MUHAMMAD BAKHTIAR UL HASSAN

The EU Legal Framework and National Strategies for Monitoring Terrorist Content Online

Dissertation to obtain a Master´s Degree in Law, in
Specialty of International and European Law

Supervisor:

Athina Sachoulidou, an Assistant Professor in Criminal Law at NOVA School of Law, Lisbon

September, 2022

Anti-Plagiarism Statement

I hereby declare that the work I presented here is my own work and that all my citations are correctly acknowledged. I am aware that the unacknowledged extraneous materials and sources constitute a serious ethical and disciplinary offence.

Muhammad Bakhtiar Ul Hassan

List of Abbreviations:

UNODC	United Nations Office on Drugs and Crime
EU	European Union
JHA	Justice and Home Affairs
AI	Artificial Intelligence
NATO	North Atlantic Treaty Organisation
SDF	Syrian Democratic Forces
FTFs	Foriegn Terrorist Fighters
ISIS	Islamic State of Iraq and Syria
PKK	Kurdistan Workers Party
REMT	Racially or Ethnically Motivated Behaviour
CTTF	Countering Transnational Terrorism Forum
LECG	Law Enforcement Coordination Group
US	United States
EUROPOL	The European Union Agency for Law Enforcement Cooperation
INTERPOL	The International Criminal Police Organization
UK	United Kingdom
VERLT	Violent Extremism and Radicalisation that lead to Terrorism
EUROJUST	European Union Agency for Criminal Justice Cooperation
JITs	Joint Investigation Teams
SNE	Seconded National Experts
ECTC	European Counter Terrorism Center
TE-SAT	EU Terrorism Situation and Trend Report
TFEU	Treaty on the Functioning of European Union
CoE	Council of Europe
PACE	Council of Europe´s Parliamentary Assembly
IT	Information Technology

HSPs	Hosting Service Providers
ISPs	Internet Service Providers
EFTA	European Free Trade Association
EUIF	European Union Internet Forum
EU-IRU	European Union Internet Referral Unit
EUCP	European Union Crisis Protocol
CSEP	Civil Society Empowerment Program
RAN	Radicalisation Awareness Network
INCL.	Icluding
DSA	Digital Services Act
VLOPs	Very Large Online Platforms
NetzDG	Network Enforcement Act
LCEN	Law for Trust in the Digital Economy
OCLCTIC	Directorate General of the National Police, the Central Office for Combating ITC-related Crime
CSI	Homeland Security Code
TCAP	Terrorist Content Analytics Platform
TCO	Terrorist Content Online
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
NGOs	Non-Governmental Organisations
CDT	Center for Democracy and Technology

Declaration

It is stated that, the body of the Thesis starting from Introduction to the Conclusion, consists of six Chapters, number of Pages are 56 and the Characters including Spaces are 131,970.

Abstract

It is generally but rightly said that while everyone understands what terrorism is, no one has agreed on its definition yet. The scenario is no different when it comes to the issue of online terrorist content. The ambit and the scope of legal definition pertaining to the terrorist organization online has always been an issue for the European Union Member States. With the increasing frequency of online terrorist content and their changing spectrums has made this task for the jurists a bit difficult and hard nut to crack. There was always a need to not only analyze the issues that the EU Member States face in defining the ambit of it, but it seemed quite necessary that the scope of those provisions which pertains to the distribution of terrorist content online much be re-defined or at least defined. The legal framework that has been taken into account has somehow served the purpose in this regard. However, holistic efforts are required in this regard. On the similar account, the surveillance of the online terrorist content in European Union is needed to be tighten up. For that, this study assessed the ways in which the EU Member States are monitoring and handling online terrorist content and related issues in the region. In this regard, number of commissions under the ambit of European Union and other working under national authorities have shown significant work. These Commissions are continuously studying the matter of handling illegal content on online platforms and have already organized a number of educational and informational activities. The weaknesses and strengths of the European Union Members States to counter online terrorist content is of grave concern. There is need to present and evaluate the EU Member States' strategies regarding online terror related content. Analysis can be made over case studies of France and Germany. The study moves forward by assessing and evaluating the remedial measures in this regard as well. The major focus is based upon assessing the remedies and complaint procedures to address the distribution of terrorist content online under the Regulation (EU) 2021/784. Similarly, an effort has been made to explore the current implementation status and

hurdles regarding the Regulation (EU) 2021/784. Lastly, the analysis could only be cemented through recommending reforms at administrative and legislative level in the EU for efficient mitigation of online terrorism and associated threats. It is need of hour to enact such laws, statutes and regulations that not only accurately defines the illegal or terrorist content but also enables the Internet Services Providers to have clear litmus test for such content along with the authority to be given to the Internet Services Providers and other regulatory authorities to struck down content falling under the criterion set for the online terrorist content

Table of Contents

Chapter 1: Introduction

1.1 Research Background

Terrorists use the Internet to communicate, plan attacks, disseminate propaganda, raise funds, and recruit new members. Terrorist websites host, among other things, messages and propaganda videos to boost morale and improve recruitment and fundraising systems. The term ´cyberterrorism´ is usually used to refer to the use of the internet as a vehicle for an attack. Today, the globe is more linked than it has ever been. Greater connectivity has many advantages, but it also brings with it an increased danger of fraud, theft, and abuse. Increasingly widespread cyber assaults including corporate security breaches, spear phishing, and social media fraud may be traced back to the rise of technology in the world and its dependence thereon. The protection of cyberspace necessitates the employment of both cybersecurity and law enforcement expertise. Law enforcement must investigate and prosecute a wide range of cybercrimes, ranging from theft and fraud to child exploitation, in order to meet national and transnational cybersecurity goals.

Regulating the use of the Internet for terrorist purposes is something the United Kingdom has been doing for a long time; the authorities have been able to combat digital terrorist interest within national borders, even while maintaining the freedoms and advantages the Internet has brought to citizens. However, they acknowledged that the threat is transnational. As a result of joint action in making international legal harmony, the global network may hope to confront terrorists' use of the internet effectively. Since the British government welcomed UNODC's guidance in creating an e-book on this topic, the British government has been eager to help UNODC develop the e-book so that lawmakers, police officers, and criminal justice experts can use it to expand and enforce legal agendas that can disrupt terrorist actions in the digital sphere[1]. In 2001, the "Council of Europe Convention on Cybercrime", also known as the "Budapest Convention"[2], became the most effective multidimensional, lawfully linking

[1] Kristina Ramešová, 'Public Provocation to Commit a Terrorist Offence: Balancing between the Liberties and the Security' (2020) 14 Masaryk University Journal of Law and Technology 123.
[2] '1680a6992e.Pdf' <https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e> accessed 13 September 2022.

instrument for discussing illegal activity committed over the Internet at that time. Furthermore, to ensure that terrorist crimes can be properly prosecuted and actions will be taken to help those who have been victimized by terrorism, the Council of the European Union adopted the Framework Decision 2002/475/JHA of 13 June 2002[3], which defined terrorist crimes across European Union (EU) Member States.

The Framework Decision 2002/475/JHA was principally based on the provisions of the "Council of Europe Convention on the Prevention of Terrorism[4]" for crimes of public provocation to commit a terrorist offence, Recruitment for terrorism or Training for terrorism.

The Framework Decision 2008/919/JHA amending Framework Decision 2002/475//JHA on combating terrorism[5], provides to criminalize offences linked with terrorist acts to enhance general policy for the prevention of terrorism by reducing dissemination of such materials which may lead to the incitement of terrorist attacks, further approximated the definition of terrorist offences covering "public provocation to commit a terrorist offence", "training for terrorism", and "recruitment" when committed intentionally and included new offences involving conduct that has the potential to lead to the acts of terrorism, independent of the strategy or technical tools used to perpetrate these crimes. The terms of the Framework Decision 2008/919/JHA, like those to be found in the Council of Europe Convention on the Prevention of Terrorism, are not Internet-specific but may include activities carried out over the Internet.

There was a problem in the application of Framework decisions as the member states were free to choose the means to get the results and able to appeal against it before the Court of Justice of the European Union. After the Lisbon Treaty came into force, Framework decisions were replaced by Directives obliging EU Member States to abide by Regulations or Directives.

The Directive (EU) 2017/541 of the European Parliament and of the Council, adopted on March 15, 2017[6], provides for the terrorist offences, such as, "providing training, recruitment for terrorism , public provocation to commit a terrorist offence, receiving

[3] Council Framework Decision of 13 June 2002 on combating terrorism 2002 (OJ L).
[4] '16808c3f55.Pdf' <https://rm.coe.int/16808c3f55> accessed 13 September 2022.
[5] 'EUR-Lex - 32008F0919 - EN - EUR-Lex' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0919> accessed 13 September 2022.
[6] 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 2017.

training for terrorism, travelling for the purpose of terrorism or facilitating travelling for the purpose of terrorism, terrorist financing or aiding, abetting, inciting and attempting" and establishes the legal basis for prosecuting the distribution of terrorist planning and bomb-making proficiency via the Internet to the extent that such distribution is done deliberately and meets the requirements of those violations[7].

Additionally, to combat further dissemination of terrorist content online and making techs legally bounding, stronger and eligible, in taking actions against terrorism related online contents and of their removal, Regulation 2021/784[8] enacted in 2021 to issue removal orders of online terrorist content within specific time and also to support small platforms to comply with the regulation[9].

In the light of the Regulation (EU) 2021/784, this thesis examines the difficulties associated with and the mitigating methods related to online terrorist content and the removal thereof. Besides this, it explores the current implementation challenges as to resolving the problem of publication and distribution of terrorist content.

1.2 Literature Review

According to (Reiffenstuel 2021)[10], The European institutions, particularly the European Union and the Council of Europe, were obliged to change their legal framework for counterterrorism as a result of the threats and immediate domestic pressure. Europe can reclaim its reputation as a credible global player and a regional powerhouse with a successful counterterrorism policy that combines member nations' capabilities and relies on deep trust among intelligence agencies and law enforcement collaboration(Scheinin 2019)[11]. In case of working slowly or not paying focused attention towards policy making against terrorism of any shape, the EU's credibility and

[7] 'Regulating Terrorist Content on Social Media: Automation and the Rule of Law | International Journal of Law in Context | Cambridge Core' <https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1> accessed 13 September 2022.

[8] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) 2021 (OJ L).

[9] 'THE ONLINE REGULATION SERIES | EUROPEAN UNION (Update) - Tech Against Terrorism' (10 December 2021) <https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/, https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/> accessed 13 September 2022.

[10] Alexander Reiffenstuel, 'EU COUNTERTERRORISM STRATEGY: Understanding the Background, Measures and Limits of Europe's Counter-Terrorism Strategy between 2014 and 2020'.

[11] Martin Scheinin, 'The EU Regulation on Terrorist Content: An Emperor without Clothes' 2.

authority will be further eroded, populist parties will be able to take advantage of yet another fertile ground, and terrorists will be able to disrupt states' social cohesiveness and faith in government.

According to (Argomaniz, 2014); The use of the Internet for terrorist purposes is an area that European organizations are taking into mind. As of yet, the EU's response has focused on raising organizational pliability criteria to prevent cyberattacks. In spite of this, security concerns about computer espionage, criminal activity, and sabotage have fueled the belief that terrorist attacks are no longer a possibility.

According to the (Reeve 2020)[12]; There have been new legal techniques allowed to regulators and intelligence companies to monitor Internet users since the Internet has become a mainstream communications technology. A quite characteristic example is the Facebook´s use of AI to match images[13] in the case attempting to upload images or videos which are already identified as terrorist and to prevent its users from doing so again. Another example is the Facebook´s text understanding engine[14] which is employed to analyze text already removed for supporting terrorism or their organizations, and to make such algorithms that can detect similar posts in future, and also use of AI by the same platform to remove terrorist clusters[15] by mean of algorithms that detect pages or groups supporting activities of terrorism. These algorithms have targeted people suspected of terrorist acts and organizations that have used the Internet to publicize their activities and develop a scattered sense of society in particular. A wide variety of behaviour is prohibited as "supporting" or "apologizing" for terrorist attacks since anti-terrorism policies have emerged as preemptive measures. The European legal agenda is being tested in terms of confidentiality and non-discrimination through the lengthy investigation and detailing of terrorism suspects. That their uneven character is troublesome for these values and may cause challenges in cross-border regulatory enforcement cooperation is argued by those who believe in equal rights.

---

[12] Zoey Reeve, 'Repeated and Extensive Exposure to Online Terrorist Content: Counter-Terrorism Internet Referral Unit Perceived Stresses and Strategies' [2020] Studies in Conflict & Terrorism 1.

[13] 'The Image Similarity Challenge and Data Set for Detecting Image Manipulation' <https://ai.facebook.com/blog/the-image-similarity-challenge-and-data-set-for-detecting-image-manipulation/> accessed 13 September 2022.

[14] 'Introducing DeepText: Facebook's Text Understanding Engine - Engineering at Meta' <https://engineering.fb.com/2016/06/01/core-data/introducing-deeptext-facebook-s-text-understanding-engine/> accessed 13 September 2022.

[15] 'Hard Questions: How We Counter Terrorism' (*Meta*, 15 June 2017) <https://about.fb.com/news/2017/06/how-we-counter-terrorism/> accessed 13 September 2022.

1.3 Research Questions

Following are the main research questions this thesis aims to address:

1. Which are the main issues the EU member countries may face when attempting to define the ambit and scope of the provisions regarding the distribution of terrorist content online?
2. Which are the means, the EU member states employ to monitor and handle online terrorist content? To what extent have the strategies adopted by the EU Member States reduced the impact of and the vulnerability to online terrorist content?
3. What are the major provisions of the Regulation (EU) 2021/784 and their specificities as part of the EU counterterrorism agenda?
4. The complaint procedures to address the distribution of terrorist content online under the Regulation (EU) 2021/784 of the European Parliament and of the Council and which are the legal remedies provided for therein?
5. Which is the current implementation status of the Regulation (EU)/2021/784 and what are the implementation hurdles which have already been strived for?
6. What kind of reforms are required to effectively address terrorist content online in the EU? What are the next steps after the adoption of the Regulation (EU)/2021/784?

1.4 Research Objectives

The research objectives are the following:

1. To analyze the issues that the EU Member States face in defining the ambit and scope of provisions regarding the distribution of terrorist content online.
2. To assess the ways in which the EU Member States are monitoring and handling online terrorist content and related issues in the region.
3. To present and evaluate the EU Member States' strategies.
4. To assess the remedies and complaint procedures to address the distribution of terrorist content online under the Regulation (EU) 2021/784.
5. To explore the current implementation status and hurdles regarding the Regulation (EU) 2021/784.
6. To recommend reforms at administrative and legislative level in the EU for efficient mitigation of online terrorism and associated threats.

1.5 Research Methodology

This thesis undertakes a Qualitative research method. For this purpose, different books, articles, international and regional legislative instruments have been studied, analyzed and examined in order to reach to a certain conclusion.

Chapter 2: From Terrorism to Cyber-terrorism and the Way Towards the Adoption of the Regulation (EU)2021/784

2.1 Terrorism

The international community has frequently stated its opposition to all forms of terrorism.

Preventing terrorism and combating violent extremism and radicalization are necessary components of maintaining international peace and security. However, the international community and European Union in particular, also as part of NATO allies, and many other countries often seem to ignore terrorism's national, religious, or ethnic origins.

"Terrorism" is an ambiguous term. Bruce Hoffman[16] argues that while everyone understands what terrorism is, no one has agreed on a definition. The meaning of the term has evolved significantly during the last 200 years. The Latin word ´terror´ has been used as a political term since the French Revolution. Additionally, it has been used to refer to the Jacobins' state terrorism. It has since been used to refer to a variety of items in a variety of contexts. Voluntary activities by weaker governments to further the interests of larger ones (so-called "covert war"), as well as acts of violence committed by religious extremist organizations, are examples of what is called 'terrorism'.

Terrorism is a violent act. However, not all violent acts constitute terrorism. The primary difference between terrorism and other types of violence is that terrorism is committed for political purposes. For instance, "terrorism" is defined as "the deliberate slaughter of civilians or security forces for political purposes." Many acts of violence, even if no one is killed, can be categorized as terrorism. This is a succinct statement. Terrorism is a "crime." However, not all governments consider bombing, human trafficking, high jacking, bodily integrity breaches, and threats, as to be crimes. Terrorism is designed to tip the power balance in favour of a certain group. Terrorist groups are a sign of ineffective politics. These organizations are incapable of winning elections or exerting influence through peaceful protests, petitions, or non-governmental operations. They chose terrorism in order to get a large impact with a small budget. Terrorism occurs when individuals attempt to achieve political goals using unorthodox means. The effectiveness of this approach is contingent upon the use

[16] 'Bruce Hoffman | Council on Foreign Relations' <https://www.cfr.org/expert/bruce-hoffman> accessed 13 September 2022.

of contemporary communication technologies and media. It aims to strengthen a less powerful group over a more powerful one.

Terrorism is a psychological force multiplier. The objective is to create fear in others by the use of violence or threats of damage. The terrorists' goals are not limited to those harmed in the attack. Numerous people are terrified by a single person who is willing to die for his ideals. Terrorism requires a specific group of people to organize and commit a single attack. The global world has seen significant changes in terms of group organization. Groups can now be organized informally through the use of social media and the internet. Additionally, a single individual may assemble a group, resulting in a massacre, as was the case with the 2011 Norway assaults. Anders Behring Breivik allegedly released a manifesto on the internet titled "A European Declaration of Independence" eight hours before murdering people. He was charged with violating it. These definitions aid in our understanding of terrorism. Consider how the legal term "terrorism" is used. The law is the most effective and necessary means for preventing and punishing terrorism. In 1937, the League of Nations adopted a Convention against terrorism. This has been the first step toward defining terrorism at international level. Terrorism occurs when someone purposely causes or threatens to cause violence by the use of firearms, weapons, explosives, lethal devices, or hazardous substances, resulting in death or serious bodily injury, as well as severe property damage. This covers anybody who murders or injures another individual or group on purpose. It was ineffective. At the moment, the United Nations does not have a broadly acknowledged definition of terrorism. The UN frequently uses this word in its decisions and operations related to the war on terrorism. a snafu The Comprehensive Convention on International Terrorism has been negotiated since 1966, but no agreement has yet been reached owing to disagreements among United Nations member nations. The European Union is the first international body to define terrorism. This is not a significant problem, given the EU was founded to avoid bloody border clashes, most notably between Germany and France. The six founders sought to establish an effort that would contribute to Europe's security and peace. Decision No. 2 on the Framework (June 2002): The Council accepted this resolution in June, and the EU confirmed it in July. According to the Decision, significant national law offences include those that threaten to destabilize or destroy the core political, constitutional, economic, or social institutions of a country or an international organization. It not only defines terrorism in general for all member states, but also goes into detail on terrorist crimes and terrorist organizations.

"Terrorism, the calculated use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective. Terrorism has been practiced by political organizations with both rightist and leftist objectives, by nationalistic and religious groups, by revolutionaries, and even by state institutions such as armies, intelligence services, and police"[17].

"Terrorism is a destructive force, ignoring any nation, religion, or ethnic group". International law includes no universally accepted definition of terrorism. When someone refers to an act of terrorism as "terrorism," they are referring to the fact that it possesses certain characteristics of terrorism but cannot be justified as terrorism as of the absence of internationally recognized definition. However, it is controversial if certain types of violence are appropriate in particular settings without being classified as terrorism. In turn, an overbroad definition of terrorism can be used to suppress peaceful dissent and undermine democracy. A specific definition of terrorism is necessary to prevent terrorism in conformity with the rule of law and international human rights norms. Not only does it carry with it, terrible political and moral overtones. Additionally, the word has legal repercussions both domestically and internationally, including intelligence sharing, enlisting foreign help, freezing and seizing assets, and extraditing individuals.[18]

Terrorism can take place anywhere and in any form. A concerted effort to undermine democratic democracy, most notably through influence on politicians and lawmakers; and an indiscriminate targeting technique aimed to instill fear and terror in a society. Terrorist activities are criminal offences and will be prosecuted as such. Human rights standards apply regardless of whether an occurrence is classified as a terrorist attack or a serious criminal offence. The definitional difficulty of terrorism may be overcome by focusing on preventing and/or punishing terrorist activities. Even though the international community has not reached an agreement on a definition of terrorism, some behaviours constitute terrorist offences. They are now covered by 18 international treaties and conventions that the United Nations or one of its agencies has ratified. The UN Security Council asserts that terrorism consists of three components: criminal acts,

[17] 'Terrorism | Definition, History, & Facts | Britannica' <https://www.britannica.com/topic/terrorism> accessed 13 September 2022.
[18] Terrorism is a destructive force.

including those committed against civilians, with the intent of causing death or serious bodily harm or kidnapping; whether motivated by political, philosophical, ideological, racial, ethnic, religious, or other similar reasons, the objective is to instill fear in the general public or a group of people. On October 8, 2004, the United Nations Security Council adopted Resolution 1566 (2004). The first UN Special Rapporteur on the promotion and protection of human rights in the context of counterterrorism endorsed the resolution 1566 (2004) definition of terrorism. According to him, the resolution's first two criteria might be used to identify other types of behaviour. Domestic law should define "terrorism" and associated offences in non-discriminatory, non-restorative terms. Individuals should be able to grasp and interpret the laws that govern them. The police and judiciary should conduct themselves lawfully and plainly. This is a prerequisite for individuals to comprehend and obey the law. Additionally, it establishes the framework for effective and responsible counterterrorism action, including police action that adheres to the rule of law and international human rights norms.

2.1.1 Terrorist Threats and Concerns across the World

Europe has had to deal with a wave of terrorist threats. Foreign terrorist organizations, returning foreign fighters from Iraq and Syria, local terrorists, and Iran-backed terrorists all made threats against the United States. In spite of losing all of its land, ISIS displayed its might by assaulting and recruiting from European countries. The vast bulk of these atrocities took place in Western Europe and Russian Federation. In the vast majority of these cases, pedestrians were injured or killed by common items and cars.

The Syrian Democratic Forces (SDF) continued to retain a considerable number of FTFs from Europe in the closing months of 2019. European and other countries should return its nationals to the United States, as the United States has demanded. The bulk of Western European nations, excluding Ireland and Italy, did not penalize or repatriate their citizens, despite their affluence and well-developed legal systems. Citizens of some Western European countries who travelled to Syria or Iraq to join ISIS have been expelled from their country. Kosovo and Bosnia and Herzegovina, two Southeast European countries, were successful in repatriating substantial numbers of ISIS fighters, including foreign fighters from Syria.

The Kurdistan Workers Party (PKK) and the Revolutionary People's Liberation Party/Front continued to plan attacks against the Turkish police and military targets while seeking funding for their cause in other countries. Racial or ethnically motivated behaviour (REMT) like preparing assaults against the religious or other minorities has also begun in a number of European countries.

In 2019 and 2020, European countries took real steps to avoid terrorism supported by the Iranian regime. Albania, Denmark, and France severed diplomatic ties with Iran after the latter threatened to kill or bomb citizens of those nations. Tehran's terrorist capabilities are on full show in Europe's heartland. The United States formed the Countering Transnational Terrorism Forum (CTTF) in 2019 in response to Iran's terrorist ambitions in Europe. A worldwide network of law enforcement, prosecutors, and finance professionals has been developed to disrupt Iranian terrorist activity and networks. European nations continue to participate in the US-Europol Law Enforcement Coordination Group's (LECG) fight against Hizballah's terrorist and unlawful operations across the world. In the year 2019, the LECG met twice.

Many European governments are becoming worried about the threat that REMT poses. An attempted synagogue attack in Halle, Germany, in October 2019 showed that REMT offenders who utilize the internet and social media to distribute violent propaganda continue posing a threat. European governments stepped up their efforts to combat the threat presented by REMT individuals and organizations.

With regard to the war against terrorists, European countries played an important role in 2019. In order to defeat ISIS, a worldwide coalition of nations has formed. This alliance was founded by 39 European countries, the EU, Interpol, and NATO. Allies of NATO revised the NATO Counterterrorism Action Plan in December 2019. An important component of this plan is a tightening of cooperation between the United States and its NATO allies as well as other countries. ISIS-defeating coalitions in Afghanistan and Iraq, as well as NATO's Iraq mission, have finances remaining[19].

[19] 'Country Reports on Terrorism 2019 - United States Department of State' <https://www.state.gov/reports/country-reports-on-terrorism-2019/> accessed 13 September 2022.

2.2. Counter Terrorism

All government agencies must work together to counter this menace of terrorism. This is a difficult undertaking for anyone, let alone governments. When it comes to the EU, coordinating 28 institutions becomes substantially more difficult. The EU Counter Terrorism Coordinator, Gilles de Kerchove sees terrorism as the greatest danger to democracy. According to him, the act of terrorism is contagious. Viruses are difficult to eliminate because they are able to adapt to different surroundings and become more dangerous.

Terrorism must be prevented at all costs by eliminating the conditions that foster its development. There must be a multi-directional approach to countering terrorism. When fighting terrorism, it is critical to maintain the highest level of physical protection possible. Metal detectors at airports and retail centers as well as the protection of important infrastructure such as tunnels are all included in this effort. Data collection and analysis are essential if you want to do more to combat terrorism. Improved target recognition and resource allocation may be the result. Additionally, terrorist organizations are being undermined in order to deter their members from committing crimes. Stopping the flow of money to terrorists would be the most important priority in this circumstance. Criminalization of terrorist conduct and prosecution of terrorists are important components of counter-terrorism policies. Identifying and bringing criminals to justice would serve as a deterrent to future crimes. Terrorist-supporting governments and organizations are more likely to be punished by individuals who seek revenge. These countries should not be allowed to join international organizations or receive armaments from the United States as retribution. Terrorism is something that has to be prevented, protected from, pursued, and responded to.

The EU counter terrorism strategy policy and agenda, The European Union's Counter-Terrorism Strategy does not include "pre-emptive actions" like the United States implemented after September 11, 2001. If a state intervenes before anything horrible happens, it may be simpler. However, the Union may be unable to. For Europeans, pre-emptive responses may be too severe because of their preference for diplomacy and negotiations rather than forceful measures[20].

[20] Sinem Cevik, 'The Development Of The Eu's Counter Terrorism Policies In The Post 9/11 Era' 105.

Numerous occurrences on European soil throughout 2020 have served as a reminder of the danger terrorism still poses to the region. Following the recent spate of incidents in France and Austria, the EU and the UK have increased the threat level from terrorism and reviewed their existing legislation and counterterrorism strategies. A new "Counter-Terrorism Agenda" was released by the European Commission in December as part of the EU's response to the increased threat levels.

2.2.1. Strategic Approach to Countering Terrorism

Terrorists require a variety of resources to plan and carry out operations, including recruitment and sympathizers, cash, weapons, the freedom to travel freely, and hiding and communication locations. Thus, in order to prevent acts of terrorism, a diverse set of policies and procedures must be in place. The study entitled "Ten areas where best practices may be applied to combat terrorism" by United Nations Special Rapporteur, Martin Scheinin published on December 22, 2010[21]. When it comes to putting an end to terror, it is critical to understand the following: Strategic counterterrorism techniques frequently include a plethora of distinct objectives and cover a plethora of distinct phases in the growth of terrorism. Individuals who wish to prevent others from becoming terrorists, provide them with opportunities to do so, and assist them in escaping violent extremism and radicalization that lead to terrorism (VERLT). Additionally, they deny terrorist assistance, resources, and tools necessary to plan and carry out attacks. States have a responsibility to safeguard their citizens from acts of terrorism, which implies they should devote significant resources to preventing terrorism. Their international legal and political commitments reflect this. Actions to help prevent and defeat terrorism, as well as measures to make sure that the fight against terrorism is founded on human rights and the rule of law, are all things that the UN Global Counter Terrorism Strategy recommends.

The UN Security Council resolution 1373 (2001) mandates all governments to enact appropriate anti-terrorism legislation, rules, and institutions. These include the following: “abstain from providing any kind of assistance, active or passive, to entities

[21] Martin Scheinin and UN Human Rights Council Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, ‘Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin ’: <https://digitallibrary.un.org/record/704287> accessed 13 September 2022.

or persons involved in terrorist actions; Prevent and repress terrorism funding; suppress terrorist recruitment; and eliminate the supply of weapons to terrorists".

Additionally, they seek to deny safe havens to those who finance, plan, assist, or perpetrate terrorist actions, as well as those who supply safe havens. They seek to ensure that anyone who assists in financing, planning, supporting, or carrying out terrorist activities gets prosecuted. Furthermore, State governments must ensure that any action taken to combat terrorism complies with international law, particularly human rights, refugee, and humanitarian law as stated in Resolution 1456 and on subsequent UN Security Council decisions[22].

2.2.2. Terrorism and Counter-Terrorism Instrument Policies at the EU Level

Terrorism poses a significant threat to the safety of European citizens. The number and severity of terrorist acts in the European Union have increased in recent years. Recent years have seen an increase in the number of terrorist cases managed by Eurojust's National Members and Liaison Prosecutors. This includes the terrorist attacks on the Thalys train in Paris and Saint-Denis, as well as on the Thalys trains in Brussels, Zaventem, and Nice. Terrorist groups are becoming increasingly organized and acting across the borders, making it more difficult for national authorities in Member States and third countries to put an end to terrorism. The unpredictable nature of "lone-actor" terrorism complicates national governments' response to terrorist attacks. While the possibility of mass-casualty terrorist strikes directed by international organizations in Europe has diminished, the threat remains more deadly than ever in many ways. Lone-actor attacks driven by a variety of beliefs and frequently involving mental health issues are growing more prevalent, and it's becoming more difficult to identify and stop them. On the other side, the development of the extreme right is beginning to resemble militant Islamist groups. Terrorism takes numerous forms, but it continues to have a significant impact on European identity and liberal ideals. It occurs against the backdrop of widespread anti-immigrant sentiment and political divisiveness[23].

[22] Organisation für Sicherheit und Zusammenarbeit in Europa and Office for Democratic Institutions and Human Rights (eds), *Preventing Terrorism and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Community Policing Approach* (OSCE 2014).

[23] The Evolving Terrorism Threat in Europe | Current History | University of California Press' <https://online.ucpress.edu/currenthistory/article-abstract/121/833/102/120172/The-Evolving-Terrorism-Threat-in-Europe?redirectedFrom=fulltext>

Furthermore, the European Judicial Counter-Terrorism Register was developed by Eurojust to gather information on judicial counter-terrorism cases from all EU Member States and to explore any linkages to other cases in the same country. Through judicial cooperation and with the help of Eurojust, governments can ensure that terrorist attack victims are protected, their rights are maintained, and they receive the aid they need to recover from their trauma. This agency is also involved in international cooperation in the battle against specific threats, such as the repatriation of European FTFs (Foreign Terrorist Fighters) to their homeland[24].

Due to the fact that acts of terrorism are regularly carried out across national borders, international judicial cooperation is essential. We must work together to stop terrorist attacks, catch those who instigate them, and track down the people who support them, as well as to find out what triggers their behaviour in the first place and treat those issues. By coordinating investigations and prosecutions and encouraging judicial cooperation in cross-border terrorist matters, Eurojust aids national authorities. The Agency helps law enforcement and judicial professionals accomplish their duties more efficiently by establishing and maintaining joint investigation teams (JITs), organizing coordination meetings and coordination centers, and organizing joint action days. An SNE (Seconded National Expert) on terrorism aids Europol's European Counter Terrorism Center (ECTC) in the field.

This is how Eurojust assists the EU and its network of Justice and Home Affairs (JHA) agencies in collaborating more effectively in the fight against terrorism through the courts. These measures include enhancing data interchange, determining how to deal with returning foreign terrorist fighters (FTFs), and assisting victims of terrorist acts. Additionally, it communicates what it learns about different behaviour of terrorism by working with national authorities to assist them in combating terrorism, as well as the findings of its research, with those who work in the field, as well as with EU and national officials and parliamentarians. Sharing experiences and discoveries enables people to gain a better understanding of the issues confronting judicial authorities. Additionally, it enables the EU to collaborate on developing a unified approach to

[24] 'Terrorism | Eurojust | European Union Agency for Criminal Justice Cooperation' <https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/terrorism> accessed 13 September 2022.

prosecuting terrorism-related offences in order to avoid trying individuals in many countries concurrently[25].

Europol, the European Union's law enforcement agency, publishes an annual report about the terrorist threat in Europe and the changes that have occurred over time, including *inter alia*, information about terrorist attacks and arrests related to terrorism in the European Union. It is based on data provided by EU member states.

The annual EU Terrorism Situation and Trend Report (TE-SAT) published by Europol provides an assessment of the terrorism situation and trends in the EU over a given year. Europol's efforts to combat terrorism include the deployment of TE-SAT, which is one of their most critical pieces of strategic analysis. It provides information about terrorism in the EU to law enforcement officers, policymakers, and the general public, as well as information about emerging trends in this crime area that Member States provide to Europol. Europol has produced the study annually since 2007 to demonstrate how terrorism has evolved and remained constant. Several of these factors may evolve or vanish over time as politics or socioeconomics change; meld with other ideas or beliefs; or serve as the building blocks for new and occasionally unique and very individual motives[26].

Between 2018 and 2020, a large number of persons were detained in EU countries for terrorism-related activities, while another 739 were arrested in the UK. In 2020, the most often arrested offence was membership in a terrorist group, followed by spreading terrorist propaganda, planning terrorist attacks, and aiding and financing terrorism[27].

The Objective of the EU Counter-Terrorism Strategy

The EU counterterrorism policy was agreed by the council in 2005 to combat terrorism globally and make Europe safer. Fighting terrorism is a critical priority for the EU, EU Member States, and the EU's allies as deadly terrorist attacks continue to target people in Europe and beyond. The European Parliament and the Council are empowered to

[25] ibid.

[26] 'EU Terrorism Situation & Trend Report (TE-SAT)' (*Europol*) <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> accessed 13 September 2022.

[27] 'Terrorism in the EU: Facts and Figures - Consilium' <https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/> accessed 13 September 2022.

propose minimum standards for the definition of particularly serious crimes with a cross-border component, such as terrorism, under Article 83 TFEU.

Objectives

The approach concentrates on four priorities (pillars): "anticipate, prevention, protection, and response" in order to effectively combat terrorism. The strategy acknowledges the value of collaboration with non-EU nations and international organisations across these pillars.

Prevention

The EU's top objective is to address the factors that lead to radicalization and the recruitment of terrorists. By understanding the tactics, messaging, and tools utilised by terrorists, the "prevention" pillar seeks to prevent radicalization and the recruitment of terrorists. The EU facilitates information sharing, good practise determination, and coordination of national policy. The EU's policy to combat radicalization and terrorism recruiting, which was updated in 2014, attempts to do so while taking into consideration emerging trends including lone-wolf terrorism, foreign fighters, and terrorists' use of social media. It has been further modified by a series of Council conclusions on responding to terrorist attacks on EU soil.

Examples of ongoing work in the area of countering violent radicalisation are:

- the Radicalization awareness network
- follow up on the High-Level expert group on radicalization
- An example of ongoing work in the area of countering radicalization online is
- the progress made by the EU internet Forum underpinned by the recommendation on tackling online content specific focus on terrorist content.

Protection

The second aim of the EU counterterrorism strategy is protecting infrastructure, minimising vulnerability to attacks, and safeguarding citizens. As part of this, efforts

should be made to secure external borders, enhance transportation security, safeguard key targets, and lessen the vulnerability of vital infrastructure[28].

2.2.3 Counter-Terrorism Instruments at the Level of the Council of Europe

The Committee of Ministers and the Parliamentary Assembly endorse the primary tools used to combat terrorism. The Committee of Ministers is the official decision-making and treaty-adoption body of the Council of Europe (CoE). It is composed of Foreign Ministers from Member States. The Council of Europe's Parliamentary Assembly (PACE) is the body that issues non-binding recommendations, resolutions, and views. It possesses no authority. The CoE's primary objectives in combating terrorism are to strengthen the legal framework, combat the causes of terrorism, and safeguard fundamental values. Both committees must monitor the anti-terrorism policies and practices of the state parties.

The CoE has employed a variety of strategies in the fight against terrorism. Its primary anti-terror treaty is the Council of Europe Convention on the Prevention of Terrorism, which was signed on May 16, 2005[29], and entered into force on June 1, 2007. It overrides the previous European Convention on Terrorism Suppression. (Approved 27 January 1977; became effective 4 August 1978). The Convention's overall objective is to enhance the effectiveness of current international anti-terrorism treaties. Additionally, it aims to assist Member States in combating terrorism by criminalizing certain acts that potentially result in terrorism: public provocation, recruiting, and training. Additionally, it wishes to assist Member States in collaborating to combat terrorism both within and across borders (modification of existing extradition and mutual assistance arrangements and additional means)[30].

[28] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond 2020.
[29] '16808c3f55.Pdf' (n 4).
[30] ibid. Preamble

2.3. Cyber Terrorism

Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives[31].

Attacks on computer networks are committed by terrorists to wreak havoc and bring down entire governments. What are the chances of anything like this actually happening? In this essay, we examine the rise of cyberterror and the evidence that might be utilized to foresee an oncoming disaster. Cyberterrorism because of a combination of psychological, political, and economic factors cause increasingly fears[32]. Computer phobia and skepticism go hand in hand because of our shared dread of unpredictable, violent attacks. There is a problem, and it is just going to get worse. This means that handling the danger without inflating it is considerably more important.

Cyber-terrorism occurs when individuals use computers and other technology to inflict injury or destruction in order to coerce others into doing things they do not wish to do or to alter how the government operates and more importantly, through cyber space, terrorist make use of it for the recruitment from all over the world, giving recruits training online for certain acts of violence or terrorism, and also to get fundings for terrorist attacks. Additionally, cyber-terrorism, which should be distinguished from hacktivism and cyber-warfare, include the destruction of key infrastructure. There are numerous parallels and distinctions between cyber-terrorism and terrorism in general, all of which relate to how counterterrorism measures are conducted in both circumstances.

Computer networks can be used to harm or shut down government entities in cyberterrorist attacks (such as energy, transportation, government operations). Governments and critical infrastructure now confront new concerns as they become more reliant on digital networks. In cyberterrorism, "a gigantic electronic Achilles' heel" is the foundation. Cyberterrorism is attractive to modern terrorists because of its anonymity, damage, psychological effects, and media prominence. Cyberterrorism is a matter of concern for the media, security agencies, and the IT industry since it might affect the country and its population. If you are a skilled hacker, you may inflict havoc

[31] 'Statement of Dr. Denning' <https://irp.fas.org/congress/2000_hr/00-05-23denning.htm> accessed 13 September 2022.
[32] Gabriel Weimann, 'Cyberterrorism How Real Is the Threat?' 12.

on critical infrastructure like dams and air traffic networks, potentially putting millions of lives at risk. A cyber-created catastrophe has been predicted, although no real incidents of cyberterrorism have been found[33].

How real is the threat of cyberterrorism? In Western countries, cyberterrorism is a major issue since most important infrastructure is computerized. It has been demonstrated by terrorists that anybody can get their hands on crucial information and disrupt important systems. While it is possible for hackers to target industrialized economies such as the United States' military, financial, and service industries, terrorists may hypothetically follow in their footsteps. Our societies become increasingly vulnerable as they become more reliant on information technology. Terrorists can now reach previously inaccessible targets such as the national defense and air traffic control systems. Cybercriminals are more likely to target citizens in more technologically advanced countries.

The threat of cyberterrorism is real. Concerns have been voiced in the media, in Congress, and in other places. This does not mean they are all sane, though. Nonsense scares some people, while others are more wary of it. Many individuals failed to notice that cyberterrorists were capable of far more than was realized. Internet is being used by international terrorists to recruit terrorists online by using chat rooms, websites and servers. They used social media platforms to propagate their manifesto and spreading their teachings in favor of extreme acts and also to gain sympathies by posting videos and photos of attacks by foreign forces. Terrorists' organizations are also seeking abilities to make usage of internet as a weapon to damage critical infrastructure of governments such was in the case of Bali attacks in 2002 where Indonesian Police believed that attacks were supported through online credit card fraud(Theohary 2011)[34].

In the following analysis, the term "cyberterrorism" is further defined, and the history of the phenomenon is traced. Subsequently, this master thesis examines the Western world´s reaction to cyberterrorism. More specifically, it looks at current studies and publications to evaluate if people's anxieties about cyberattacks are legitimate. Lastly,

[33] ibid.

[34] Catherine A Theohary, *Terrorist Use of the Internet: Information Operations in Cyberspace* (DIANE Publishing 2011).

it is concluded that while we should be aware of potential dangers, we should not let our fears govern our actions[35].

2.3.1. International Cooperation Towards Countering Cyber Terrorism

There are numerous strategic reasons why terrorist groups and their sympathizers are increasingly utilizing the internet for a variety of purposes, including recruitment and fundraising. One of these strategic factors is technological advancements. While the Internet's numerous benefits are obvious, it may also be used by terrorist groups to communicate, disseminate information about, and solicit support for, planned terrorist operations. Thus, the respective criminal offenses require specialized technological skills on the part of law enforcement agencies. At the same time, regardless of the gravity of their offences, alleged terrorists should be afforded the same procedural protections under criminal law as other suspects. This is a critical component of the rule of law in the war on terrorism. Human rights and fundamental freedoms must be observed at all times, including when developing and implementing legislative instruments to combat terrorism.

Using the Internet for terrorist objectives is on the rise, which necessitates a coordinated response from all Member States. Assistance is provided to members of the United Nations Office on Drugs and Crimes (UNODC) in strengthening their criminal justice systems' ability to comply with international legislation against terrorism. International human rights and recognized legal standards guide the UNODC's activities.

There is currently no worldwide legislation specifically addressing this widespread phenomenon. Additionally, there is a dearth of specialized training on how to investigate and prosecute incidents of terrorism including the use of the Internet for terrorist purposes. The UNODC has already committed significant resources in combating terrorism and cybercrime. Additionally, it discusses the importance of having integrated, specialized knowledge to assist its members in combating this ever-changing danger. It was made possible with the assistance of the Great Britain’s and Northern Ireland's government. UNODC is extremely appreciative. The document[36] on the use of Internet for Terrorist Purposes by the United Nations Office on Drugs and Crime, which can be utilized alone or in conjunction with UNODC capacity-building

[35] Gabriel Weimann, ‘Cyberterrorism: The Sum of All Fears?’ 21.
[36] ‘The Use of the Internet for Terrorist Purposes’ 158.

efforts, provides guidance on how to handle terrorist situations involving the Internet[37]. Additionally, it provides information about how the law and practice operate in various countries and regions around the world[38]. Terrorism, in all of its manifestations, impacts everyone. The use of the Internet to assist terrorists circumvents national borders, which may have a greater impact on those harmed.

2.4. Terrorist Content Online and Global Increase in Terrorist Content Online and Recent Problems Due to Terrorist Content Online in the EU

Governments' concerns about terrorist content online have increased significantly over the last four years, as have efforts to regulate the Internet. At Tech against Terrorism, they work with technology firms ranging from social media platforms to smaller file-sharing sites, messaging applications, and financial technology platforms to assist them in responding to terrorist propaganda while respecting fundamental human rights[39].

Current initiatives vary from content removal requests within a limited period of time to compensation for automated content management practices. While these efforts have the potential to alter some of the norms governing the Internet and online speech, they may fall short of preventing terrorist propaganda online. Additionally, a number of the approaches considered might have an effect on freedom of speech, the rule of law, sectorial competitiveness and innovation. The issue is that democratic governments may set an unfavorable precedent in this regard.

2.4.1. Terrorist Content Online

The term “Terrorist contents online” stands for those contents which are disseminated by terrorists or their organisations such as ISIS or Al-Qaeda, over the Internet for various purposes: e.g., recruitment of people to enlarge their armies, radicalisation of individuals to prepare them to do certain acts which they consider as Holy acts, fundraising for their organisations to help them achieve their goal or for the spread of their message all over the world. The continuous existence of terrorist content online poses a serious risk to both individuals and society as a whole. Terrorists are using the

[37] ibid. pg 12
[38] ibid. pg 22-23
[39] ‘About Tech Against Terrorism - Tech Against Terrorism’ (4 September 2017) <https://www.techagainstterrorism.org/about/, https://www.techagainstterrorism.org/about/> accessed 13 September 2022.

Internet because of its versatility and availability to everyone around the world. By using different platforms such as Facebook, Twitter or Youtube, terrorist can spread their message globally just by striking one key and without being exposed. These types of contents are available in form of videos, audios or written texts and their detection often cause difficulties to law enforcement agents.

The purpose of the Internet is not what terrorist are using it for. The Internet boost digital economy by connecting the world at one place and having views and information from all around it. Nonetheless, it can also be abused for illicit purposes, including (but not limited to) terrorism. This is problematic for citizens, businesses and societies as a whole. Against this backdrop, online platforms become the target in the fight against online terrorism. Offering the channel for terrorist content to be spread, online services providers become co-responsible for tackling illegal content disseminated through their platforms.

"The European Commission has enacted the Regulations (EU) 2021/784 to make Hosting Services Providers (HSPs) and Internet Services Providers (ISPs) responsible for the quick removal or disabling access to online terrorist content so as to stop further dissemination of such content. Among other responsibilities, the Regulation ask for putting in place an effective safeguard to avoid unintended removal, develop new tools and technologies to automatically detect and removal of terrorist content, to stop proliferation of terrorist propaganda online"[40].

2.5. The Role of EU Internet Forum

Since 2015, people from the EU and EFTA (European Free Trade Association) countries, as well as people from other countries, like the members of the Global Internet Forum to Counter Terrorism, have come together to talk about how to prevent people from becoming radicalized. Those created the EU Internet Forum, namely a place where people can talk about how terrorists use the Internet and how to stop child sex abuse in the online world.

Trying to combat terrorist content on the internet will need more coordination between the private sector and government agencies in addition to compliance with regulatory

[40] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance).

requirements. The voluntary agreements reached by the EU Internet Forum (EUIF) have had a range of implications. The EUIF also contacted a variety of other service providers, including Facebook, YouTube, Microsoft, Twitter, the Internet Archive, Justpaste.it, Wordpress, Snap, Soundcloud, Baaz, Dropbox, Mega, Userscloud, and Telegram[41]. The EUIF established more specific terrorism-related reporting metrics. Platforms include reporting tools. On the other hand, not every business gives information on terrorism. According to the European Commission, public-private cooperation at the EU Internet Forum is anticipated to continue, if not grow, in the future. To prevent violent extremism, both technology companies and governments have committed to collaborating to develop anti-extremism solutions. However, both IT companies and the European Commission argued that maintaining or expanding the voluntary method would be insufficient to tackle terrorist content.

Social media companies will be compelled to take proactive measures, such as the deployment of new technologies, to better protect their platforms and users from terrorist exploitation, based on the likelihood that terrorist content would be disseminated over their platforms. If firms invest in new technology to detect and remove terrorist and violent extremist information, it would have to be taken from the internet[42].

The following steps have been taken to cut down on the amount of terrorist material that can be found on the internet: The EU Internet Referral Unit (EU IRU)[43] in Europol refers terrorist content to more than 300 platforms and talks to businesses in an effort to make them more resistant to propaganda from terrorist groups. This is what happened after the March 2019 attack in Christchurch, New Zealand. The EU Internet Forum also approved the EU Crisis Protocol (EUCP)[44] to make sure law enforcement and industry can work together and share information in times of crisis. A group called the Civil

[41] 'European Union Internet Forum (EUIF)' <https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en> accessed 13 September 2022.
[42] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 2018.
[43] 'Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda' (*Europol*) <https://www.europol.europa.eu/media-press/newsroom/news/europol's-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda> accessed 13 September 2022.
[44] 'EU Internet Forum Committed to an EU-Wide Crisis Protocol' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009> accessed 13 September 2022.

Society Empowerment (CSEP)[45] has been set up by the European Commission, in order to help civil society's positive voices be heard on the Internet, so it has given 10 million euros in action grants. The Radicalization Awareness Network (RAN) and online platforms like Facebook, Google, and Twitter are part of the program. It aims to make sure that the organizations have the skills and knowledge to run effective online campaigns that reach vulnerable people and those at risk of radicalization and recruitment by extremists[46]. The EU Internet Forum also helped drafting Regulation to stop dissemination of online terrorist content.

2.6. The Way Towards Adopting the Regulation (EU) 2021/784 and the Regulation´s contents in a nutshell

Terrorist groups have become more and more likely to use the internet to spread their propaganda and recruit new followers in recent years. Even though the general public's fear of terrorist attacks puts a lot of pressure on policymakers, politicians also use this anxiety to make the internet more secure and show that they are capable and concerned in the respective matters. The European Commission has enacted a new law to stop terrorist content from being spread on the internet. This is the latest example of election-motivated policy making, and it shows how the European Commission keeps making "solutions" to terrorist propaganda on the internet.

The Effectiveness of Content Removal

Many individuals believe that social media corporations are not doing enough to purge their platforms of extreme information. However, owing to automatic identification and removal, technology companies are already eliminating extremist information at a high rate. Additionally, several social media corporations have been able to reduce the popularity of certain extremist organizations by removing their profiles and material. For instance, in 2018, Facebook removed the information of the terrorist organization Britain First[47]. However, technological and definitional challenges significantly affect

[45] 'Civil Society Empowerment Programme' <https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/civil-society-empowerment-programme_en> accessed 13 September 2022.
[46] 'European Union Internet Forum (EUIF)' <https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en> accessed 13 September 2022.
[47] 'Facebook Bans Britain First and Its Leaders | The Far Right | The Guardian' <https://www.theguardian.com/world/2018/mar/14/facebook-bans-britain-first-and-its-leaders> accessed 13 September 2022.

the effectiveness of content removal, making the European Commission's recommended measures difficult to implement. While automated systems for detecting extremist information online are promising, they frequently generate a high number of false negatives and positives due to the massive volume of fresh content published to social media each day. Indeed, even the resource-intensive systems now in place on the largest social media sites are unlikely to be sufficient to keep terrorist propaganda out without also banning legal content, particularly during the one-hour interval provided for in the new legislation. Individuals who work for small enterprises that lack the resources to engage human moderators are even less likely to be precise when removing material or responding fast to complaints made via the suggested system for restoring content that has been wrongly deleted[48].

Regulation (EU) 2021/784

The "Regulation 2021/784 on Addressing the Dissemination of Terrorist Content online"[49] was "born" in the aftermath of the Commission´s Communication[50] on tackling illegal content online in September 2017 and the Commission´s Recommendations[51] on measures to effectively tackle illegal content online, in March 2018. And it primarily aims to stop terrorist content from being spread online.

The Regulation has laid down rigid rules regarding the misuse of hosting services to disseminate terrorist content online to the public. Notably, the Regulation regulates, the application of due care and measures to be taken by the hosting service providers (HSPs) and Member States respectively for the identification and quick removal of terrorist content online, and to cooperate with each other and with Europol[52].

[48] 'Against the Clock: Can the EU's New Strategy for Terrorist Content Removal Work?' <https://www.rusi.orghttps://www.rusi.org> accessed 13 September 2022.
[49] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance).
[50] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond (n 28).
[51] 'COMMISSION RECOMMENDATION (EU) 2018/ 334 - of 1 March 2018 - on Measures to Effectively Tackle Illegal Content Online' 12.
[52] See Article 1(1)(a)(b) of the Regulation (EU) 2021/784

Materialistic Domain ("terrorist content");

The Regulation provided for the material that will fall under the domain of terrorist content and has embraced the definitions of terrorist offences laid out in the Directive (EU) 2017/541[53] on combating terrorism and makes use of them for preventive purposes. The material that directly or indirectly; ask someone to commit or to assist to terrorist offences or to participate in activities of a terrorist group, ignites or advocates terrorist offences, like the glorification of terrorist acts[54]. Provides directions on how to conduct attacks[55].

Material can be in a form of text, images, sound recordings, videos, and live transmissions of terrorist offences, which cause a danger of further such offences being committed[56].

This Regulation provided for the exception related to such material is that; "Material disseminated for educational, journalistic, artistic or research purposes or for the purpose of preventing or countering terrorism, will not be considered to be "terrorist content"[57].

Applicability;

> The Regulation is applicable to all hosting service providers those who are offering services in the EU, no matter of the place of their main establishment[58]. HSPs are providers of information services which store and spread information to the public and material provided by user of the service on request, irrespective of whether the storing and dissemination to the public of such material is of a mere technical, automatic and passive nature. Such platforms can be social media, video image and audio-sharing services. Whereas, interpersonal

[53] 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 (n 6).
[54] See Article 2(7a-7b) of the Regulation
[55] See Article 2(7d) of the Regulation
[56] See Recital 11 of the Regulation (EU) 2021/784
[57] See Article 1(3) of the Regulation (EU) 2021/784
[58] See Article 1(2) of the Regulation

> communications services such as private messaging or emails will remain outside of the applicability domain of this Regulation[59].

The One-hour rule;

> "The Regulation stressed on removing terrorist content as early as possible to avoid its further spread. Hence, HSPs will be obliged to stop the dissemination of such content as early as possible and in any event within one hour"[60].

Issuance of Removal Orders;

> "The competent authority of each EU Member State has the power to issue a removal order directly requiring HSPs to remove or disable access to terrorist content in all Member States"[61]. "HSPs must designate or establish a contact point for the receipt of removal orders by electronic means and ensure their expeditious processing"[62]. For the purpose of issuance of removal orders, the competent authority must fill in all the necessary information for HSPs, the templates[63], established the Regulation[64].

The EU is about to extend its upload filter regime for copyright to content[65] that is linked to terrorism. This is a big problem for the way the internet works and is free. As a whole, making internet companies keep track of everything we say online is bad for our freedom of speech and could lead to a lot of people getting arrested.
In sum, the Regulation ensures that there are clear and transparent rules in place as to how to deal with terrorist content online across the EU. In parallel, it puts in place strong safeguards to make sure that people´s freedom of expression and information are fully

[59] See Recital 14 of the Regulation (EU) 2021/784
[60] See Article 3(3) of the Regulation
[61] See Article 3(1) of the Regulation
[62] See Article 15(1)
[63] See Annex I of the Regulation (EU) 2021/784
[64] 'Regulation Addressing the Dissemination of Terrorist Content Passed' <https://eucrim.eu/news/regulation-addressing-the-dissemination-of-terrorist-content-passed/> accessed 21 November 2022.
[65] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market 2016.

protected[66]. The most important provisions out of those summarised above will be presented in detail in the following chapters of this thesis.

[66] 'Terrorist Content Online' <https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_en> accessed 13 September 2022.

Chapter 3: Other measures of EU and its Member States to Manage Illegal (Incl. Terrorist) Content Online and Expected Success of the Strategies in Reducing the Impact of Terrorist Content Online

3.1. EU wide Actions to Make Internet a safer (and terror-free) space

3.1.1 The Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online

The persistent existence of terrorist content online poses a serious risk to both individuals and society as a whole. The European Union space has a history in the application of soft law or self-regulatory framework. From 2008, efforts were made to make internet a safer place.

In 2008 "Social Networking Task Force" held meetings with regulators, social networking groups such as Facebook, YouTube or MySpace and academic experts. In result of this process, "Safer Social Networking Principles for the EU" were created to minimise the risk attached with social networking for children by means of upgraded privacy settings and safety of information. Furthermore, in 2010, The UK, Germany, Netherlands, Belgium and Spain sponsored "Clean IT" project by European Commission, which would make ´principles and practices´ to combat terrorist content and illegal use of internet(Gorwa 2019)[67].

In order to recruit supporters, organize terrorist operations, and create fear, terrorist organizations increasingly turn to the Internet. There were several voluntary actions performed before the Regulation 2021/784 passed. Given the limits of these actions, the Member States encouraged the EU to do more. Proposals were created to make it simple to identify who is in charge of erasing material in order to prevent people's rights from being abused. The European Commission has also proposed a number of voluntary and statutory actions and efforts to address the terrorist threat. This initiative was associated with concerns that the efforts to remove illegal content from the Internet are not going far enough and to address issues such as incitement to terrorism, illegal

[67] 'Gorwa - 2019 - The Platform Governance Triangle Conceptualising .Pdf' <https://web.archive.org/web/20200506195742id_/https://www.econstor.eu/bitstream/10419/214074/1/IntPolRev-2019-2-1407.pdf> accessed 13 September 2022.

hate speech, child pornography, infringements of intellectual property rights, and consumer protection, making an EU-wide coordinated approach necessary. The Commission issued a recommendation regarding how to handle terrorist content effectively. This Recommendation[68] formalizes a previous communication's[69] political commitment to combating online terrorist content, but it is not legally binding.

The Commission is continuously studying the matter of handling illegal content on online platforms and has already organized a series of seminars with industry. These interactions have played vital role in providing input to the Recommendation. In 2018, a number of Commissioners met with Internet platforms[70] to ascertain their commitment to combatting illegal content and the implementation of the communication for the removal of illegal content. The plan towards the removal of online content from Internet strictly complies with the Copyright Directive[71], especially on contentious matters such as the responsibility of online platforms. Additionally, it is perfectly consistent with the Audio-Visual Media Directive's[72] rewriting. The Commission suggested conducting an early impact evaluation of measures aimed at boosting the battle against illegal online content. The impact study was conducted[73] using the findings of an open public consultation on additional ways for combating unlawful material online. To further tackle dissemination of illegal content online, the Commission has proposed newer legislations, such as The Digital Services Act, to set accountable and transparent standards for the online services providers and make them more responsible for the contents posted on their platforms.

---

[68] 'COMMISSION RECOMMENDATION (EU) 2018/ 334 - of 1 March 2018 - on Measures to Effectively Tackle Illegal Content Online' (n 51).

[69] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling Illegal Content Online Towards an enhanced responsibility of online platforms 2017.

[70] 'Tackling Illegal Content Online – Meeting with Online Platforms of 9 January 2018 | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/tackling-illegal-content-online-meeting-online-platforms-9-january-2018> accessed 13 September 2022.

[71] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) 2019.

[72] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) 2010.

[73] 'Summary Report of the Public Consultation on Measures to Further Improve the Effectiveness of the Fight against Illegal Content Online | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal> accessed 13 September 2022.

3.1.2. The Digital Services Act

The European Commission has proposed a Digital Services Act (DSA) in December 2020, in order to tackle illegal products, services, and information on the internet (DSA). The E-Commerce Directive does not oblige online intermediaries and also prohibit Member States to impose obligation to monitor information they provide to protect users' fundamental rights[74]. There was a need to revise such legislative instruments to further control the spread of online hate material, which was not possible due to the existence of such freedom provided by the E-Commerce Directive to online intermediaries as internet and online business models have changed and the dissemination of online illegal content has increased. For that, the DSA was proposed to provide evidence-based rules to make internet intermediaries legally certain and accountable and responsible for digital services. The DSA would bring major changes because of its material and territorial scope, such as, drafted rules will be applicable to online intermediaries as per their services, categories and size in the online space[75] and will be applicable to all service providers providing services in EU whether established in or outside of EU[76]. The DSA will oblige intermediary services providers to ensure transparency, protection of fundamental rights and to act responsibly in enforcing restrictions on the use of their services such as algorithmic decision-making Review[77]. Intermediary service providers have to report on disabling or removing of information considered illegal or contrary to terms and conditions set by providers[78] and they have to make single point of contact for the direct communication with authorities of Member States and in case of establishment established outside of the EU, have to designate their legal representative in the EU[79].

The Commission proposes in DSA draft, taking into consideration about protection of user rights and fighting against illegal content online, notice, action and sufficient appeal mechanism for online platforms and hosting service providers. They have to place notice and action mechanisms to enable third parties for the notification about the presence of illegal content and to provide statement of reason in case of decision they make for the removal of disabling access to specific information[80]. Proposal has

[74] See Article 15 of the E-Commerce Directive
[75] Article 2 of the Proposed DSA
[76] Article 1 of the Proposed DSA
[77] Article 12 of the Proposed DSA
[78] Article 13 of the Proposed DSA
[79] See Also Article 10 and 11 of the Proposed DSA
[80] See Also Article 14 and 15 of the Proposed DSA

introduced new term of Trusted Flaggers they will be appointed by Member State authorities and will be comprises of competent experts in dealing with illegal online content and will be given priority by online platforms in case of notices received by trusted flaggers.

Furthermore, proposed regulation will oblige very large online platforms (VLOPs) as a whole due to their impact on society, economy and responsibility with regard to the spread of illegal content online. The Proposal provided high standards of responsibility and accountability to such large platforms for their content moderation(Madiega 2020).

3.2 Measures to Handle Illegal (incl. Terrorist) Content Online at EU Member States Level

Different EU Member states like France and Germany have taken steps to combat all forms of terrorism even before the adoption of the Regulation (EU)2021/784, because of continuous terrorism acts and threats. These efforts also include measures to counter the dissemination of terrorist content in the online world. Such measures, which are to be presented below, are limited to territorial jurisdiction with the evolving threat of cyber terrorism having, however, to be tackled beyond national borders considering the border-less nature of the Internet.

3.2.1. The Case Study of Germany

Improvements have been seen in Germany after 2015 in blocking or taking down illegal content online. Germany introduced the "Network Enforcement Act, NetzDG"[81] incentivizing tele-media services (social networks) providers to take steps to block, take down or filter illegal content. The NetzDG defines various content that are to be deemed unlawful[82] and encompasses offences under the German Criminal Code including the formation of a terrorist organization[83] and the defamation of religion[84].

[81] 'Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)' (*Bundesministerium der Justiz*) <https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.html> accessed 13 September 2022.

[82] '§ 1 NetzDG - Einzelnorm' <https://www.gesetze-im-internet.de/netzdg/__1.html> accessed 13 September 2022.

[83] 'German Criminal Code (Strafgesetzbuch – StGB)' <https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1310> accessed 13 September 2022.

[84] See Section 166 of German Criminal Code

NetzDG provides to remove or to block the access to content within 24 hours of receiving complaint, the content that is manifestly unlawful[85], and oblige social network providers to provide their users with a procedure of complaint submission about easily, directly accessible or recognizable illegal contents[86]. The NetzDG applies to profit-making tele-media services providers that allow their users to share any content with others and to social network providers who have more than two million users in Germany[87].

The German Government argued in support of NetzDG by presenting transparency reports of not have evidence of over-blocking. In the views of the German Ministry of Justice and Consumer Protection, companies are able to examine online contents reported by users quickly and thoroughly. The scope of NetzDG is not limited to blocking or removing contents related to terrorism, but it is expanded to expanded to taking down illegal content online[88].

3.2.2. The Case Study of France

France seems to be very keen in fighting against terrorism of any kind, which depicts of his being a party to all those Conventions of Council of Europe that govern internet. France has ratified Convention on the Prevention of Terrorism of Council of Europe in fight against terrorism.

In the fight against online terrorism, France has various laws and regulations enabling filtering of websites, removal or taking down of unlawful contents from websites. The most important French law of this kind is the Law No. 2004-575 of 21 June 2004, Law for Trust in the Digital Economy (LCEN) which was supplemented by Law No. 2014-1353 of 13 November 2014 to bolster counter terrorism provisions. The LCEN in its Article 6.1.8 explained that judicial authority upon application may require that hosting service or by default the online public communication access provider take any appropriate measures to prevent damage or harm resulting from an online public communication service[89]. By virtue of new provisions introduced by French legislature

[85] '§ 3 NetzDG - Einzelnorm' <https://www.gesetze-im-internet.de/netzdg/__3.html> accessed 13 September 2022.
[86] See Section 3(1) of NetzDG
[87] Matthias C Kettemann, 'FOLLOW-UP TO THE COMPARATIVE STUDY ON "BLOCKING, FILTERING AND TAKE- DOWN OF ILLEGAL INTERNET CONTENT"' 12.
[88] William Echikson and Olivia Knodt, 'Germany's NetzDG: A Key Test for Combatting Online Hate' (22 November 2018) <https://papers.ssrn.com/abstract=3300636> accessed 13 September 2022.
[89] See also Article 6.1.8 of LCEN

in the LCEN in 2014, websites spreading images constituting a criminal offence under the legislation relating to incitement or condoning acts of terrorism, may be blocked or removed from internet and these measures can take place by the decision of competent administrative authority without any intervention of court.

Furthermore, to implement new provisions introduced to counter terrorism in 2014, a Decree was issued on 5 February 2015, in which Directorate General of the National Police, the Central Office for Combating ITC-related Crime (OCLCTIC) was prescribed as a responsible authority for the removal or blocking of websites. By applying Article 6-1.1 LCEN, OCLCTIC can order internet hosting services (ISPs) to remove content. If not removed within 24 hours of such order, OCLCTIC may notify directly ISPs of the electronic addresses which are in violation of criminal-law provisions. Then ISPs within 24 hours of notification must by appropriate measures prevent access to services of notified electronic addresses.

Moreover, in case of failure to comply with LCEN obligation regarding content inciting or condoning terrorism, legal entities will be liable to punishment of a fine of 375000 euros and prohibition, whether permanent or for a maximum period of five years from carrying out professional or social activities[90].

In 2021, a new chapter was added to LCEN obliging large online platforms and search engines to fight hate speech on their networks. Article 42(6-4)[91] creates new obligation for large platforms to adopt human and technological measures to respond in-time to courts to remove hate speech, preserve them for investigative purposes, to designate point of contact for receiving and responding to such orders, making available their terms and conditions to tackle hate speech, to put in place such mechanism in which users are able to notify hate speech, to make redressal available in case of unfair removal[92].

[90] 'DisplayDCTMContent.Pdf' <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000168065497f> accessed 13 September 2022.

[91] 'Article 42 - LOI N° 2021-1109 Du 24 Août 2021 Confortant Le Respect Des Principes de La République (1) - Légifrance' <https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000043964847> accessed 13 September 2022.

[92] '1680a6578d.Pdf' <https://rm.coe.int/france-comments-on-the-country-update-report-final/1680a6578d> accessed 13 September 2022.

Additionally, in fight against terrorism and to protect national security of France, the Homeland Security Code (CSI)[93] also provides for intelligence gathering with cooperation of internet operators. For that, Article L.851-1 of CSI authorizes that, with the help of ISPs to collect information or documents processed on their networks[94].

Further in 2015, an Intelligence Bill[95] was announced to provide intelligence services legal framework. With the application of this Bill, the Prime Minister on the opinion of National Commission for the Monitoring of Intelligence Techniques, can oblige ISPs and particularly hosting services to implement means of identification of terrorist threat from the information processed and exclusively on the basis of anonymous data automatically processed. The purpose of this system of identification is only to prevent terrorism, and the Prime Minister can waive anonymity for the identification of threat.

3.3. The Overlying Features among the Laws

National governments have set severe time limits for removing illegal or damaging content. Businesses have limited time to remove illegal content after receiving a takedown request from a government entity. From one hour for EU terrorist content to four hours in Turkey[96]. A firm is frequently penalized for failing to promptly delete information.

National governments, mainly in Europe, have contemplated letting digital businesses decide whether material is legal. This has already happened. As a result of this, corporations, not courts or other judicial bodies, are required by law to evaluate whether material is unlawful when notified by the government or users. This tendency, which is

[93] 'Internal Security Code - Légifrance' <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/2022-08-16/> accessed 13 September 2022.
[94] 'Article L851-1 - Code de La Sécurité Intérieure - Légifrance' <https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030935595/> accessed 13 September 2022.
[95] LAW n° 2015-912 of July 24, 2015 relating to intelligence (1).
[96] 'Turkey: Law on Internet Publications Amended | Library of Congress' <https://www.loc.gov/item/global-legal-monitor/2014-02-24/turkey-law-on-internet-publications-amended/> accessed 13 September 2022.

also observed in Australia[97], raises serious questions about who should decide what is good and wrong.

Suggestions have been suggested to hold internet platforms legally liable for the illegal or damaging contents. Such as the case of US, where discussions[98] are made to amend Section 230 of the Communications Decency Act, which protect services providers from legal liability for the illegal content on their platforms.

Platforms are increasingly relying on automated content filtering. The EU's Terrorism Content Regulation, Pakistan's 2020 Citizens Protection Rules, and India's 2021 Guidelines for Intermediaries and Digital Media Ethics Code all openly promote or require these incentives. Platforms also benefit from short removal dates. Businesses may try to use technology to help them quickly locate and remove data in order to meet deadlines.

Administrations have also tried to enforce domestic laws abroad. They encouraged sites to remove foreign content that violates local regulations. Pakistan[99] has passed similar law. These procedures may allow the use of national speech rules globally, raising issues about territoriality.

Several additional proposals emphasized platform transparency and accountability. To improve the handling of illegal content, IT companies may be required to report on their compliance with applicable laws. Cyber-Hate Speech Law of France and EU Terrorist Content Regulation all have identical provisions. Similar to the EU's draught Digital Services Act (DSA) and India's 2021 Guidelines, other nations' laws emphasize

---

[97] Transport Department of Infrastructure, 'Consultation on a Bill for a New Online Safety Act' (*Department of Infrastructure, Transport, Regional Development, Communications and the Arts*, 25 August 2021) <https://www.infrastructure.gov.au/have-your-say/consultation-bill-new-online-safety-act> accessed 13 September 2022.

[98] 'Section 230 - Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 | Casetext Search + Citator' <https://casetext.com/statute/united-states-code/title-47-telecommunications/chapter-5-wire-or-radio-communication/subchapter-ii-common-carriers/part-i-common-carrier-regulation/section-230-protection-for-private-blocking-and-screening-of-offensive-material> accessed 13 September 2022.

[99] 'CP (Against Online Harm) Rules, 2020.Pdf' <https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2c%202020.pdf> accessed 13 September 2022.

systemic accountability and transparency, such as forcing algorithms to be transparent or simplifying moderation standards[100].

In the existence of these scattered directions, hosting service providers or content moderators will remain confused to which law they should implement and to avoid legal repercussions.

3.4. Current Industry Practices

Politicians do not always pay enough attention to what the global technology industry is doing right now as to the removal of illicit content online. It may not be ideal, but the majority of large corporations (and an increasing number of smaller ones) now have rules and enforcement practices in place for information that is "harmful" yet lawful in the location in which it is posted. Numerous businesses took this step long before recent calls for them to do so. Many people believe that terrorist content is ubiquitous on the Internet, although the majority of large platforms automatically delete 95 percent or more of it, and the majority of smaller platforms respond within hours of receiving takedown requests. Since December 2020, the Terrorist Content Analytics Platform (TCAP), which is developing to assist tech businesses in promptly removing proven terrorist content, indicates that 94 percent of URLs linking to verified terrorist content have been deleted by smaller platforms after the latter got informed[101]. TCAP have worked with over 25 different platforms as part of their Mentorship Program, and 12 of them have updated their anti-terrorism policy. Five of them have significantly enhanced their capacity to filter material. However, some platforms continue to refuse to engage with content moderation requests, and some of them are "alt-tech" sites that deal only with content that mainstream platforms avoid.

The objective of providing this analysis is not to absolve platforms of responsibility or to pretend that the threat is not real, but to examine the evidence that informed the latest legislative wave and its specific provisions. Few governments articulate specific reasons for enacting particular laws or regulations.

---

[100] 'Online Regulation of Terrorist and Harmful Content - Lawfare' <https://www.lawfareblog.com/online-regulation-terrorist-and-harmful-content> accessed 13 September 2022.

[101] 'Terrorist Content Analytics Platform' <https://www.terrorismanalytics.org/> accessed 13 September 2022.

Chapter 4: The Regulations (EU) 2021/784 of the European Parliament

The Regulation 2021/784, also known as the "TCO" or "TERREG" was enacted in June of 2021 and was scheduled to go into effect in June of the following year. It addresses the prevention of spreading terrorist content on computers and the internet. When the EU Commission said in October 2021 that it would fund programs to assist smaller platforms in compliance with the rule, as Tech against Terrorism had advocated in our response[102] to the legislation. The PERCI tool developed by Europol to help implementing the Regulation, will be used by the "competent authorities" of the member states.

During a review of the EU's Counter-Terrorism Agenda, seven UN Special Rapporteurs voiced their objections to the measure. TCO regulation's definition of ´terrorist content´ might be understood to include legal forms of communication, according to their letter. An explanation of the European Union's "operational conformance with human rights criteria for legal clarity" was requested by reporters. Before the TCO was approved by the legislature, it encountered a number of obstacles[103].

4.1. Definition of 'Terrorist Content'

The Regulation adopts the definitions of terrorist offences contained in the Counter-Terrorism Directive 2017/541 and utilizes them to assist in preventing persons from getting into difficulties. Solicits someone to conduct or assist in terrorist acts or terrorist group activities; inspires or promotes terrorist acts, for example, by praising them; and provides directions on how to carry out attacks. Material used for educational, journalistic, artistic, or research purposes, or to raise awareness, will not be considered "terrorist content."

[102] 'Tech-Against-Terrorism-Response-to-EU-TCO-June-2021-1.Pdf' <https://www.techagainstterrorism.org/wp-content/uploads/2021/06/Tech-Against-Terrorism-response-to-EU-TCO-June-2021-1.pdf> accessed 13 September 2022.

[103] 'THE ONLINE REGULATION SERIES | EUROPEAN UNION (Update) - Tech Against Terrorism' (10 December 2021) <https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/, https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/> accessed 13 September 2022.

The definition of "terrorist content" in Article 2(7) of Regulation (EU) 2021/784 is far too broad and leaves far too much room for interpretation as it will be problematic for HSPs or ISPs to differentiate between illegal content online or terrorist content online for their removal within specified time. More specifically, 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"[104].

To delete terrorist content swiftly and efficiently, online hosting services require both precise legal definitions of such content and industry guidelines as to how to interpret "terrorist content" when examining referrals or removing content on their own. When there is doubt about whether a piece of content qualifies as terrorist, it is unclear who makes the ultimate determination. This cannot be left to the supplier; rather, it must be made more explicit in the Regulation.

[104] See Article 2(7) of the Regulation (EU) 2021/784

4.2. Competent Authorities

According to Article 12 of the Regulation, the EU Member States shall designate authorities that have the authority to issue removal orders (that is orders issued by competent authorities of Member State to hosting service providers to remove terrorist content or to disable its access)[105], monitor the implementation of preventative measures, and penalize those who fail to comply.

Designation of competent authorities

The authorities designated under Article 12 of the Regulation will have the powers provided in other articles such as provided in Article 3,4,5, and of 18 of the Regulation to issue removal orders to hosting service providers to remove terrorist content or disable its access[106]. The authority will be competent to scrutinize the removal orders to assess intentional infringement of the Regulation or freedom provided by Charter and to make decision within 72 hours[107]. The competent authority can oversee the specific measures provided in article 5 of the Regulation, about its implementation, and can impose penalty to hosting services providers in case of infringement of this Regulation, taking care of all relevant circumstances provided in article 18(2) of the Regulation[108]. Each Member State will make sure of contact point is established within competent authority to deal clarification requests of removal orders issued by the competent authority[109].

However, it is unclear whether authorities to issue removal orders would be granted the new Regulation's powers, such as the capacity to remove and issue recommendations. This should be more precise. To ensure that impacted firms understand which authority is accountable for them, the number of authorities must be reduced. All enterprises with their headquarters in a Member State should be subject to a single judicial authority. This means that no one authority should have the authority to act against any business. To be able to supervise and implement the regulation, some authorities' powers to issue orders may need to be expanded. The plan does not specify which authorities' authority should be enhanced. Certain powers granted to responsible authorities by the Regulation appear to be excessively broad. For example, a judge should have the

[105] See also Article 3(1) of the Regulation 2021/784
[106] See Article 3 of the Regulation
[107] See Article 4(3) of the Regulation
[108] See Article 18 and 18(2) of the Regulation
[109] See Article 12(2) of the Regulation

jurisdiction to determine whether the proactive steps implemented by hosting service providers are sufficient, and the capacity to request more measures from the responsible authorities.

4.3. Cross-border Removal Orders Under Article 4 of the Regulation (EU) 2021/784

The Regulation provides for the procedures to issue removal orders in case the establishment or the legal representative of the hosting service providers is established cross-border. In such a case, if removal order is issued by the competent authority of a Member State in which the establishment or its legal representative is not residing or established, the competent authority will simultaneously submit a copy of removal order to the competent authority of the Member State in which hosting service provider´s establishment is established or its legal representative is residing[110]. Upon receiving removal order by the competent authority of the Member State, where the establishment is established or the legal representative is residing of the hosting service provider, the competent authority may within 72 hours of receiving the copy of the removal order, scrutinize the order to determine about its intentional infringement of the Regulation and in result of infringement, adopt an appropriate decision to the removal order[111].

Hosting service providers or the content providers do have a right to request for the scrutiny of the removal orders. Within 48 hours of receiving removal order, hosting service provider can request to the competent authority of the Member State where its establishment is established or its legal representative is residing, for the scrutiny of the removal order. The competent authority, within 72 hours of receiving request for scrutiny, make reasoned decision as to whether there is an infringement or not[112].
Definitely, terrorist content on the internet should be taken down as soon as possible after finding out about it. The right time and steps to unveil this information depend on the type of content and the type of infringement. The steps and procedures for taking-down or disabling access to terrorist content are improving progressively. The Regulation gives a deadline of one hour of the removal of terrorist content after its exposure over internet. This is too short. Any requirement to act quickly after receiving

[110] See Article 4(1) of the Regulation
[111] See Also Article 4(3) of the Regulation
[112] See Article 4(4) of the Regulation

a notice could lead to people making disputable, if not wrong, decisions and removing content simply to avoid possible penalties. This could end up blocking legal content, which is against the fundamental rights of the citizens. It should be focused on when the company learns about the order, not when it gets it.

Structure and content of Removal Order

The Regulation established templates[113] that authorities must complete with all the information required to HSPs. Removal orders must include an explanation of why the item is deemed to include terrorist content, as well as instructions on how to contest the order.

4.4. Specific Measures Under Article 5 Regulation (EU) 2021/784

Companies should set up alerting systems that are easy for employees to utilize. Anti-terrorist and anti-counterfeiting measures should be included in these measures, as well as proactive ways for identifying and eliminating unlawful information. It is imperative that businesses put in place effective and appropriate protections to ensure that content removal decisions are based on facts and are not arbitrary. This is of particular importance when utilizing computerized systems. These safeguards should involve human oversight and verification. Laws governing fundamental rights, free expression, and data protection should be followed while creating them. Special emphasis should be paid to small businesses. The business should cooperate and exchange ideas, practice guidelines, and technology solutions on a voluntary basis, especially those involving automatic recognition technologies. It is envisaged that this shared responsibility would benefit smaller platforms with fewer resources and experience in particular. Businesses should collaborate with law enforcement more closely if there is evidence of a serious criminal offence or a suspicion that illegal material poses a threat to life or safety.

The Regulation provides for the various specific measures to be taken by the hosting service providers to stop further dissemination of terrorist content online, removal or disable access thereto.

A hosting service provider is considered to be exposed to terrorist content, when competent authority of the Member State where the main establishment of the hosting service provider is established or its legal representative resides, has taken decision

[113] See Annex I of the Regulation

depending on objective factors and hosting service provider has received two or more removal orders within last 12 months finding that hosting service providers is exposed to terrorist content[114].

Specific measures

Hosting service providers can add to their terms and conditions of their services for its use, and also can apply provisions to address the misuse of their services for dissemination of terrorist content to public. But keeping in mind while doing so, to take such measures in such a non-discriminatory and diligently manner that do not infringe other fundamental rights of the users particularly freedom of expression and information in a democratic society to avoid removal of contents which are not terrorist contents[115].

Terrorist exposed hosting service provider can take specific measures for the protection of its services against spread of terrorist content to public and the choice as to take which measures remains vested with the hosting service provider. Regulation enlists various measures that can be taken by the hosting service provider, such as, by taking operational and technical measures or by staffing and opting technical means for the identification, removal and disabling access to terrorist content, providing easy mechanisms for users to "flag" alleged terrorist content or by increasing awareness of terrorist content or any other measure hosting service provider consider appropriate[116].

Specific measures taken by the hosting service provider must be in a manner which is non-derogatory and diligent, appropriate and targeted taking into account the vulnerability of exposure to terrorist content, must not infringe the user fundamental rights of freedom of expression, and most importantly, when measures are taken by technical means, human oversight must be provided to avoid removal of non-terrorist content[117].

The Regulation requests that all hosting service providers use "operational and technological procedures" that make it simpler for authorities to analyze content

[114] Article 5(4) of the Regulation
[115] See Article 5(1) of the Regulation
[116] Article 5(2) of the Regulation
[117] Article 5(3) of the Regulation

supplied to them immediately. To implement these safeguards, businesses will have to invest significantly more money. This is due to the Regulation's broad reach. All organizations that hold user-generated material would be required to provide an adequate facility for tracking referrals. Small enterprises, in particular, would be harmed by having to invest so much time and money. Additionally, "trusted flaggers" are already in use on a number of social networking platforms. Hosting service providers will now be responsible for law enforcement, since they will be required to review the content in question and determine if it should be deleted. Due to their involvement, a hosting service provider bears greater responsibility. The Regulation vests hosting service providers with a quasi-judicial function whereas HSPs are in no manner meet the requirements of a court and also, they are subjected to societal pressure when courts are free from such pressure. The breadth of one's own existence, is applicable to all hosting service providers operating in the European Union. In this sense, hosting service providers are individuals who provide information services by storing and making accessible to the public the information and material that service users submit when they want it. It is irrelevant if the archiving and dissemination of such content is purely technological, automated, and passive. Among these HSPs, there are social networking sites, video picture and audio sharing services, and cloud infrastructure providers, all of which are not covered by the Regulation in its entirety.

4.5. Complaint Procedures under the Regulation (EU) 2021/784

The Regulation (EU) 2021/784 provides for a mechanism of complaining against unjustified removal of contents, and an effective remedy to hosting service providers or content providers. Hosting service providers have to establish effectively accessible mechanism which allow content providers to submit a complaint, against unjustified removal of their content or disabling access thereto, for the reinstatement of the content removed and if it is found to be unjustified removal, hosting service provider have to reinstate the content without undue delay[118]. Further, this Regulation also provides for the remedy to challenge the removal order before the courts of the Member States whose competent authority issued the removal orders[119]. Moreover, those platforms which are using automated tools to detect terrorist content online, have to have a human

[118] See Article 10(1) and 10(2) of the Regulation
[119] See Article 9 of the Regulation

oversee to avoid erroneous removals of contents(Luyten 2021). The complaint procedure is a kind of protection of freedom of speech and the right to information. More specifically, it protects content provider´s right, under freedom of expression and information, against erroneous removal or disabling access to content online[120].

The Regulation (EU) 2021/784 is making hosting service providers liable to make such mechanism that can be effective and accessible and allowing content providers to make complaint, against such removal or disabling of their contents, for the reinstatement or the access of the contents removed due to the actions or measures taken under Article 5 of the Regulation[121]. Each hosting service provider have to pay attention in examining all complaints they receive through the mechanism provided for in the Regulation and have to reinstate content or access to it without any delay if in case of unjustified removal or access thereto. Hosting service providers have to inform about the result of complaint within two weeks of its receipt and in case of rejection of complaint, hosting service providers will explain about the reasons of their decision[122].

Further, the Commission will receive information from the EU Member States who will collect data from the competent authorities and hosting service providers every year on the 31st of March about the number of complaint procedures initiated and about actions taken by hosting service providers under Article 10[123].

Safeguards to Protect Fundamental Rights

The freedom of expression is safeguarded by different means: Transparency reports on actions taken to remove terrorist content and on any erroneous deletions of legitimate expression online will be required by both Member States and hosting service providers on an annual basis. User notice and recourse are offered in cases where content is deleted without their consent. As quickly as possible when content is removed erroneously, there are systems in place to guarantee that it is returned. Both content creators and internet platforms have the option of appealing the removal order to the appropriate authorities or going to court in their home countries to seek redress. Exempt content includes anything which is distributed for the purposes of education,

[120] See Recital 33 of the Regulation
[121] See also; Article 10(1) of the Regulation
[122] See also; Article 10(2) of the Regulation
[123] See Article 21(d) of the Regulation

journalism, the arts, or research. Dissemination of information aimed in combating terrorism will be exempt from this rule as well[124].

4.6. A Squandered Opportunity to Reconcile Counter-Terrorism and Fundamental Human Rights

On 7 June 2022, the Regulation (EU) 2021/784 on countering terrorist information online entered into force. As explained above, the Commission proposed the bill in 2018. Earlier postings on the CiTiP blog[125] examined the Commission´s Proposal for this Regulation, the talks that led to it, and the concerns of employing automated technologies to delete information. Before the Regulation was approved, human rights organizations expressed worries about probable difficulties associated with the protection of fundamental human rights, including freedom of expression, access to information and privacy.

On March 25, 2021, 61 human rights organizations requested the members of the European Parliament to reject the proposed Regulation. Using automated content moderation techniques to discover and remove terrorist content was more likely under the proposed Regulation, according to the letter[126]. Automated technologies may not distinguish between terrorist content and activism or comedy about terrorism, and thus, lawful content may be removed. The same organizations also expressed their concerns with regard to the degree of latitude the EU Member States had in determining which online content could be removed. So yet, no appropriate supervision system has been proposed. Furthermore, these organizations encouraged the European Parliament to consider the proposal's impact on, *inter alia*, freedom of expression, the right to information, privacy, and the rule of law.

[124] '202104_terrorist-Content-Online_en.Pdf' <https://home-affairs.ec.europa.eu/system/files/2021-05/202104_terrorist-content-online_en.pdf> accessed 13 September 2022.
[125] 'About' (*CITIP blog*) <https://www.law.kuleuven.be/citip/blog/about/> accessed 13 September 2022.
[126] 'MEPs_TERREG_Letter_EN.Pdf' <https://edri.org/wp-content/uploads/2021/04/MEPs_TERREG_Letter_EN.pdf> accessed 13 September 2022.

In 2019, the European Data Protection Supervisor (EDPS) issued official comments[127] criticizing the Proposed Regulation. The EDPS, like other human rights organizations, warned against employing automated decision-making methods, such as profiling, to identify and delete terrorist information posted online. The EDPS stated by giving reference to GDPR[128], of prohibition of solely making of automated decision, that can bring legal repercussions for data subject[129]. Human oversight and verification should always be present to ensure correctness and foundation of judgments. Also, according to the EDPS, an imprecise statement of providers' duties is problematic. The selected competent authorities should be able to keep an eye on them given the proposal's underlying trend of giving private groups a law enforcement authority.

After the Regulation came into effect, there still remain questions related to the protection of human rights. This Regulation should be enforced while maintaining vital rights like freedom of speech and privacy as provided for in its recitals and binding provisions saying about people´s overlook of automated technologies looking for terrorist information online. National competent authorities are chosen by each member state. A judicial review of removal orders was not included in the Regulation, which states that national responsible authorities shall perform their duties objectively and non-discriminatorily[130]. Aside from that, the Regulation states that the hosting service providers are not required to monitor for unlawful activity. Terrorist content may be stopped online by the providers. The removal order must be executed within one hour of receipt.

The Regulation entered into effect on June 7, 2022 and its outcome remains to be seen when implemented at national level in the EU Member States. Also, it remains to be seen whether this set of rules has achieved to strike the right balance between security and freedom[131].

---

[127] '2018-02-13_edps_formal_comments_online_terrorism_regulation_en.Pdf' <https://edps.europa.eu/sites/default/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_en.pdf> accessed 13 September 2022.

[128] See also Article 22(1) of the GDPR

[129] '2018-02-13_edps_formal_comments_online_terrorism_regulation_en.Pdf' (n 127). Section 3.3.2

[130] See Article 13(2) of the Regulation

[131] 'The New Regulation on Addressing the Dissemination of Terrorist Content Online: A Missed Opportunity to Balance Counter-Terrorism and Fundamental Rights? - CITIP Blog' <https://www.law.kuleuven.be/citip/blog/the-new-regulation-on-addressing-the-dissemination-of-terrorist-content-online/> accessed 13 September 2022.

4.6.1. Expected Hurdles in the Implementation of the Regulation (EU) 2021/784

Critics are concerned that governments may use the upload filter to prevent NGOs from chronicling events in war zones by aggressively removing extremist content and censoring their citizens. Also, they have concerned that Regulation may lead platforms towards the adoption of poor technological tools such as Hash Database referred in Explanatory Memorandum to the Regulation, as lawmakers have not much knowledge of Hash Database, and how it will serve this goal and will not contradict human rights or democratic values.

The Center for Democracy and Technology (CDT), a think tank that is partially funded by Amazon, Apple, Facebook, Google, and Microsoft, is one of the most outspoken detractors. It sent an open letter[132] to the European Parliament arguing that the rule will "drive internet platforms to adopt untested and poorly understood technologies to restrict online expression". Among the 41 signatories to the letter were the Electronic Frontier Foundation, Digital Rights Watch, and Open Rights Group.

According to Jens-Henrik Jeppesen in an interview to The Verge, a CDT's director for European affairs, "these filtering technologies are clearly being adopted by the major platforms," but the government "should not be pushed to implement technology in this manner"[133]

Even if the moderator properly identifies the material as illegal, omitting precise details may be detrimental to human rights organizations who rely on them to document assaults. Human rights abuses in Syria's civil war can be documented in a variety of ways, including through video recordings. Between 2012 and 2018, Google servers destroyed over 100,000 recordings, erasing critical evidence. Military combat video specialists have been obliged to back up their own film in order to avoid it being lost for good. The Syrian Archive is one of these organizations. Comparisons to YouTube's Content ID system, which is incompatible with the legislation, have been made by opponents, such as CDT. Copyright holders can use this ID to submit takedown requests for films that include copyrighted content, however the system may delete films

[132] 'Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.Pdf' <https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf> accessed 13 September 2022.

[133] 'Here's How the EU Plans to Fight Online Terrorism Content - The Verge' <https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu> accessed 13 September 2022.

submitted by their original owners and mistakenly identify original footage as copyrighted. Additionally, it is handy for commuting inside the neighborhood.
Additionally, proponents of anti-legislation like CDT, argue that current voluntary measures are adequate to halt the spread of terrorist information on the Internet. According to them, the majority of terrorist propaganda has already been removed from the major social media platforms, and users would have to search for it on an unrelated website. Every social network, regardless of size, should be held accountable to these same standards, Creighton[134] argues that these criteria should be established democratically. Each social network has its own internal policies and procedures for monitoring content, and there is less public information about them at the moment.

According to Creighton, "at the moment, every technology business is essentially implementing and abiding to its own laws." Under the proposed laws, all technology companies might be required to employ the same filtering technology. That is, it would be helpful to share results between platforms, EU member states, and law enforcement organizations such as Europol. While the EU's capacity to respect the rule of law is laudable, denying the Syrian Archive access to extremist information may prohibit other non-governmental organizations from obtaining terrorist content.

Regardless of how disturbing, these parties must have access to the information in order to conduct an adequate investigation into possible war crimes. Their independence from governments may result in their inability to perform their tasks under the new regulations. According to Creighton, freely sharing this knowledge with the public is not the solution. It is insufficient to state that you must "research and document ISIS recruitment in East London" if the information "directs to terrorist acts in London, Paris, or Dublin".

4.6.2. Implications for Countering Terrorism Online

A narrow perspective ignores the fact that smaller companies lack funding and that terrorist organizations utilize internet channels to propagate their message. Smaller IT businesses are already at danger of being utilized by terrorists, and governments failing to account for their capacity restrictions simply exacerbates the problem.

[134] 'Lucinda Creighton | Counter Extremism Project'
<https://www.counterextremism.com/people/lucinda-creighton> accessed 13 September 2022.

Many smaller platforms are controlled by one person or a small group of individuals. Because smaller platforms are not as big as larger corporations, they may not have specialized trust and safety teams or subject matter specialists. Also, many of these smaller sites cannot afford to design and utilize automatic content control systems. Terrorist organizations aim to exploit their lack of funds. In spite of terrorists' desire to exploit large platforms and circumvent moderation systems, they are significantly more effective and able to create long-term presence on smaller networks.

Ignoring smaller platforms by countries may have a major influence on the effectiveness of global regulatory methods. For example, the EU's "terrorist content" legislation will take effect in June 2022. These sites must delete suspicious information within one hour. How can a platform with only one employee fulfil a one-hour deadline? No surprise for the most used sites by terrorist groups. What happens if several of the most vulnerable platforms do not respect the law? How can smaller platforms compete when they face increased responsibility and government interference?

Governments do not appear to care about smaller platforms being transparent and honest when it comes to internet anti-terrorism rules. Several platforms have used our Mentorship Program to prepare their first transparency report. To collect proper data may be a lengthy and challenging procedure, especially for small firms. While greater transparency in the digital sector is a laudable aim, the rules for smaller platforms may be cumbersome and inefficient without enough assistance. We created the Tech against Terrorism Guidelines to set a norm for firms and push for more significant government openness, which is currently lacking.

4.6.3 The Risks to Freedom of Expression and Other Fundamental Human Rights

Despite good intentions, internet legislation often fails to preserve free expression and other fundamental human rights and the rule of law. For consecutive 11th year, global internet freedoms have declined, according to Freedom House[135]. Terrorism and violent

[135] 'Freedom on the Net 2021: The Global Drive to Control Big Tech' (*Freedom House*) <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech> accessed 13 September 2022.

extremism, as many politicians will argue, equally threaten free expression both online and offline. In reality, governments should enhance their own countermeasures. In my opinion, there is no contradiction between the two.

Freedom of speech concerns are evident when platforms are required to delete information swiftly or face sanctions for not doing so. The damage to democratic norms like the rule of law is significant when governments delegate this task to private IT businesses as provided in Regulation to put responsibilities over Internet Services Providers to detect and remove or disable access to online terrorist content.

Also, some of the legislation considered is overly wide in scope and lacks specificity. To cease spreading harmful, abusive, insulting, deceptive, confusing, vulgar or profane language is illegal in Kenya. Content that "threatens the unity, integrity, defense, security, or sovereignty of India" is prohibited in India. Some definitions may be worthless, as terrorist content definitions are a circle. The UK's Online Safety Bill defines terrorist content as content that leads to a terrorist act.

Platforms are less likely to respect laws by implementing suitable and balanced moderation measures if crucial phrases are defined vaguely. Vagueness also jeopardizes many people's freedom of speech. Platforms may try to play it safe by interpreting broadly to cover all bases. They may also delete genuine speech. The necessity for future regulation may be emphasized by legislators, yet it may hinder tech businesses' examination and implementation of new legislation.

The subject of enforcing national laws outside of the country is also raised. In many cases, the regulations explored for the purposes of this master thesis require content to be deleted from sites outside State's own jurisdictions. Brazil's legislation, for example, might be used to prohibit the spread of terrorist information globally. The Pakistani Citizens Protection Rules state that they apply to all Pakistanis, regardless of where they reside. Local speech laws may represent local concerns, but they should not be used to censor legitimate speech in other countries[136].

[136] 'Online Regulation of Terrorist and Harmful Content - Lawfare' (n 100).

Chapter 5: Required Reforms and Recommendations to Tackle Online Terrorism

5.1. Fighting Terrorism is a Priority for the EU

Fighting terrorism is a top priority for EU, its Member States and for its international partners inasmuch as terrorism is a threat to freedom, security, democratic values and rights of European citizens. After the attacks of 9/11, European Union adopted various measures to fight terrorism and contributed to fight terrorism as EU played a major role to coordinating the respective efforts of its Member States, no matter if the responsibility to combat crime and ensuring security lies with them. In a joint statement issued by EU leaders in 2015[137], to guide the EU and its Member States in their work against terrorism to focus on (i) cooperation with international partners to stop terrorism coming from neighborhood by making border controls more efficient, (ii) protection of citizen´s security by means of cooperation of judicial authorities, law enforcement agencies and Member States´s security services, information sharing through Europol and Eurojust and due to the importance of cyber-security, quickly adopt the Network and Information Security Directive, and (iii) the prevention of radicalisation by means of detecting and removing online contents promoting extremism and terrorism over the Internet through sufficient measures in accordance with national constitutions, by cooperation between private and public sectors at EU level and by working with Europol to establish internet referral capabilities.

Then in November 2020, after terrorist attacks in France, Germany, and Austria, the EU Home Affairs Ministers decided to bolster their cooperative efforts in the fight against terrorism without jeopardizing the EU's shared ideals of democracy, justice, and freedom of expression[138].

[137] 'Informal Meeting of the Heads of State or Government Brussels, 12 February 2015 - Statement by the Members of the European Council' <https://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/> accessed 13 September 2022.

[138] 'Joint Statement by the EU Home Affairs Ministers on the Recent Terrorist Attacks in Europe' <https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/> accessed 13 September 2022.

5.1.2. Prevention of Radicalization, Addressing the Dissemination of Terrorist Content Online

Radicalisation is not a new problem, but its weight has grown seriously in recent years. Terrorist propaganda and extremism's growth have benefited from advancements in internet communication technologies, which have made it easier for terrorists to communicate across national borders. From 2015 onward EU has taken many steps towards fighting against terrorism whether online or offline.

Europol has created a unit (EU Internet Referral Unit, EU IRU) to deal with online terrorist propaganda, which aims to detect such contents over internet, investigate and to provide relative support to member states. This unit also flag violent and terrorist online content and share it with relevant partners, request removal of such content and immediately carry out the referral process[139].

Furthermore in 2015, the EU launched the Radicalisation Awareness Network (RAN) which comprises of more than 6000 professionals from different fields across Europe, like law enforcement agents, Prison staff and teachers to exchange best practices, in order to understand the reasons behind vulnerability to radicalization of some people and to provide action plan to protect them from being radicalized.

In a joint statement by the EU Home Affairs Ministers in 2020, they affirmed important measures such as, upholding freedom and acting with determination, strengthening European framework for Counterterrorism, to be taken due to the transnational nature of terrorist networks and to prevent radicalisation by taking systematic action. After attack on teacher in France, which pays more focus on combating terrorism propaganda or hate speech over internet.

Lastly, to fight against continued presence of terrorist content online to recruit, intimidate or radicalizing for terrorist purposes, the EU has adopted the Regulation 2021/784 for the instant removal of online terrorist contents, which was presented in the previous chapters of the thesis.

[139] 'EU Internet Referral Unit - EU IRU' (*Europol*) <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru> accessed 13 September 2022.

5.2. Recommendations

Given the circumstances and the provisions provided above either at the EU level or its Member States level, there is a need to have a uniform mechanism and structure to follow and to have a single directed Rules or Regulations in order to fight against the menace of terrorism in an online space as to the cross-border nature of Internet.

Such Law or Regulation should be enacted by which Internet Services Providers have no doubt about the definitions of illegal or terrorist content and to which contents should be removed and under whose authority.

The rule of one hour, near me, is also kind of giving space to such filthy contents over internet even for only one hour. Instead, the hosting service providers or content moderators should not be allowed to even upload such contents on the internet. For that, internet providers, hosting service providers or the content providers have to have filter system that detect such content before being published over internet, as during one hour, millions of users can be affected.

The right to freedom of expression should not be allowed to use it to play with the emotions of other as to their religious matter, as it is leaving some serious consequences for the society and making people more radicalized and violent on the other side. This right need to be refined.

In the near future, it is imperative to build a worldwide strategy to combat cyber terrorism. Eight stages have been outlined in a global strategy to tackle cyber-terrorism: According to the UN, terrorism and cyberterrorism must have the same definition. As a precondition for using the phrase "cyber terrorism," a definition must be provided for what comprises and what does not (for example, hacking, propaganda, and attacks on key infrastructure). Otherwise, the phrase has no real significance. Starting with a common language or a technical language that everyone understands is one option.

Further, there must be a substantial amount of legal action both domestically and internationally. International legal conventions must be established. As a result, national and international rules must coexist peacefully.

It is essential that governments all around the globe form bilateral and multilateral agreements to cooperate on cyber security.

At long last, we've arrived at our destination. Any country should be able to receive and exchange information with any other country at the same time through an intelligence pool. In this scenario, observing terrorist websites should not be the exclusive method

of acquiring intelligence. In the event of a projected cyberattack, it should also include the gathering of electronic evidence.

Training and deploying cyber defense professionals throughout the world are a must in the case of an attack by another government. NATO's Computer Incident Reaction Capability and Cooperative Cyber Defense Center of Excellence may help national governments by increasing the number of fast response teams available. The cyber security training offered at this facility is open to anyone from all around the world.

Countries should organize and engage in multinational counter-cyberattack exercises in order to learn from one another.

To stop or avoid a cyberattack, an efficient worldwide decision-making framework is required. Those who are legally bound to respond to threats to international security should do so. There must be a comprehensive examination after an attack to find and fix the system's vulnerabilities. A poll should be used to assess whether or not any adjustments are needed.

Chapter 6: Conclusion

The European Union has depended on trial and error, collaboration, and voluntary agreements to tackle terrorist content, and is now taking the next step by proposing legislative measures. The fight against terrorism and radicalization in Europe requires the cooperation of all segments of society, including those who operate online. Though little scientific evidence exists on the social repercussions and consequences of terrorist material, regulation is necessary to control terrorist information on the internet. Despite the necessary adjustments, more political support is still needed before the idea can be formalized into legislation. Indeed, it is a groundbreaking initiative that illustrates an unwavering dedication to action in the face of danger. To keep things as they are, the EU and a large majority of its members must change course. Legislation must work with civil society and the voices of those who support it in order to successfully counteract unpleasant or possibly hazardous online attitudes. We learned that efficient counterterrorism measures and protecting freedom of expression are not always mutually exclusive; in practice, they may be complementary and enhance one another as well as the state. Anyone who believes in the need of preventing the spread of terrorist propaganda on the internet, including the group's most vocal critics, is in agreement. For practical and effective solutions to these problems while still adhering to applicable human rights rules, the Council, Commission, and European Parliament must work together in coordination.

Bibliography

‘§ 1 NetzDG - Einzelnorm’ <https://www.gesetze-im-internet.de/netzdg/__1.html> accessed 13 September 2022

‘§ 3 NetzDG - Einzelnorm’ <https://www.gesetze-im-internet.de/netzdg/__3.html> accessed 13 September 2022

‘1680a6578d.Pdf’ <https://rm.coe.int/france-comments-on-the-country-update-report-final/1680a6578d> accessed 13 September 2022

‘1680a6992e.Pdf’ <https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e> accessed 13 September 2022

‘2018-02-13_edps_formal_comments_online_terrorism_regulation_en.Pdf’ <https://edps.europa.eu/sites/default/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_en.pdf> accessed 13 September 2022

‘16808c3f55.Pdf’ <https://rm.coe.int/16808c3f55> accessed 13 September 2022

‘202104_terrorist-Content-Online_en.Pdf’ <https://home-affairs.ec.europa.eu/system/files/2021-05/202104_terrorist-content-online_en.pdf> accessed 13 September 2022

‘About’ (*CITIP blog*) <https://www.law.kuleuven.be/citip/blog/about/> accessed 13 September 2022

‘About Tech Against Terrorism - Tech Against Terrorism’ (4 September 2017) <https://www.techagainstterrorism.org/about/, https://www.techagainstterrorism.org/about/> accessed 13 September 2022

‘Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)’ (*Bundesministerium der Justiz*) <https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.html> accessed 13 September 2022

‘Against the Clock: Can the EU’s New Strategy for Terrorist Content Removal Work?’ <https://www.rusi.orghttps://www.rusi.org> accessed 13 September 2022

‘Article 42 - LOI N° 2021-1109 Du 24 Août 2021 Confortant Le Respect Des Principes de La République (1) - Légifrance’ <https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000043964847> accessed 13 September 2022

‘Article L851-1 - Code de La Sécurité Intérieure - Légifrance’ <https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030935595/> accessed 13 September 2022

‘Bruce Hoffman | Council on Foreign Relations’ <https://www.cfr.org/expert/bruce-hoffman> accessed 13 September 2022

Cevik S, ‘The Development Of The Eu’s Counter Terrorism Policies In The Post 9/11 Era’ 105

‘Civil Society Empowerment Programme’ <https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/civil-society-empowerment-programme_en> accessed 13 September 2022

‘Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.Pdf’ <https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf> accessed 13 September 2022

‘COMMISSION RECOMMENDATION (EU) 2018/ 334 - of 1 March 2018 - on Measures to Effectively Tackle Illegal Content Online’ 12

‘Country Reports on Terrorism 2019 - United States Department of State’ <https://www.state.gov/reports/country-reports-on-terrorism-2019/> accessed 13 September 2022

‘CP (Against Online Harm) Rules, 2020.Pdf’ <https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2c%202020.pdf> accessed 13 September 2022

Department of Infrastructure T, ‘Consultation on a Bill for a New Online Safety Act’ (*Department of Infrastructure, Transport, Regional Development, Communications and the Arts*, 25 August 2021) <https://www.infrastructure.gov.au/have-your-say/consultation-bill-new-online-safety-act> accessed 13 September 2022

‘DisplayDCTMContent.Pdf’ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168065497f> accessed 13 September 2022

Echikson W and Knodt O, ‘Germany’s NetzDG: A Key Test for Combatting Online Hate’ (22 November 2018) <https://papers.ssrn.com/abstract=3300636> accessed 13 September 2022

‘EU Internet Forum Committed to an EU-Wide Crisis Protocol’ (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009> accessed 13 September 2022

‘EU Internet Referral Unit - EU IRU’ (*Europol*) <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru> accessed 13 September 2022

‘EU Terrorism Situation & Trend Report (TE-SAT)’ (*Europol*) <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> accessed 13 September 2022

‘EUR-Lex - 32008F0919 - EN - EUR-Lex’ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0919> accessed 13 September 2022

‘European Union Internet Forum (EUIF)’ <https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en> accessed 13 September 2022

‘——’ <https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en> accessed 13 September 2022

‘Europol’s Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda’ (*Europol*) <https://www.europol.europa.eu/media-press/newsroom/news/europol’s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda> accessed 13 September 2022

‘Facebook Bans Britain First and Its Leaders | The Far Right | The Guardian’ <https://www.theguardian.com/world/2018/mar/14/facebook-bans-britain-first-and-its-leaders> accessed 13 September 2022

‘Freedom on the Net 2021: The Global Drive to Control Big Tech’ (*Freedom House*) <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech> accessed 13 September 2022

‘German Criminal Code (Strafgesetzbuch – StGB)’ <https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1310> accessed 13 September 2022

‘Gorwa - 2019 - The Platform Governance Triangle Conceptualising .Pdf’ <https://web.archive.org/web/20200506195742id_/https://www.econstor.eu/bitstream/10419/214074/1/IntPolRev-2019-2-1407.pdf> accessed 13 September 2022

‘Hard Questions: How We Counter Terrorism’ (*Meta*, 15 June 2017) <https://about.fb.com/news/2017/06/how-we-counter-terrorism/> accessed 13 September 2022

‘Here’s How the EU Plans to Fight Online Terrorism Content - The Verge’ <https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu> accessed 13 September 2022

‘Informal Meeting of the Heads of State or Government Brussels, 12 February 2015 - Statement by the Members of the European Council’ <https://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/> accessed 13 September 2022

‘Internal Security Code - Légifrance’ <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/2022-08-16/> accessed 13 September 2022

‘Introducing DeepText: Facebook’s Text Understanding Engine - Engineering at Meta’ <https://engineering.fb.com/2016/06/01/core-data/introducing-deeptext-facebook-s-text-understanding-engine/> accessed 13 September 2022

‘Joint Statement by the EU Home Affairs Ministers on the Recent Terrorist Attacks in Europe’ <https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/> accessed 13 September 2022

Kettemann MC, ‘FOLLOW-UP TO THE COMPARATIVE STUDY ON “BLOCKING, FILTERING AND TAKE- DOWN OF ILLEGAL INTERNET CONTENT”’ 12

‘Lucinda Creighton | Counter Extremism Project’ <https://www.counterextremism.com/people/lucinda-creighton> accessed 13 September 2022

‘MEPs_TERREG_Letter_EN.Pdf’ <https://edri.org/wp-content/uploads/2021/04/MEPs_TERREG_Letter_EN.pdf> accessed 13 September 2022

‘Online Regulation of Terrorist and Harmful Content - Lawfare’ <https://www.lawfareblog.com/online-regulation-terrorist-and-harmful-content> accessed 13 September 2022

Organisation für Sicherheit und Zusammenarbeit in Europa and Office for Democratic Institutions and Human Rights (eds), *Preventing Terrorism and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Community Policing Approach* (OSCE 2014)

Ramešová K, ‘Public Provocation to Commit a Terrorist Offence: Balancing between the Liberties and the Security’ (2020) 14 Masaryk University Journal of Law and Technology 123

Reeve Z, ‘Repeated and Extensive Exposure to Online Terrorist Content: Counter-Terrorism Internet Referral Unit Perceived Stresses and Strategies’ [2020] Studies in Conflict & Terrorism 1

‘Regulating Terrorist Content on Social Media: Automation and the Rule of Law | International Journal of Law in Context | Cambridge Core’ <https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1> accessed 13 September 2022

‘Regulation Addressing the Dissemination of Terrorist Content Passed’ <https://eucrim.eu/news/regulation-addressing-the-dissemination-of-terrorist-content-passed/> accessed 21 November 2022

Reiffenstuel A, ‘EU COUNTERTERRORISM STRATEGY: Understanding the Background, Measures and Limits of Europe’s Counter-Terrorism Strategy between 2014 and 2020’

Scheinin M, ‘The EU Regulation on Terrorist Content: An Emperor without Clothes’ 2

Scheinin M and Terrorism UHRCSR on the P and P of HR and FF while C, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin ': <https://digitallibrary.un.org/record/704287> accessed 13 September 2022

'Section 230 - Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 | Casetext Search + Citator' <https://casetext.com/statute/united-states-code/title-47-telecommunications/chapter-5-wire-or-radio-communication/subchapter-ii-common-carriers/part-i-common-carrier-regulation/section-230-protection-for-private-blocking-and-screening-of-offensive-material> accessed 13 September 2022

'Statement of Dr. Denning' <https://irp.fas.org/congress/2000_hr/00-05-23denning.htm> accessed 13 September 2022

'Summary Report of the Public Consultation on Measures to Further Improve the Effectiveness of the Fight against Illegal Content Online | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal> accessed 13 September 2022

'Tackling Illegal Content Online – Meeting with Online Platforms of 9 January 2018 | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/tackling-illegal-content-online-meeting-online-platforms-9-january-2018> accessed 13 September 2022

'Tech-Against-Terrorism-Response-to-EU-TCO-June-2021-1.Pdf' <https://www.techagainstterrorism.org/wp-content/uploads/2021/06/Tech-Against-Terrorism-response-to-EU-TCO-June-2021-1.pdf> accessed 13 September 2022

'Terrorism | Definition, History, & Facts | Britannica' <https://www.britannica.com/topic/terrorism> accessed 13 September 2022

'Terrorism | Eurojust | European Union Agency for Criminal Justice Cooperation' <https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/terrorism> accessed 13 September 2022

'Terrorism in the EU: Facts and Figures - Consilium' <https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/> accessed 13 September 2022

'Terrorist Content Analytics Platform' <https://www.terrorismanalytics.org/> accessed 13 September 2022

'Terrorist Content Online' <https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_en> accessed 13 September 2022

'The Image Similarity Challenge and Data Set for Detecting Image Manipulation' <https://ai.facebook.com/blog/the-image-similarity-challenge-and-data-set-for-detecting-image-manipulation/> accessed 13 September 2022

‘The New Regulation on Addressing the Dissemination of Terrorist Content Online: A Missed Opportunity to Balance Counter-Terrorism and Fundamental Rights? - CITIP Blog’ <https://www.law.kuleuven.be/citip/blog/the-new-regulation-on-addressing-the-dissemination-of-terrorist-content-online/> accessed 13 September 2022

‘THE ONLINE REGULATION SERIES | EUROPEAN UNION (Update) - Tech Against Terrorism’ (10 December 2021) <https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/, https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/> accessed 13 September 2022

‘——’ (10 December 2021) <https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/, https://www.techagainstterrorism.org/2021/12/10/the-online-regulation-series-european-union-update/> accessed 13 September 2022

‘The Use of the Internet for Terrorist Purposes’ 158

Theohary CA, *Terrorist Use of the Internet: Information Operations in Cyberspace* (DIANE Publishing 2011)

‘Turkey: Law on Internet Publications Amended | Library of Congress’ <https://www.loc.gov/item/global-legal-monitor/2014-02-24/turkey-law-on-internet-publications-amended/> accessed 13 September 2022

Weimann G, ‘Cyberterrorism How Real Is the Threat?’ 12

——, ‘Cyberterrorism: The Sum of All Fears?’ 21

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling Illegal Content Online Towards an enhanced responsibility of online platforms 2017

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond 2020

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) 2010

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 2017

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) 2019

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market 2016

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 2018

Council Framework Decision of 13 June 2002 on combating terrorism 2002 (OJ L)

LAW n° 2015-912 of July 24, 2015 relating to intelligence (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 (Text with EEA relevance) 2021 (OJ L)