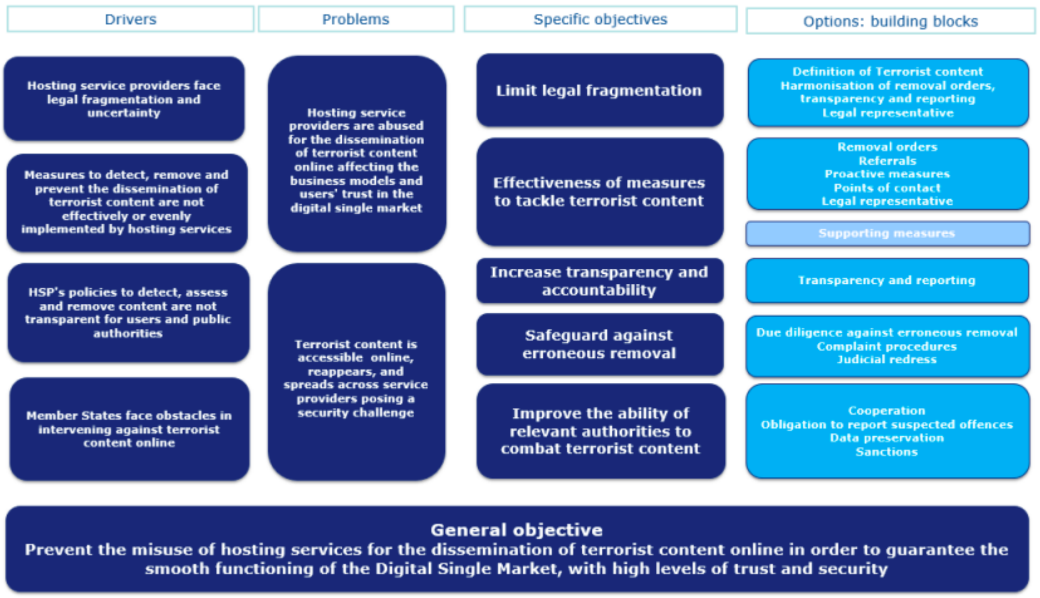

Drivers
Problems
Specific objectives
Options: building blocks
Hosting service providers face legal fragmentation and uncertainty
Measures to detect, remove and prevent the dissemination of terrorist content are not effectively or evenly implemented by hosting services
HSP's policies to detect, assess and remove content are not transparent for users and public authorities
Member States face obstacles in intervening against terrorist content online
Hosting service providers are abused for the dissemination of terrorist content online affecting the business models and users' trust in the digital single market
Terrorist content is accessible online, reappears, and spreads across service providers posing a security challenge
Limit legal fragmentation
Effectiveness of measures to tackle terrorist content
Increase transparency and accountability
Safeguard against erroneous removal
Improve the ability of relevant authorities to combat terrorist content
Definition of Terrorist content
Harmonisation of removal orders, transparency and reporting
Legal representative
Removal orders
Referrals
Proactive measures
Points of contact
Legal representative
Supporting measures
Transparency and reporting
Due diligence against erroneous removal
Complaint procedures
Judicial redress
Cooperation
Obligation to report suspected offences
Data preservation
Sanctions
General objective
Prevent the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the Digital Single Market, with high levels of trust and security

Figure 3 *Intervention logic. Building blocks summarise the types of actions, but the three options and related options include variations in the design and scope of the actions.*

Figure 2 - Intervention logic behind the TCO Regulation (2018)

Source : European Commission (2018), *op. cit.*, p.27

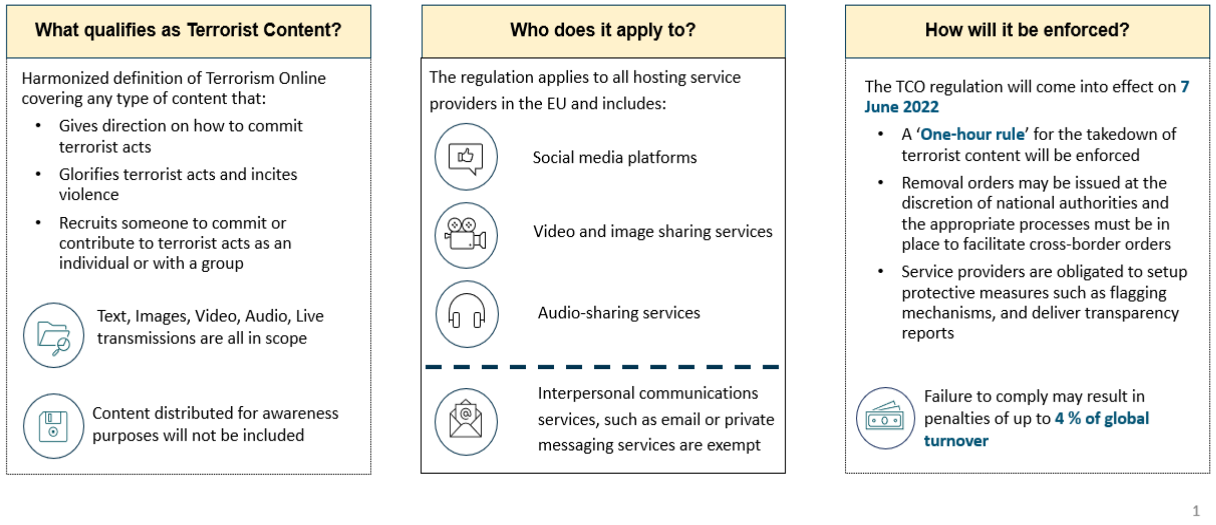
The most recent legal and technical initiatives driven by the European Union with regard to the moderation of terrorist content (i.e. the creation of the EU IRU in 2015 within Europol and the recent entry into force of the TCO Regulation) have thus participated in the launching and strengthening of a phenomenon, described by scholars as the "*public-private co-production of European security*" (i.e. "*a governance model whereby companies come to play essential role in European security*[137]"). Indeed, "*the EU seeks to play an active role in steering and influencing private practices and decisions on content removal*" as "*[c]ontent moderation never happens in a legal vacuum and evolves through confrontation and cooperation between private companies and public authorities in an international context*[138]". The 2019 Christchurch mosque shootings and the subsequent *Christchurch Call* have worked as a "*defining global moment in committing public actors and tech companies to 'eliminate terrorist and violent extremist content online', and set in motion a plethora of initiatives*[139]". In this context, the European Union has proven to be particularly proactive in recent years. What is important to recall is that the moderation of terrorist content online can not happen without the cooperation and proactiveness of private actors such as Big Tech companies and smaller hosting service providers. Curbing the phenomenon thus requires a mix of legal/regulatory obligations (such as the TCO Regulation) and non-legally binding ones (such as

[137] Bellanova, R. and de Goede, M. (2022), "Co-producing security : platform content moderation and European security integration". *Journal of Common Market Studies*, Vol. 60, Issue 5, pp. 1317-1318. URL : https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.13306

[138] *Ibid.*, pp. 1316-1317.

[139] *Ibid.*, p.1317.

public-private partnerships for instance), completed by various initiatives and activities (e.g. multifaceted cooperation, voluntary and targeted approaches, innovations and technological developments, knowledge production, awareness raising, civil society involvement, P/CVE efforts, etc.). Before presenting the findings of our studies in detail, you will find below a summary of the TCO Regulation's measures and scope.



What qualifies as Terrorist Content?

Harmonized definition of Terrorism Online covering any type of content that:

- Gives direction on how to commit terrorist acts
- Glorifies terrorist acts and incites violence
- Recruits someone to commit or contribute to terrorist acts as an individual or with a group

Text, Images, Video, Audio, Live transmissions are all in scope

Content distributed for awareness purposes will not be included

Who does it apply to?

The regulation applies to all hosting service providers in the EU and includes:

Social media platforms

Video and image sharing services

Audio-sharing services

Interpersonal communications services, such as email or private messaging services are exempt

How will it be enforced?

The TCO regulation will come into effect on **7 June 2022**

- A '**One-hour rule**' for the takedown of terrorist content will be enforced
- Removal orders may be issued at the discretion of national authorities and the appropriate processes must be in place to facilitate cross-border orders
- Service providers are obligated to setup protective measures such as flagging mechanisms, and deliver transparency reports

Failure to comply may result in penalties of up to **4 % of global turnover**

1

Figure 3 - Terrorist Content Online (TCO) Regulation Overview

The TCO Regulation was passed by the EU to protect the Internet from terrorists who abuse it to spread their message, radicalise or recruit followers.

3. Findings

3.1 Key takeaways from our investigations

Our investigation, consisting of conducting interviews and an online survey, revealed some clear development around the situation of HSPs in the European space. *In total, our team has gathered the feedback of 48 European HSPs, 33 answers through our online survey and 15 through interviews*. Our online survey has been sent: directly to more than 2000 HSPs ; indirectly through LEAs and associations of HSPs to more than 4000 HSPs. Also, in an additional *series of 21 interviews*, we spoke with representatives from various LEAs, responsible authorities, experts, and members of the European Commission and Europol.

The interviews and survey aimed to better understand the level of general awareness among HSPs about the TCO and their obligations, their preparedness to detect and deal with terrorist content on their platforms, technical and human capabilities to comply with the Regulation, as well as the main gaps, obstacles and needs for compliance.

3.2 Hosting service providers

According to the online survey outputs, the majority of HSPs who responded had less than 100,000 users (84.9%), thus providing us with an accurate pool of information on the state of play especially in relation to micro and small HSPs[140], which is the target group of the current study.

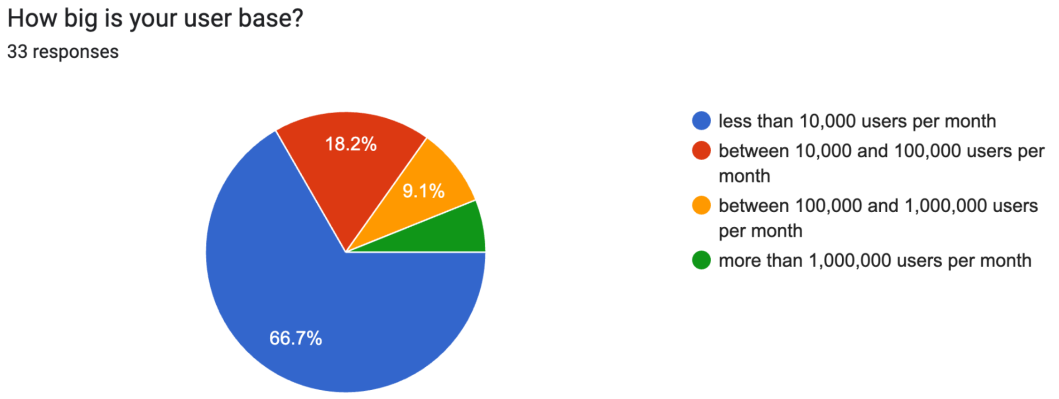


Figure 4 - Q1/ User base size

[140] Although the definition of micro and small HSPs is not defined by the number of users, we make the assumption that HSPs with less than 10,000 users will enter into this category.

These HSPs were engaged in a wide range of activities, thus giving an interesting sample of barriers and challenges. Based on the topology used in section 2.5, we have received feedback from HSPs belonging to all three categories: online storage and distribution ; networking, collaborative production and matchmaking ; selection and referencing. The HSPs that have participated in our survey *were mainly hosting long-form text-based content such as blogs (36,4%) and multimedia content (21,2%).*

Awareness about the TCO Regulation. *Most HSPs that have responded to the online survey do not moderate user-generated content (57,6%) or do so only partially (21,2%).* This lack of content moderation might also be explained by a little level of awareness regarding relevant regulations and its implications, in particular of the TCO Regulation.

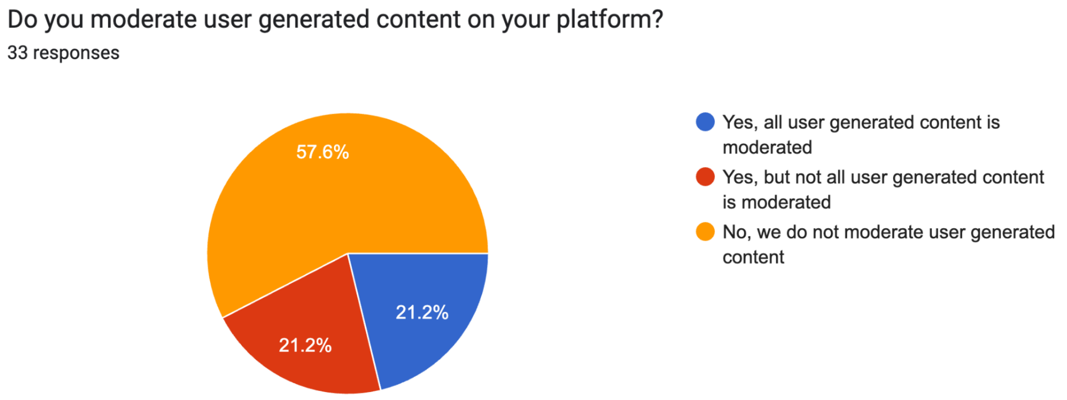


Figure 5 - Q2/ Moderation of user-generated content

Furthermore, 42,4% were not aware at all of the TCO Regulation and the remaining 48,5% were only partially aware of what the regulation entails, with only 9,1% considering having an awareness of 4 on a scale of 1=Not aware to 5=Highly Aware. Thus, micro and small HSPs tend to have a very limited knowledge of the TCO Regulation and its implications. Furthermore, there seems to be a significant difference in the level of information concerning the TCO Regulation and level of preparedness to implement it in function of the size of the HSPs – this is a clear take-away from our interviews with different HSPs.

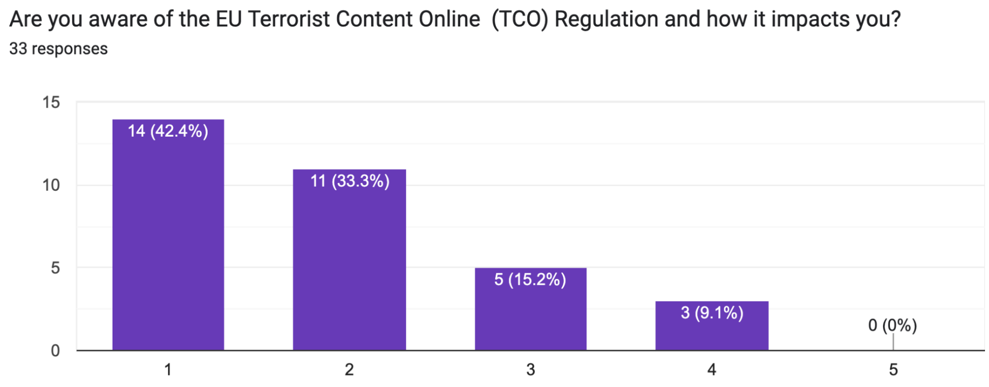


Figure 6 - Q3/ Awareness regarding the TCO Regulation

To give elements of comparison concerning awareness in relation to the TCO Regulation and the Digital Services Act (DSA), HSPs are clearly more aware of the DSA. However this still means that *33,3% were not aware at all of the DSA, 57,6% were partially aware and 9,1% were highly aware, reaching 5 on a scale ranging from 1=Not Aware to 5=Highly Aware*.

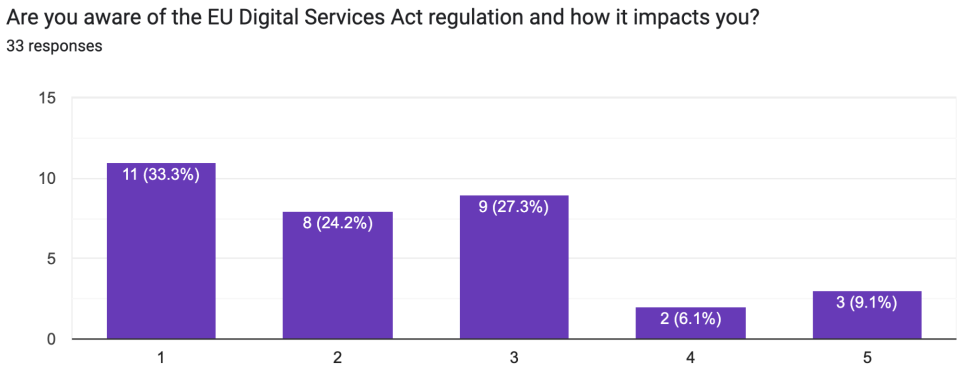


Figure 7 - Q4/ Awareness regarding the DSA

Understanding the scope of terrorist content. Defining ‘terrorist’ content is a challenge for most HSPs, as well as other actors, not to mention the fact that not everyone relies on the same definition or has the same biases regarding domestic situations. Moreover, fully-fledged terrorist content finds itself in a sea of other illegal and violent content (e.g. hate speech, CSAM, scams, bots, cult recruiting…), which, for some of them, tend to be more prevalent and attract more attention from online platforms and LEAs.

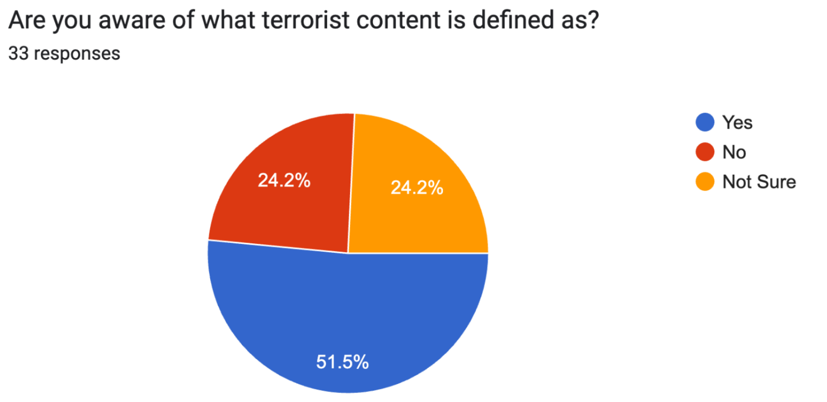


Figure 8 - Q5/ Definition of terrorist content

Only 51,5% of the respondents to the online survey could define terrorist content without hesitation and almost none of the interviewees within the scope could do so.

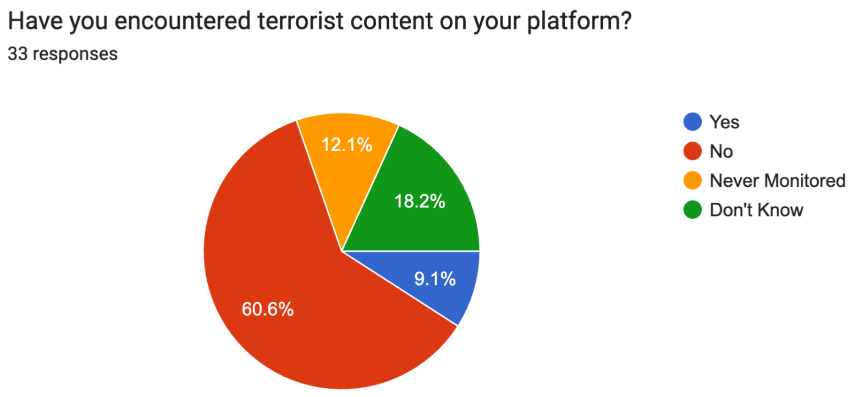


Figure 9 - Q6/ Exposure to terrorist content

Among the respondents to the online survey, *60,6% said they had never encountered terrorist content on their platforms, 18,2% said they did not know whether they have encountered it, 12,1% admitted to have never monitored and only 9,1% said they have been exposed to such content.*

Perception about exposure to terrorist content. The later point is linked to a pivotal issue, the potential asymmetry between the actual and the perceived threat. Indeed, despite the lack of awareness and preparedness, *most HSPs (72,7%) perceive themselves as at low risk for terrorist content - on a scale ranging from 1=Very Unlikely to 5=Very Likely, 51,5% considered themselves to be at the lowest risk of exposure.*

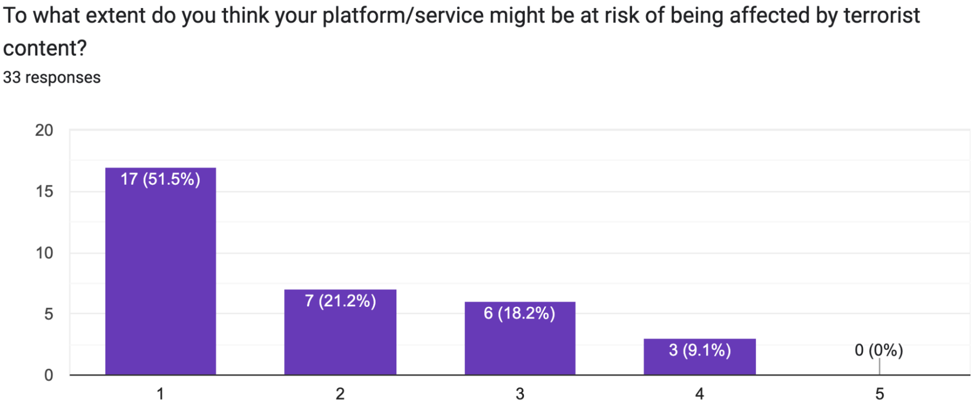
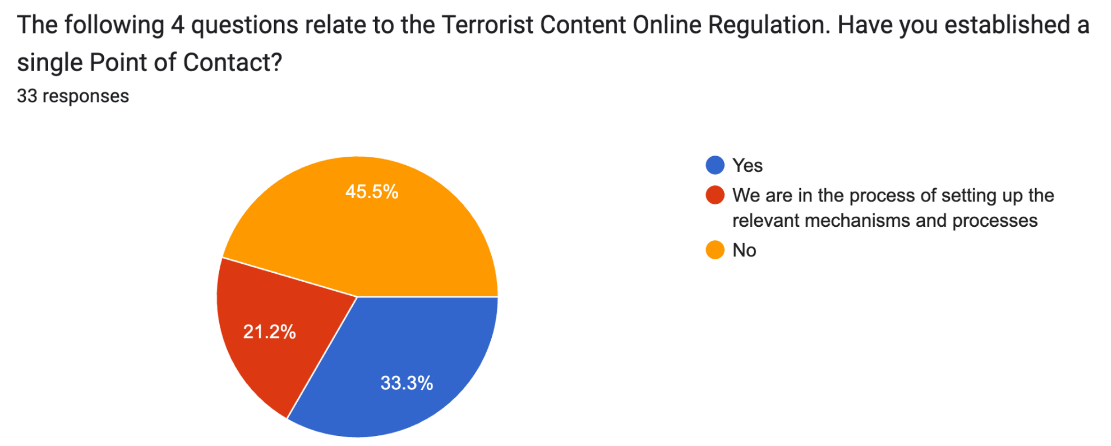


Figure 10 - Q7/ Perceived risk of being affected by terrorist content

Thus, most of them, if they did not experience terrorist content and do not have tools and processes in place such as for instance content moderation, will *probably take ad hoc measures if such content appears on their platforms*. Furthermore, some stakeholders interviewed (such as a legal representative) raised concerns that measures will be put in place only in a reactive manner once the first removal orders - or only after the first sanctions for non-compliance - are issued by respective authorities which might take years from now, based on experience with previous legislation such as the GDPR. This is further amplified by the concern that preventive measures and developing capacities to deal with TCO is not worth the investment for small HSPs that have limited human and technical resources.

This may indicate a disconnection between perceived and actual risks, highlighting the need for better education and support. Beyond perceptions, capabilities should also be challenged for smaller platforms, so to say human, technical and financial resources. For instance, small and medium-size HSPs face challenges in hiring legal representatives due to limited resources. This issue is exacerbated by additional obligations related to e-commerce regulations and the DSA. Additionally, not having the appropriate detection systems in place may further blind the platforms to the extent of any problem.

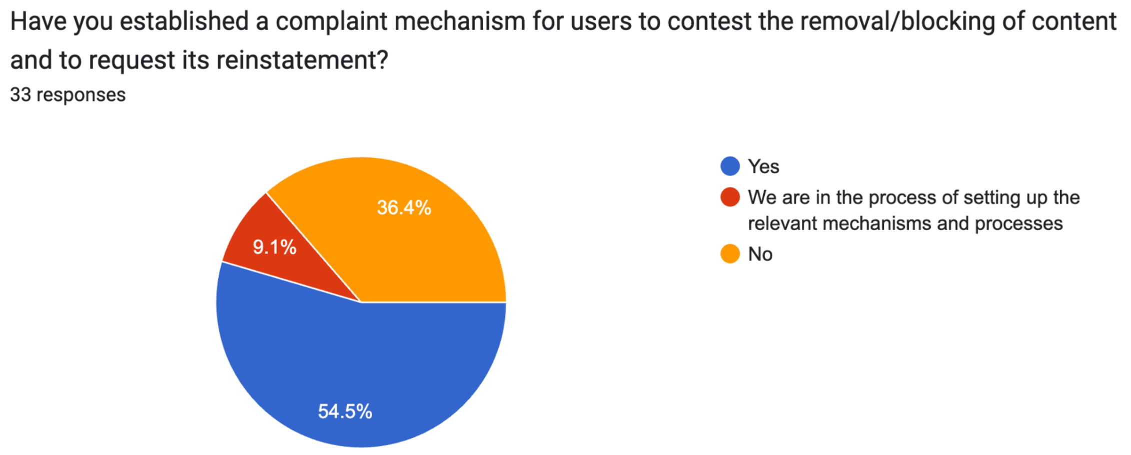
Processes and tools in place. *The vast majority of HSPs that had responded to the online survey did not have automated measures for identifying, monitoring, and removing content (69,7%), lines of communication with LEAs in place (69,7%) or transparency measures (57,6%)*. Slightly better progress has been made by platforms with the *setting up of points of contact* (33,3% of respondents have already done so, with 21,1% in the process of setting them up) and *implementation of user complaint mechanisms* (54,5% of respondents have already done so, with 9.1% in the process of doing so), however, progress is still lacking. Interestingly, the HSPs interviewed tended to have a higher rate of processes and tools in place mainly because of their own business needs and Terms of Services, still doing the content moderation manually using some simple tools.



The following 4 questions relate to the Terrorist Content Online Regulation. Have you established a single Point of Contact?

33 responses

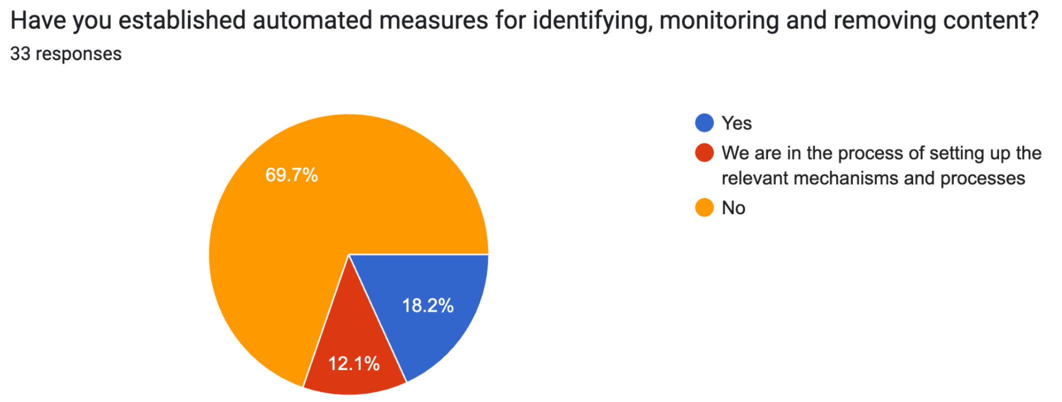
Figure 11 - Q8 / Implementation of a single Point of Contact



Have you established a complaint mechanism for users to contest the removal/blocking of content and to request its reinstatement?

33 responses

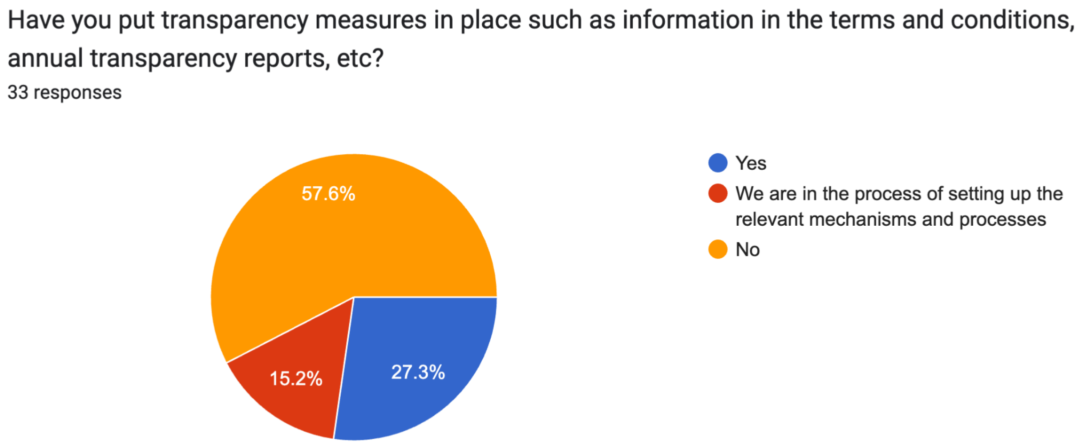
Figure 12 - Q9/ Implementation of a complaint mechanism



Have you established automated measures for identifying, monitoring and removing content?

33 responses

Figure 13 - Q10/ Implementation of automated measures



Have you put transparency measures in place such as information in the terms and conditions, annual transparency reports, etc?

33 responses

Figure 14 - Q11/ Implementation of transparency measures

3.3 Law enforcement agencies National & Competent Authorities

Awareness about the TCO Regulation. As expected, LEAs have a significantly better understanding of the TCO Regulation than HSPs. In some Member States, LEAs have built upon previous relationships with HSPs, to initiate outreach campaigns and are prepared to engage with HSPs as necessary once a greater rollout of tools has been done such as PERCI. One challenge is the national disparities in preparedness and awareness among LEAs. These disparities create a state of limbo, with TCO implementation cases or cross-border removal orders remaining absent.

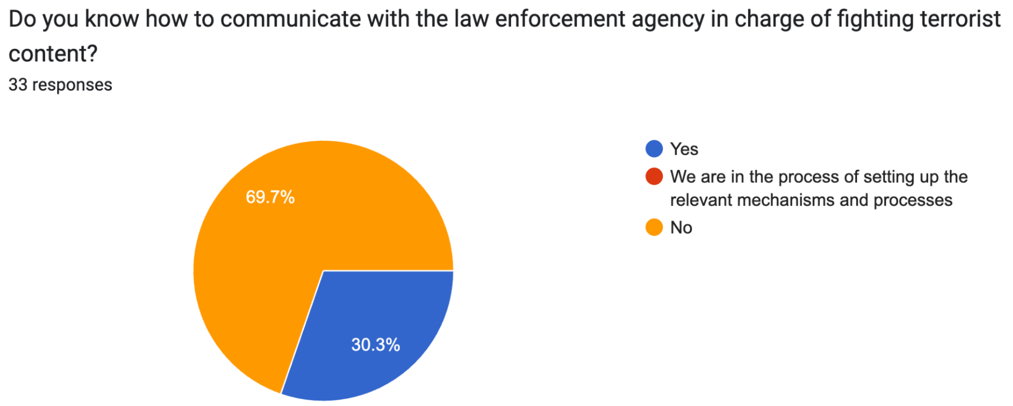
Divergence in defining terrorist content. Despite the use cases provided by the TCO Regulation, defining and identifying terrorist content remains a challenge not only for HSPs as mentioned previously, but also for some LEAs. This situation is further complicated by the fact that online platforms may receive removal orders that conflict with local laws or infringe on users' rights to free speech or access to information. Platforms may thus face pressure from LEAs from different countries or regions with different legal and cultural norms, making it challenging to navigate and comply with multiple jurisdictions. This lack of consensus, which participants said would never occur at the EU level, may lead to tensions around cross-border removal orders.

Additionally, HSPs more frequently encounter other types of illegal and violent content, such as hate speech, scams, bots, cult recruiting, and child pornography, rather than ‘pure terrorist content’. As a result, the detection, signalling, and removal of terrorist content become part of the broader issue of ‘cyber-maliciousness’, which also affects LEAs.

Communication between HSPs and LEAs. A crucial aspect of the relationship between HSPs and LEAs is that it is built on communication. Based on our online survey *69.7% of the responding HSPs do not know how to communicate with LEAs and none of them is in the process of setting up the relevant mechanisms and processes.*

At present, there are different channels for communication between LEAs and online platforms, but these often take place through non-secure, sometimes *ad hoc* means, such as phone calls, text messages, or emails. Sometimes it is even difficult to find the right contact for a given platform, and similarly, online platforms often have difficulties in finding the proper communication channels with LEAs. Both parties have expressed a desire to foster greater communication and coordination between them. However, *the challenge for HSPs lies in adhering to the timeline for reacting and removing content after receiving an order*, as they do not always operate on a 24/7 basis.

Interestingly, none of the interviewed HSPs or LEAs have issued or received removal orders under the TCO framework until now. However HSPs anticipate difficulties in *responding to removal orders within 1 hour and storing terrorist content with appropriate safeguards*. Such LEA requests would make it even harder for HSPs to achieve compliance with the regulation, beyond the general concern over the lack of operational capabilities expressed by several interviewees.



Do you know how to communicate with the law enforcement agency in charge of fighting terrorist content?

33 responses

Figure 15 - Q12/ Communication with LEAs

PERCI. The *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (PERCI) is a single system to connect all EU Member States and HSPs for the facilitation of the referrals and removal orders, to be developed and operated by Europol. Based on our interviews LEAs have different approaches to PERCI, with some seeing it as confusing their current processes while others believe it will have a positive impact on communication both internally and with HSPs. While some LEAs currently use *Internet Referral Management Application* (IRMA), others have participated in trainings related to PERCI. However, there remains some uncertainty about how PERCI will function, and thus many LEAs are awaiting the rollout before running more workshops on the TCO Regulation. Europol has stated that PERCI's launch has been delayed due to new recommendations from the GDPR European Regulator on using cloud-based technologies, however it has expressed confidence that it should be rolled out soon, following which we will likely see greater movement in this area.

4. Conclusions

General level of awareness concerning the TCO Regulation

One of the take-aways from our online survey and interviews with key stakeholders concerns the awareness in relation to the TCO Regulation: *HSPs tend to have a very limited awareness and knowledge of the TCO Regulation even compared to Digital Services Act*. Also, larger HSPs and in general LEAs have clearly a better understanding of the TCO Regulation. Nevertheless, if LEAs are clear regarding their duties in relation to the TCO Regulation, national disparities are striking as we witness different levels of preparedness. The lack of awareness regarding the TCO Regulation may be due to several reasons:

- a lack of understanding of who the category 'HSP' applies to, as it was often misunderstood or lost in translation, and leading to some uncertainty as to whether the platform falls under the TCO Regulation's scope - for a more detailed discussion about the TCO Regulation's definition of HSP, see part 1.2 ;
- insufficient level of communication from public authorities about the TCO Regulation and its implications, thus paving the way for awareness raising activities ;
- a belief shared by most HSPs who do not perceive themselves as being potentially exposed to terrorist content and thus believe that the TCO Regulation will not have any impact on their activities.

Moreover, despite the use cases given by the TCO Regulation, defining and identifying what is in practice 'terrorist content' is also a challenge for most HSPs. The boundaries between terrorism, other violent actions or for instance hate speech is not always clear for all stakeholders and may have a different 'meaning' in different national contexts as interviews with some national LEA have shown this.

Technical resources and processes

Micro and small HSPs fundamentally lack the tools (e.g. for automated detection, monitoring, content moderation, etc.) but even more importantly the processes to efficiently implement the provisions of the TCO Regulation. This is reflected by the fact that only slightly over 20% of the HSPs responding to our online survey moderate all content generated by users on their services. Furthermore an important majority of the responding HSP have not set-up tools and processes that would significantly foster compliance with the TCO Regulation. Micro and small HSPs will face particular challenges in developing capacities in both - automated and human monitoring, assessment and classification of content.

It is also clear that the readiness to comply with the TCO Regulation increases with the size of the HSPs. Some of the interviewed medium sized HSPs were showing more processes and tools in place mainly because of their own business needs and Terms of Services, still doing the content moderation mainly manually but using some simple tools. While automated detection tools (including intelligent AI tools) have been also used by some medium sized and mostly larger HSPs, practitioners and researchers have previously also highlighted that the human factor/oversight in verifying AI-flagged content remains key, in order to put content into context[141].

In general several stakeholders have pointed out the lack of resources that micro and small HSPs are facing. This also affects their willingness to invest in developing the right processes and implementing efficient tools not only to be compliant with new regulations but also to serve their own business needs. This would only be changed in case an imminent manifestation of a (terrorist) threat would push them to do so, otherwise these investments would be likely to be postponed as much as possible.

Since there is a fundamental lack of awareness and lack of general understanding of the implications of the regulation, we see a real added value in providing support to implement processes in line with the TCO Regulation. Any technical tool to be implemented by HSPs can only be part of a more general compliance process.

Another concern for HSPs is the potential implications of communicating with HSPs and responding within one-hour to removal orders under the TCO - especially if issued by a competent authority of a member state other than the HSPs country of origin. PERCI has an important role in the ecosystem. However in its absence, HSPs will most likely require technical tooling to help them manage any potential interactions with competent authorities under the TCO. This tooling could potentially also serve micro and small HSPs to comply with their obligations under the DSA.

Human competences, knowledge and skills

All HSPs enter the scope of TCO Regulation independently of their size, however micro and small companies are exempt from certain obligations within the DSA (for example the obligations for online platforms and obligations for transparency reporting). This means that based on the TCO a small platform with a few employees and few thousand users would have to implement the same provisions with very different levels of human resources to comply with the TCO compared to a much larger online platform with more significant resources.

Encouragingly, *there is a strong desire among HSPs to learn more about the TCO Regulation (81,8%) and receive guidance to tools for content moderation (66,7%) and automated content identification tools (63,6%).*

[141] Radicalisation Awareness Network (2022), "The Online Dimension of Extremism andImproving Online P/CVE Efforts", RAN Cross-cutting event conclusion paper, 27 September 2022. https://home-affairs.ec.europa.eu/system/files/2022-12/ran_paper_online_dimension_extremism_improving_online_pcve_efforts_27092022_en.pdf

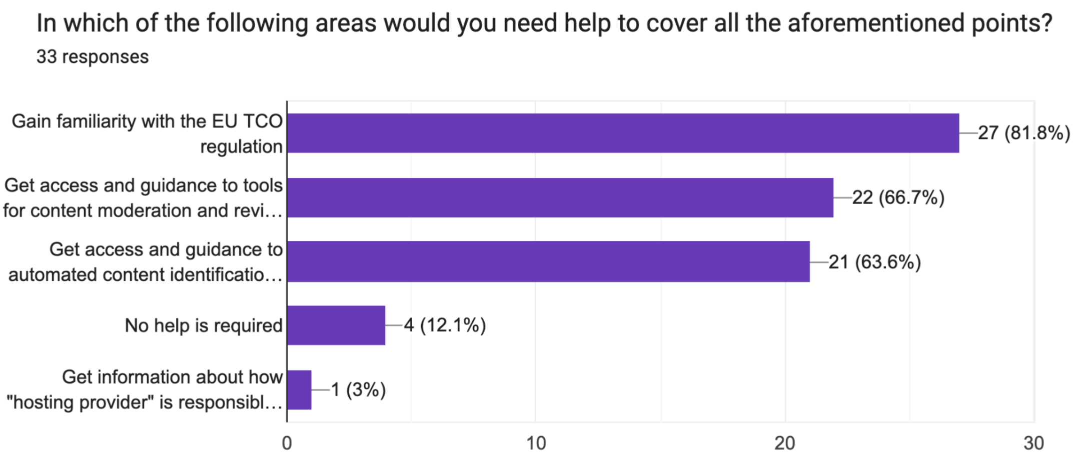


Figure 16 - Q13/ Potential help areas

Providing support would help to clear the current lack of information that has left many HSPs unaware of both their requirements as well as how to reach these requirements. Participation in FRISCO's training and awareness activities may help bridge this knowledge gap and improve HSPs' ability to effectively address terrorist content on their platforms. In addition, FRISCO’s products focussed on fostering knowledge exchange and providing guidance on good practices and available tools is likely to directly address HSPs needs of practical know-how when implementing the TCO Regulation.

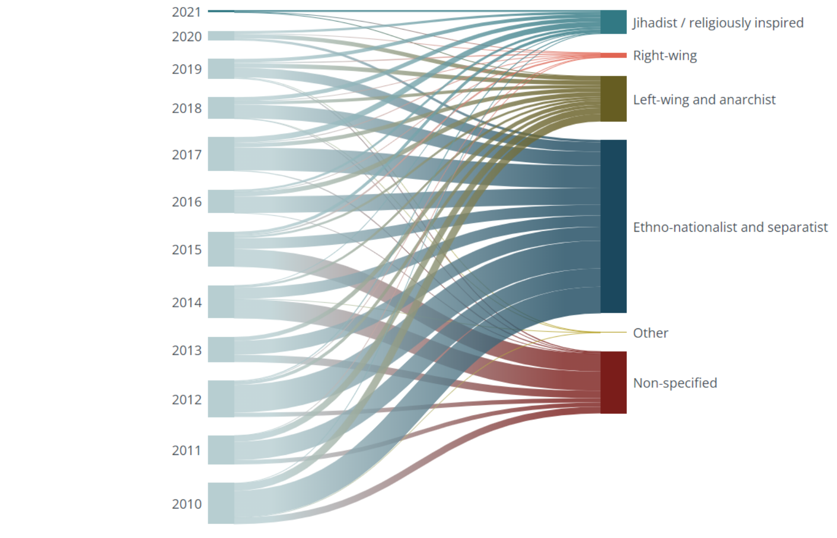
Next steps for the FISCO project.

As next steps the consortium of the FRISCO project will concentrate on sharing our findings with stakeholders and collecting feedback about our findings. Also based on the findings of the mapping report a detailed specification of the tools, frameworks and mechanisms to be developed will be finalised. In parallel the needs of micro and small HSPs’ for training and capacity building materials will be documented and a roadmap will be defined to involve micro and small HSPs into the awareness raising activities.

5. Appendices

5.1 Overview of the terrorist threat in the European Union

The *EU Terrorism Situation and Trends Reports* (TE-SAT), published by Europol, distinguishes between 5 categories of terrorism, differentiated on the basis of ideological drivers: jihadist terrorism, right-wing terrorism, left-wing terrorism and anarchist terrorism, ethno-nationalist and separatist terrorism, and other types of terrorism[142]. Between 2010 and 2021, a total of 1810 terrorist attacks (completed, failed or foiled) have been notified by EU Member States[143]. Of these attacks, 130 were related to jihadist or religiously-inspired terrorism, 28 to right-wing terrorism, 229 were attributed to left-wing terrorism, 1043 to ethno-national or separatist terrorism, 6 to other types of terrorism and 374 to non-specified forms of terrorism[144]. It is interesting to remark that, maybe counter-intuitively, ethno-national and separatist terrorist attacks are, by far, the most recurrent within the EU, far ahead from the much more publicised jihadist and right-wing attacks. During the same period, 8774 terrorism-related arrests have been carried out by Member States : 4466 were related to jihadist or religious terrorism, 258 to right-wing terrorism, 564 to left-wing terrorism, 1423 to ethno-national or separatist terrorism, 15 to other types of terrorism and 2048 to non-specified forms of terrorism[145].



Source: Europol's annual EU terrorism situation and trend reports (from 2011 to 2021)

Figure 17 - Terrorist attacks in the EU between 2010 and 2011
Source : Infographic - Terrorism in the EU: facts and figures

[142] Europol (2022), *op. cit.*, p.6.

[143] Please note that figures from 2010 to 2019 include the United Kingdom, both for attacks and arrests.

[144] See : European Council - Council of the European Union (2023), "*Infographic - Terrorism in the EU : facts and figures*". URL : https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/

[145] *Ibidem*.

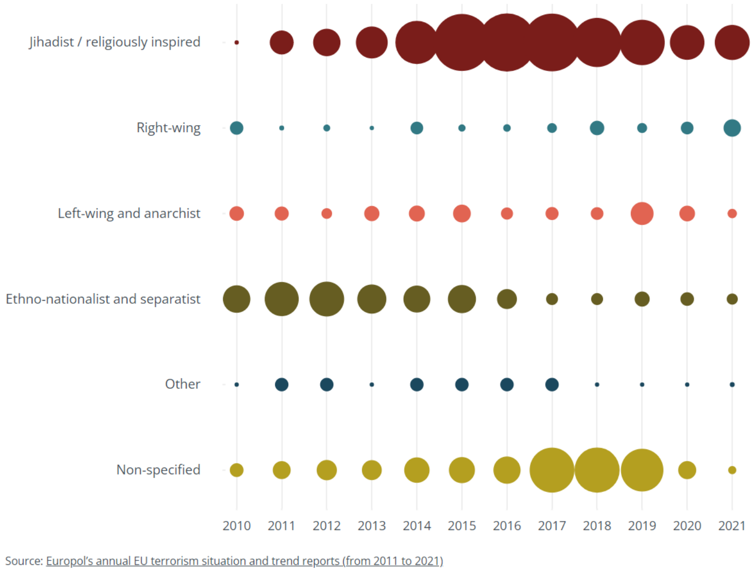


Figure 18 - Terrorism-related arrests in the EU between 2010 and 2011
Source : Infographic - Terrorism in the EU: facts and figures

According to the latest TE-SAT's findings, in 2021, there were "only" 15 completed, failed or foiled terrorist attacks in all Member States, 11 related to jihadist or religious terrorism, 3 to right-wing ideologies and 1 to left-wing ones - 4 of these attacks were successful, 3 jihadist and one inspired by left-wing ideologies[146]. The number of attacks notified in 2021 is significantly lower than it was in 2020 (57) and 2019 (55) because of the significant decrease in left-wing inspired terrorist attacks[147]. Regarding the terrorism-related arrests, we also witness a decrease since 2019 (723), with 449 in 2020 and 388 in 2021, all types of terrorism together[148]. Finally, there have been 423 convictions for terrorist offences in 2021[149]. This recent decrease in attacks and arrests should not be interpreted as a permanent or lasting disappearance of the terrorist threat looming over Europe, as fluctuations in figures may originate from exogenous or intricate factors.

[146] Europol (2022), *op. cit.*, pp.4-8
[147] *Ibid.*, p.4.
[148] *Ibid.*, p.8
[149] *Ibid.*, p.4

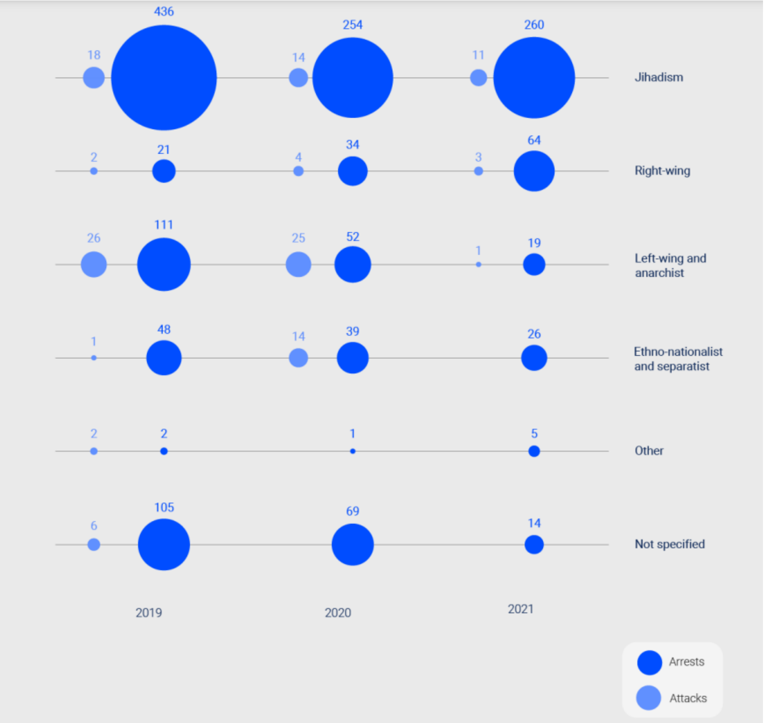


Figure 19 - Terrorist attacks and arrests in the EU between 2019 and 2021
Source : [Europol (2022), *op.cit.*, p.8]

Nevertheless, geographical and historical comparisons allow us to put this terrorist threat into perspective, a prerequisite for dealing with it in the most suitable way possible. For instance, if we take a look at the global distribution of terrorism by regions according to the [Global Terrorism Database][150], on the 22,847 deaths caused by terrorists attacks in 2020, "*97% occurred in the Middle East, Africa or South Asia*", with countries such as Afghanistan, Nigeria and Ethiopia being the most impacted - Afghanistan alone "*accounted for 44% of terrorism deaths in the world*[151]". It is thus important to recall that European countries are far from being the most affected : between 2010 and 2020, 624 persons died because of terrorist attacks in Western Europe, 3301 persons in Eastern Europe, which is dreadful, but relatively low within the global context[152].

[150] Please note that giving such data implies relying on different definitions.
[151] Hannah Ritchie, Joe Hasell, Edouard Mathieu, Cameron Appel and Max Roser (2013) - "Terrorism". Published online at OurWorldInData.org. URL : https://ourworldindata.org/terrorism
[152] *Ibidem*.

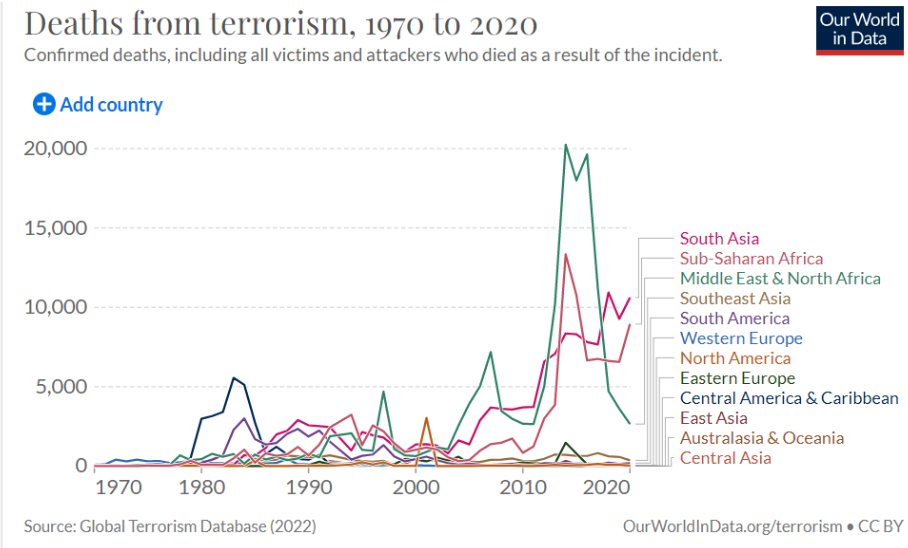


Figure 20 - Global deaths from terrorism by regions (1970-2020)

Source : Hannah Ritchie, Joe Hasell, Edouard Mathieu, Cameron Appel and Max Roser (2013) - "Terrorism" (OurWorldInData)

Moreover, if one looks at the long term, terrorism *per se* has not been on the rise in Western Europe. "*Western Europe was home to the most terrorist deaths globally*" during the 1970s, accounting "*in many years 70% to 80% of recorded deaths from terrorism*[153]" and since then terrorist attacks have been reduced in frequency and number. The recent large-scale terrorist attacks on European soil produce both volatility in year-to-year numbers and a distortion of the threat perception, thus fueling feelings that terrorism and/or overall insecurity might be on the rise, most likely because of the extensive media coverage of the events, the related emotional trauma and the 'availability heuristic' cognitive bias ("*[w]hen things become increasingly visible in the media, it's easy to assume that they're becoming more common*[154]"). For instance, according to the Special Eurobarometer 464b ("*Europeans' attitude towards security*") conducted in June 2017, so in the aftermath of major terrorist attacks in Europe (Paris, Brussels, Nice, Berlin, Manchester), Europeans continued "*to regard challenges to the internal security of the EU as important, particularly terrorism (95%)*[155]", while "*the proportion of those who [thought] that the EU [was] a secure place to live in [fell significantly] : just over two thirds (68%) [said] so in this survey compared with close to eight in ten (79%) in 2015*[156]". This Eurobarometer thus points a direct link between this decrease and the recent attacks : "*foreign terrorist fighters returning to the EU from conflict zones, and [...] a series of terrorist attacks within the EU contribute to making security and in particular terrorism at the top of European's concerns*[157]".

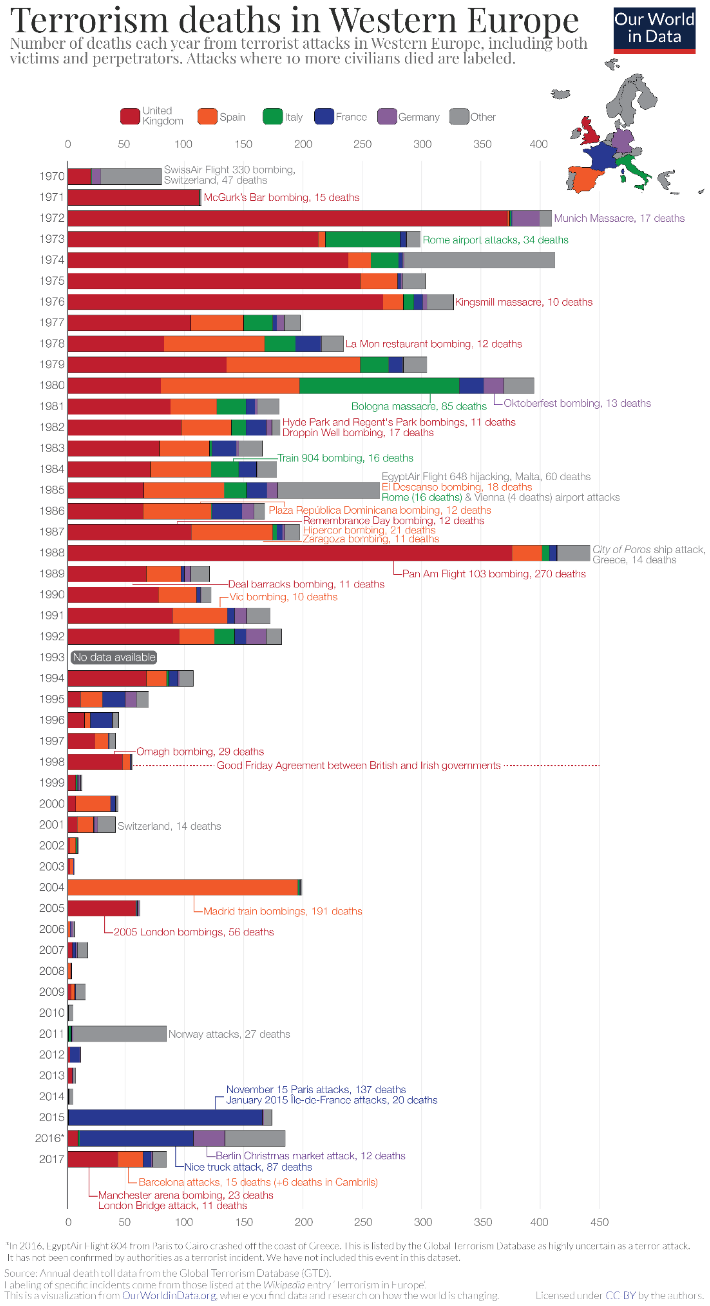
[153] *Ibidem*.

[154] *Ibidem*.

[155] "Europeans' attitude towards security - Summary ", European Commission, Special Eurobarometer 464b, June 2017, p.4. URL : https://europa.eu/eurobarometer/surveys/detail/1569

[156] *Ibid.*, p.3.

[157] *Ibid.*, p.2.



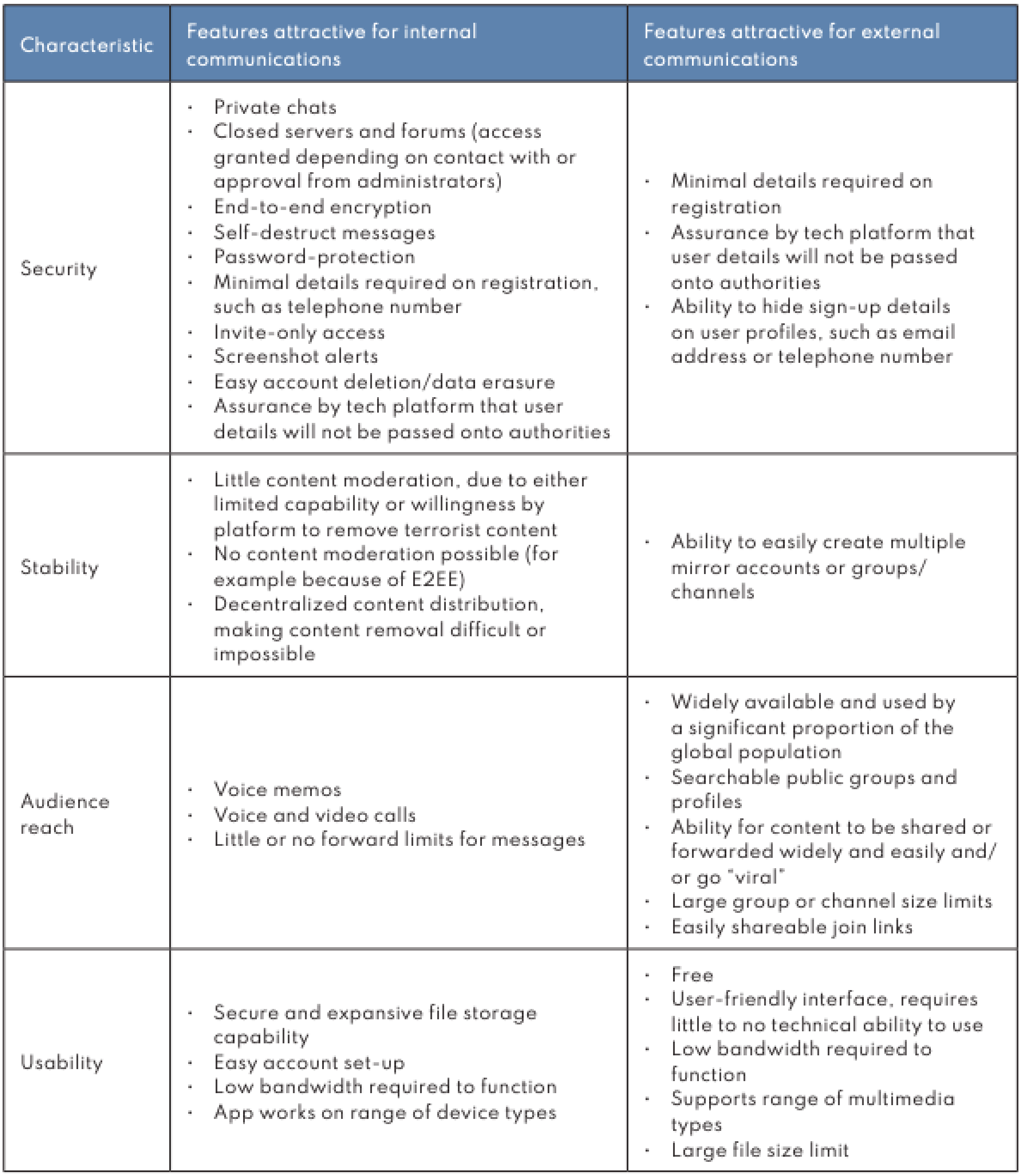
*In 2016, EgyptAir Flight 804 from Paris to Cairo crashed off the coast of Greece. This is listed by the Global Terrorism Database as highly uncertain as a terror attack. It has not been confirmed by authorities as a terrorist incident. We have not included this event in this dataset.

Source: Annual death toll data from the Global Terrorism Database (GTD).
Labeling of specific incidents come from those listed at the *Wikipedia* entry 'Terrorism in Europe'.
This is a visualization from OurWorldinData.org, where you find data and research on how the world is changing. Licensed under CC BY by the authors.

Figure 21 - Terrorism death in Western Europe (1970-2017)

Source : Hannah Ritchie, Joe Hasell, Edouard Mathieu, Cameron Appel and Max Roser (2013) - "Terrorism" (OurWorldInData)

5.2 Features attractive to terrorist groups for internal and external communications



Characteristic	Features attractive for internal communications	Features attractive for external communications
Security	· Private chats · Closed servers and forums (access granted depending on contact with or approval from administrators) · End-to-end encryption · Self-destruct messages · Password-protection · Minimal details required on registration, such as telephone number · Invite-only access · Screenshot alerts · Easy account deletion/data erasure · Assurance by tech platform that user details will not be passed onto authorities	· Minimal details required on registration · Assurance by tech platform that user details will not be passed onto authorities · Ability to hide sign-up details on user profiles, such as email address or telephone number
Stability	· Little content moderation, due to either limited capability or willingness by platform to remove terrorist content · No content moderation possible (for example because of E2EE) · Decentralized content distribution, making content removal difficult or impossible	· Ability to easily create multiple mirror accounts or groups/ channels
Audience reach	· Voice memos · Voice and video calls · Little or no forward limits for messages	· Widely available and used by a significant proportion of the global population · Searchable public groups and profiles · Ability for content to be shared or forwarded widely and easily and/ or go "viral" · Large group or channel size limits · Easily shareable join links
Usability	· Secure and expansive file storage capability · Easy account set-up · Low bandwidth required to function · App works on range of device types	· Free · User-friendly interface, requires little to no technical ability to use · Low bandwidth required to function · Supports range of multimedia types · Large file size limit

Figure 22 - Features attractive to terrorist groups for internal and external communications

Source : GIFCT - Tech Against Terrorism (2021), *op. cit.*, p.33

6. References

Reports

- Bodo, L. and Trauthig, I. K. (2022), "Emergent Technologies and Extremists: The DWeb as a New Internet Reality?", Global Network on Extremism and Technology, 2022. URL : https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf
- 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*. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0408
- European Commission (2019), Directorate-General for Communications Networks, Content and Technology, Hoboken, J., Quintais, J., Poort, J., et al., *Hosting intermediary services and illegal content online : an analysis of the scope of article 14 ECD in light of developments in the online service landscape : final report*, Publications Office, 2019. URL : https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content
- Europol (2022), "European Union Terrorism Situation and Trend Report", Publications Office of the European Union, Luxembourg. URL : https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf
- Europol (2022), "Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab", Publications Office of the European Union, Luxembourg, 2022. https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf
- 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. URL : https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf
- King, P. (2019), "Islamic State group's experiments with the decentralised web - Conference Paper". Europol, ECTC Advisory Network Conference. URL : https://www.europol.europa.eu/sites/default/files/documents/islamic_state_group_experiments_with_the_decentralised_web_-_p.king_.pdf
- Macdonald, S. and Staniforth, A. (2023), "Tackling Online Terrorist Content Together : Cooperation between Counterterrorism Law Enforcement and Technology Companies". Global Network on Extremism and Technology (GNET), January 2023. URL : https://gnet-research.org/wp-content/uploads/2023/01/31-Tackling-Online-Terrorist-Content-Together_web.pdf

- Radicalisation Awareness Network (2022), "The Online Dimension of Extremism andImproving Online P/CVE Efforts", RAN Cross-cutting event conclusion paper, 27 September 2022. https://home-affairs.ec.europa.eu/system/files/2022-12/ran_paper_online_dimension_extremism_improving_online_pcve_efforts_27092022_en.pdf.
- Radicalisation Awareness Network (2021), "Conspiracy theories and right-wing extremism – Insights and recommendations for P/CVE", Luxembourg : Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2021-04/ran_conspiracy_theories_and_right-wing_2021_en.pdf
- Radicalisation Awareness Network (2021), " The gamification of violent extremism & lessons for P/CVE", Luxembourg: Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2021-03/ran_ad-hoc_pap_gamification_20210215_en.pdf
- Radicalisation Awareness Network Practitioners (2021), "Capitalising on Crises How VRWEs Exploit the COVID-19 Pandemic and Lessons for P/CVE", Luxembourg : Publications Office of the European Union, 2021. URL : https://home-affairs.ec.europa.eu/system/files/2022-02/ran_capitalising_crises_how_vrwe_exploit_covid-19_pandemic_082021_en.pdf
- 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. URL : https://cronfa.swan.ac.uk/Record/cronfa62902
- Schmid, A. P. (2023), "Defining terrorism". *International Center for Counter-Terrorism* (ICCT Report), March 2023. URL : https://www.icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf
- Schmid, A. P. (2021), "Handbook of terrorism prevention and preparedness". *International Center for Counter-Terrorism* (ICCT Report), July 2021. URL : https://www.icct.nl/handbook-terrorism-prevention-and-preparedness
- United Nations Counter-Terrorism Centre (2022), "Examining the Intersection Between Gaming and Violent Extremism", United Nations Office of Counter-Terrorism (UNCCT), Global Programme on Preventing and Countering Violent Extremism and Special Projects and Innovation Branch, 2022. URL : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf
- United Nations Office on Drugs and Crime (2012), "The use of Internet for terrorist purposes", New York. URL : https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf

- 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. URL :https://www.icct.nl/sites/default/files/2022-12/Christchurch-report-Dec-2020_Spelling-fixed.pdf
- Tech against Terrorism (2022), “Transparency Report. Terrorist Content Analytics Platform. Year One : 1 December 2020 - 30 November 2021”, March 2022. URL : https://www.techagainstterrorism.org/wp-content/uploads/2022/03/Tech-Against-Terrorism-TCAP-Report-March-2022_v6.pdf
- Tech Against Terrorism (2022), “The Threat of Terrorist and Violent Extremist Operated Websites”, January 2022. URL : https://www.techagainstterrorism.org/wp-content/uploads/2022/02/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022.pdf

Scientific articles

- Bellanova, R. and de Goede, M. (2022), “Co-producing security : platform content moderation and European security integration”. *Journal of Common Market Studies*, Vol. 60, Issue 5, pp. 1316-1334. URL : https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.13306
- Bjørgo, T., & Braddock, K. (2022). Anti-Government Extremism: A New Threat? *Perspectives on Terrorism*, *16*(6), 2–8. URL : https://www.jstor.org/stable/27185087
- Brubaker, R. (2020), “Digital hyperconnectivity and the self”. *Theory and Society*, 49, pp.771-801. URL : https://doi.org/10.1007/s11186-020-09405-1
- Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A. and Weir, D. (2019), “Disrupting Daesh : Measuring Takedown of Online Terrorist Material and its Impacts”. *Studies in Conflict & Terrorism*, Vol. 42, Nos. 1-2, pp.141-160. URL : https://www.tandfonline.com/doi/epdf/10.1080/1057610X.2018.1513984?needAccess=true&role=button
- 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. URL : https://www.tandfonline.com/action/showCitFormats?doi=10.1300%2FJ516v04n01_03
- 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, pp. 99-117. URL : https://onlinelibrary.wiley.com/doi/epdf/10.1111/1745-9133.12249
- Holt, J. T., Lee, J. R., Freilich, J. D., Chemark, S. M., Bauer, M. J., Shillair, R. and Ross, A. (2002), “An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks”.

Terrorism and Political Violence, 34:7, pp.1305-1320. URL : https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F09546553.2020.1777987

- Holt, J. T., Stonhouse, M., Freilich, J. and Chermak, S. M. (2021), "Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups, Terrorism and Political Violence". *Terrorism and Political Violence*, 33:3, pp.527-548. URL : https://www.tandfonline.com/doi/abs/10.1080/09546553.2018.1551213?journalCode=ftpv20
- Jackson, S. (2022). What Is Anti-Government Extremism? *Perspectives on Terrorism*, *16*(6), 9–18. URL : https://www.jstor.org/stable/27185088
- Kenney, M. (2015), "Cyber-Terrorism in a Post-Stuxnet World". *Orbis*, 59, Winter 2015, pp.111-128. URL : https://www.researchgate.net/publication/270914520_Cyber-Terrorism_in_a_Post-Stuxnet_World
- Lakhani, S. and Wiedlitzka, S. (2022), "Press F to Pay Respects": An Empirical Exploration of the Mechanics of Gamification in Relation to the Christchurch Attack", *Terrorism and Political Violence*. URL : https://www.tandfonline.com/doi/full/10.1080/09546553.2022.2064746
- Lemieux, A., Brachman, J. M., Levitt, J., and Wood, J. (2014), ""*Inspire* Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model." *Terrorism and Political Violence* 26 (January), pp. 354-371. URL : https://www.tandfonline.com/doi/abs/10.1080/09546553.2013.828604#.Uu-nW_vWS_A&nbsp
- Song, Y., Chen, B., & Wang, X. Y. (2023). "Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related?". *Financial innovation*, *9*(1), 29. URL : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9860235/#CR50
- 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. URL : https://onlinelibrary.wiley.com/doi/full/10.1111/nana.12780
- Weimann, G. (2004), "Cyberterrorism. How real is the threat?". United States Institute of Peace, Special Report 119, December 2004. URL : https://www.usip.org/sites/default/files/sr119.pdf
- Weimann, G. (2004), "How modern terrorism uses the Internet". United States Institute of Peace, Special Report 116, March 2004. URL : https://www.usip.org/sites/default/files/sr116.pdf

- Weimann, G. and Vellante, A. (2021), “The Dead Drops of Online Terrorism”. *Perspectives on Terrorism*, August 2021, Vol. 15, No. 4, pp. 39-53. URL: https://www.jstor.org/stable/10.2307/27044234
- Whittaker, J. (2022), “Rethinking online radicalization”. Perspectives on Terrorism, August 2022, Vol. 16, No. 4, pp.27-40. URL : https://www.jstor.org/stable/10.2307/27158150
- Whittaker, J. (2022), “The Role of Financial Technologies in US-Based ISIS Terror Plots”. *Studies in Conflict & Terrorism*, pp.1-26. URL : https://www.tandfonline.com/doi/epdf/10.1080/1057610X.2022.2133345?needAccess=true&role=button

Legal texts

- DIRECTIVE (EU) 2015/1535 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN
- DIRECTIVE (EU) 2017/541 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN
- REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN

------End of Document------