CEU Department of Public Policy | CENTRAL EUROPEAN UNIVERSITY

Policies *vs* users' freedom?

The analysis of the Twitter debate on the EU Regulation addressing terrorist content online

By

Emmachiara Manna

Submitted to

Central European University

Department of Public Policy

In partial fulfilment of the requirements for the degree of

Master of Arts in International Public Affairs

Supervisor: *Professor Nick Sitter*

Vienna, Austria

2022

Author's Declaration

I, Emmachiara Manna, hereby declare that I am the sole author of this thesis. To the best of my knowledge this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted as part of the requirements of any other academic degree or non-degree program, in English or in any other language. This is a true copy of the thesis, including final revisions.

Date: June 15, 2022

Name: Emmachiara Manna

Don't be terrorized. Don't let fear rule your life.

Even if you are scared.

Salman Rushdie

Acknowledgements

I want to thank everyone who has been close to me during these two years. My family and friends who have always supported me.
In particular, I thank Professor Nick Sitter, who accompanied me with immense patience and unceasing optimism to the conclusion of this journey.

Abstract

Terrorism is a threat to all democratic institutions. It is a constantly evolving phenomenon. With the advent of Web 2.0, Cyber-terrorism was born. It exploits the Internet to spread its radical ideology and instill fear in people. Because of the ever-increasing role that the Web plays in terrorism's action strategies, it has become imperative to develop new measures that target this particular form of terrorism. In April 2021, The European Parliament and the Council of the European Union approved the Regulation to Combat the Dissemination of Terrorist Content Online (TERREG). This thesis aims to focus on why this Regulation was necessary, what countermeasures it introduces, and what side effects it has.

Moreover, public opinion has not willingly accepted TERREG. Through a sentiment analysis of Twitter users, this research found that the main reason why individuals opposed such Regulation is that it excessively limits their fundamental rights. It was also inferred that this discontent stems from a failure of the European Union to promote public awareness campaigns on the issue of cyber-terrorism.

Contents

List of Figures

Introduction

"Democratic nations must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend" (Apple Jr [1]). With these words, Margaret Thatcher in 1985 emphasized the central role that publicity (or propaganda) plays in terrorist groups. Through propaganda, terrorist groups can simultaneously recruit new members and spread fear.

The advent of the digitization era has offered terrorists a significant advantage: the possibility of exploiting the Internet to raise their communication with the outside world exponentially. Therefore, it has become the primary means for terrorist propaganda (Lieberman [19]). As a result, *cyber-terrorism* was born, which encompassed all terrorist activities occurring in the virtual world.

Cyber-terrorism poses a great threat to democracy. It can "strike" billions of people simultaneously with a single click. This is why world powers, including the European Union, have recognized the urgent need to combat this new form of terrorism (Bogdanoski and Petreski [5]). The most recent measure adopted by the European Union to hinder cyber-terrorism is the Regulation on Addressing the Dissemination of Terrorist Content Online, better known as TERREG (T. E. Parliament and Council of the European Union [25]). This Regulation was approved by the European Parliament and Council in April 2021 and entered into force on June 7, 2022. It aims to eliminate all terrorist content from the Web. Achieving this goal requires measures that inevitably impact the content posted by each user. Consequently, this Regulation is part of a much broader context that transcends the terrorist threat. Indeed, TERREG has become part

of the debate regarding how and whether the EU should regulate the Internet. Nowadays, the Web represents the main place where people spend most of their time. It is the medium through which they communicate and acquire information. Consequently, the moment one interferes with this dimension fuels a massive debate. Specifically, one becomes part of the discussion between those who want a free and incensed Internet and those who advocate the need to introduce measures to regulate the Web and make it a safe space.

Therefore, because cyber-terrorism, like traditional terrorism, has the primary purpose of having a powerful impact on people, and because at the same time, the counter-terrorism measures also affect individuals, public opinion on this issue acquires relevance.

Despite this, European bodies often tend to underestimate the importance of gaining public support regarding their activities. Concerning the European institutions dealing with terrorism, Europol, Eurojust, the EU Counter-Terrorism Coordinator, and TERREG specifically, there is evidence of a lack of effort to raise public awareness of the seriousness of the threat of cyber-terrorism and the consequent need for new counter-terrorism measures.

This thesis aims to focus on the new EU Regulation and analyze its pros and cons. Specifically, the goal is to bring to light the opinion that users of Twitter, the Social Media of excellence for political discussion, have about this Regulation.

Specifically, the thesis will be structured as follows: the first chapter will be devoted to studying the existing literature on terrorism and cyber-terrorism. The second chapter will be devoted to tracing the temporal and strategic evolution of terrorism from the birth of modern terrorism in the 1880s to the various forms of cyber-terrorism we face today. Next, the third chapter offers an overview of European terrorism legislation and institutions dealing with it. With the fourth chapter, we enter the heart of this thesis. In fact, it is committed to the study of the TERREG. Throughout this section, we move from an analysis of the

content of the Regulation to a consideration of its limitations and drawbacks. Finally, before reaching our conclusions, the fifth chapter analyzes Twitter users' sentiment on terrorism, cyber-terrorism, and TERREG. Through this research, and mainly through the analysis of negative tweets about the Regulation, it is possible to identify the main matrices that led people to take a stand against the adoption of the EU Regulation.

Chapter 1

Literature Review

1.1 Terrorism definition and history

To understand what is meant by cyber-terrorism and how European agencies fought it, it is necessary to have a clear understanding of what terrorism is. Many definitions of the concept of terrorism have been formulated throughout history. The United Nations Security Council in Resolution 1566 (2004) states that terrorism can be defined as: "any criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, [...], with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act" (Saul [26]). In the international arena, the Schmid definition is considered by many to be conventional. He argues that: "terrorism is a method of combat in which symbolic or random victims become the target of acts of violence. Members of a group are placed in chronic fear (terror) resulting from previous acts of violence or from the credible threat of violence [...]. The purpose of terrorism is either to immobilize the target of terror in order to produce disorientation and/or acquiescence, or to mobilize secondary targets from whom something is demanded or who constitute the target of special attention" (Schmid [28]).

The European Union, in turn, defines terrorism as offenses committed for: "intimidating a population; compelling a government or international organization to perform or refrain from performing any act; and seriously destabilizing or destroying the fundamental political, constitutional, economic, or social structures of a country or international organization" (Dumitriu [13]).

Not the least, one of the U.S. government definitions states: "terrorism is the threat or use of violence for political purposes by individuals or groups, whether they are acting for or against government authorities, when these actions are intended to shock, stun, or intimidate a target group larger than the victim itself" (Shanahan [29]).

Clearly, there has been no agreement on a common definition of terrorism. However, there are three basic aspects that unite any attempt to define the phenomenon.

First, terrorism is always about someone's "distorted" perception of justice. And, in addition, it always has a political nature involving actions designed to attract public attention and bring about political change.

Second, terrorists always distinguish themselves by being nongovernmental entities.

Finally, terrorists always target innocent civilians by carrying out surprise attacks that do not fall within international norms or "tolerated" standards for the use of violence.

So, the summa of the most distinctive features of terrorism can be identified in the fact that it involves the calculated use of violence against individuals or groups for the purpose of intimidation, inducing fear, often to kill, in the name of political, religious or other purposes. The overall purpose of intimidation is well emphasized by Raymond Aron, whose definition of terrorism states: "A violent action is called terrorism when its psychological effects are far greater than its purely physical results" (Chaliand and Blin [8]).

Having clear what is meant when we talk about terrorism, the question that

now needs to be answered is how the latter transforms and acts when it enters cyberspace. In fact, this research focuses on the section of terrorism that uses internet and Social Media as a means of communication and propaganda.

1.2 Terrorism and Social Media

When talking about cyberspace, there is a general tendency to refer to Social Media and their role within contemporary society. In fact, Social Media have become the center of both the virtual world and the daily lives of most individuals. Social media have changed the way people communicate with each other and how they interface with the outside world. Thus, as Social Media has become a cornerstone of contemporary society, terrorism has also had to deal with it.

Indeed, an aspect that academics have found interesting concerns the communication strategies of terrorist groups and how these have evolved over the years. In particular, with the advent of Web 2.0, terrorist groups have begun to see the Internet as a new frontier to conquer and an additional means to spread their message. Consequently, many scholars have focused on how terrorist groups can exploit the virtual world to achieve their goals.

Imran Awan points out how terrorist groups, e.g., ISIS, use Internet not only as a means of communication among the faithful but also, and especially, as a means of recruitment and propaganda (Awan [2]).

Terrorists strategy of using social media to share their ideology, enables them to have a global public that they would never reach with "in-person" communication. (Denning, 2010).

Moreover, Freiburger and Crane argue that Social Media are an advantage for terrorism from the prospective of the "Social Learning Theory." (Freiburger and Crane, 2008). In fact, the Internet facilitates the sharing of knowledge between people, and this learning process includes the promotion 'deviant behaviour'.

Moreover, it has been proven that the algorithms underlying Social Media play a central role in the online recruitment mechanism of terrorist groups (Dhiraj Murthy, 2021). In fact, the mechanism whereby each user is offered different content based on his or her preferences and "habits" means that if a user pays attention to a particular type of content considered "radical", then more and more content of the same type is offered to him or her. In this way, terrorist groups can exploit the growing polarization of online society in their favor, making, among other things, communication and confrontation between opposing poles even more difficult.

In addition, an absolute advantage offered by Social Media is that, for the first time, bi-lateral communication is at the center of online interaction (Majid KhosraviNik and Mohammedwesam Amer, 2022). This means that the people to whom online terrorist propaganda is directed can absorb it and, at the same time, comment on it, boosting and sharing it in turn. This makes the users an active player of the "ideological mission" they are supporting. In a social context that, until a few decades ago, was characterized by the crisis of the individual and the growing desire to make one's voice heard, this possibility of feeling part of something bigger and revolutionary has played a key role in the online communication strategies of terrorist groups.

Hence, considering the obvious cruciality that Social Media represents for the survival of terrorism in contemporary society, it became equally vital to study how the Internet could be used to combat terrorism and, in particular, the dissemination of terrorist content online.

1.3 Counter-terrorism online strategies

It is undeniable that the digital world has accelerated and facilitated the spread of terrorism in modern societies. However, it is also true that the use of specific software and Artificial Intelligence (AI) have contributed significantly to the

fight against terrorism (Singh and Lin [30]). For this reason, many researchers have studied how these tools could be implemented to become a shield, and sometimes even a weapon, against terrorism threats.

More specifically, a Joint Report by UNICRI and UNCCT highlighted how Artificial intelligence (AI) can be an indispensable tool for intercepting correlations and recurring patterns in online data that otherwise would not be detectable. (UNICRI and UNCCT [34]). As a versatile technology, this capability can also be used to the benefit of the battle against terrorism. By virtue of this, the counter-terrorism institutes around the world are studying how to use AI in pursuit of their objective.

Through the use of these technologies, is possible to blackout most terrorist content and block the accounts that create it, and simultaneously track down the physical individual (or organization) behind it (Weimann [35]).

The Internet has created the real foundations of the current and future democratic society, mainly because the values underlying the two "phenomena" are the same. The essence of the Internet, as that of democracy, is openness and inclusiveness. Openness leads to widespread participation, opportunities to express one's thoughts freely, and communication across borders and barriers. Nevertheless, the Internet allows cultures and individuals with dissonant ideas to come together and unite in a great and fruitful global debate.

From this perspective, there is a tendency to emphasize the beneficial effects of decentralization. Indeed, decentralized systems may be the ideal means to combat dangers, such as terrorism, that rely on highly distributed networks. There is a belief that an effort from "one center" can never combat the terrorist phenomenon effectively. Consequentially, a "global electronic citizenship" (understood as a network that can connect all citizens) seems to be the best way to defend against terrorist propaganda (Hintz et al. [17]).

Underlying this idea is the belief that open and transparent environments are much safer than closed environments, and connecting millions of people even

with divergent ideas in an open environment like the Internet combats the division that terrorist organizations seek.

However, the main problem behind these online counter-terrorism measures is that they are often limited to reactive rather than preventive action (Government [16]). In fact, so far, they have been limited to identifying online content for terrorist purposes and eliminating it. In contrast, much more work could be done on using Artificial Intelligence as a direct means to target and weaken terrorist organizations.

1.4 From a "State focus" to a "society focus"

Over the years, many have devoted themselves to the study of terrorism, starting from its origins to the latest forms of cyber-terrorism. However, little space has been devoted to those who are often the victims of such attacks. More specifically, although much has been said about how terrorists choose their targets, not much has been said about individuals' perceptions of terrorism. Where some scholars have engaged in this type of analysis, they have limited themselves to considering the inhabitants of regions where terrorist groups are most active and also have the most power politically and socially, such as Israel (Cohen-Louck [9]).

Instead, few words have been spent on more Western contexts. Rather, when wondering about the perception of terrorism within the European Union, for example, previous studies have limited themselves to analyzing the position of each Member State concerning terrorism, what is their stance on it, and the measures taken at the political and social level to combat this phenomenon (Bureš [6]).

Nevertheless, there is clearly a general tendency to forget, or at least underestimate, the perception of individuals residing within that geographic area.

This gap becomes even more critical when we move from the analysis of ter-

rorism to that of counter-terrorism measures and, in particular, online counter-terrorism.

As a matter of fact, the main goal of terrorist actions, especially those that take place on virtual platforms, is to spread fear among people and, at the same time, to influence them with their doctrine.

For these reasons, studying the perceptions of social media users regarding the phenomenon of terrorism on the one hand and the implementation of online counter-terrorism measures on the other allows us to understand how aware individuals are of the seriousness of this phenomenon.

Moreover, the European Union's measures to counter the spread of cyber-terrorism inevitably affect all social media users. Artificial Intelligence (AI) and algorithms that automatically filter everything posted online risk violating people's right to privacy and interfering with their right to expression.

As a result, European leaders need to have public support for the measures introduced to counter online propaganda because it means limiting resistance to their adoption.

For this reason, this paper aims to put a focus on what are the perceptions of these individuals regarding the phenomenon of terrorism, and the measures taken online to combat the spread of terrorist content on social platforms.

In addition, it has been shown by previous studies that Twitter, among all Social Media, is the preferred platform for political discussion (Davies [12]). Several academics have agreed that Twitter is the favorite social-network not only for leaders to communicate their initiatives and share their political positions, but also for the population to take part in political life and show their support (or dissent) regarding specific political issues (Spoladore [32] and Nguyen [22]).

Therefore, the present analysis will also focus on Twitter users' sentiment regarding the issue of cyber-terrorism and European anti-terrorism measures implemented online.

However, before embarking on the study of public opinion, a brief analysis of

the historical and evolutionary background of terrorism can help to get a clearer idea of what are the effects of this phenomenon on society.

Chapter 2

Cyber-terrorism background

2.1 From "traditional" terrorism to cyber-terrorism

As it turns out, it is not easy to find general agreement in defining the traits of terrorism and cyber-terrorism. However, tracing the historical evolution of this phenomenon can help the bodies responsible for combating terrorism understand the mechanisms that govern it and, consequently, develop defensive measures.

The entire world has experienced various forms of terrorism. While manifesting itself in various ways, it has always had the goal of carrying out mass slaughter and targeting civil society to assert political or religious ideas that differ from the prevailing ones.

The distinction into phases and the identification of turning points in the concept of terrorism, especially in the refinement of tactics and aims, underlies the process of reassurance to which the West aspires.

When discussing modern terrorism and its origins, the most supported theory is the "Four Waves of Modern Terrorism Theory" (David C. Rapoport). Rapoport's analysis is based on associating different contemporary global terrorist groups based on their shared ideology, strategy, and visions of the future. According to the Wave Theory, modern terrorism originated in Russia in the

1880s. In addition, regarding the main events that have been a turning point in the history of terrorism, there is no doubt that over the years, numerous terrorist incidents have been directed at ethnic cleansing or opposing the ruling political.

However, the September 11, 2001 attack on the Twin Towers shook public opinion more than others. This attack highlighted for the first time that terrorism is now a global phenomenon, no longer confined within the borders of one state. Moreover, it brought to light that combating it requires appropriate systems that ensure practical cooperation among states.

Moreover, terrorism has evolved both because of a transformation in the ideologies behind it and the impetus provided by the advent of new technologies. As Audrey Kurth Cronin states *"an innovation can result from an idea, practice, or technological development"*(Cronin [10]).

Further evidence of this is that contemporary terrorism uses modern technologies to establish itself and, in particular, it uses the extraordinary capacity of the media to spread terror worldwide. It is no longer essential to make striking actions like 9/11, but it is enough to perform a small act, as long as the media amplify it.

In fact, terrorism, to survive, needs to publicize the outcome of its devastation for the purpose, precisely, of terrorizing the population. Nowadays, more than ever before, terrorism feeds on itself.

Hence, cyberspace is the new frontier of terrorism because of the possibility of multiplying the message and spread ideals through the media. Today as never before, terrorist groups can reach anyone in any corner of the world. The ability to communicate in virtual space has allowed terrorism to reach a number of people previously unthinkable. More importantly, hyperspace has allowed terrorism to reach with extreme ease the very people who are the most important to them: young people. Indeed, young people are those who most approach the virtual world, those who spend most of their days connected online, navigating

between one social media outlet and another. In addition, young people, who are still developing their cultural and ideological backgrounds, are those most easily influenced and indoctrinated.

As the digital reality has become the focus of contemporary terrorist activity, an ad hoc term has been coined to refer to all terrorist activities that take place in this dimension: *"Cyber-terrorism."*

2.2 Cyber-terrorism faces

Cyberspace has the (unique) ability to even out political imbalances, which dominate international relations, by placing subjects of the most diverse nature on the chessboard: individuals, non-state actors, as well as states. These act on an almost equal playing field, thus disappearing all forms of asymmetry. In a "traditional" act of war, the physicality of those acting on land, at sea, or in the air makes the actors easily identifiable.

The same is not the case in cyberspace, where, because of its inherent digitized nature, it is very complex not only to impute the action promptly to one or more specific actors but also to understand the reason for the attack and its objectives, as much as, to prevent those who actually acted from easily evading all legal, political, diplomatic, economic and military responsibility.

This new "aspatial" dimension presents itself as "deterritorialized," "decentralized," and marked by simultaneity, anonymity, "depersonalization," and "detemporalization" of activities.

Defined as the "fifth domain of conflict" (Mbanaso and Dandaura [21]), it is poised to be the new battleground and geopolitical contest in the 21st century. A fascinating domain, constantly and rapidly evolving, it represents one of the most critical fields of international politics today and potentially tomorrow, as well as a real threat to national and international security.

Into this already complex context comes the so-called "Cyber-terrorism." Cyber-

terrorism is identified as a category of cyber threat and one of the new faces of terrorism.

Thanks to the inherent characteristics of cyberspace, the new terrorist strategy, from national and transnational, has now become globalized. In fact, the Net is shaping up as an ideal arena for terrorism because it represents a technology that offers easy access and allows it to reach a worldwide audience.

In the academic field, it is possible to find two defining orientations of cyber-terrorism: in the first, target-oriented, the Net is understood as the target and weapon; in the second, tool-oriented, the Net is referred to primarily as the tool and as the support (Singhal [31]).

As a matter of fact, terrorist organizations or individual terrorists use the Internet for different purposes: either to damage and compromise the computer systems or critical infrastructure of a given country (the Network constitutes the target and the weapon), or to carry out all the activities inherent to the management and survival of the terrorist organization, such as propaganda, fundraising, communication, and recruitment (the Network represents a tool).

In conclusion, cyber-terrorism can be declined in three different ways. It can take the shape of **cyber-crime** when primarily pursuing the interests of individuals through actions committed in violation of international and national legislation (where present) involving the use of computers. The acquisition of confidential data and fraud are among these crimes. Another shade of cyber-terrorism is **cyber-attack**, which aims to weaken or neutralize the computer systems under attack. Behind it is the desire to compromise a country's national security seriously. The ultimate goal is to cause the paralysis of the victim, publicly demonstrate its fragility, and disseminate terror in individuals. Finally, cyber-terrorism is closely related to the phenomenon of **propaganda**. Namely, the dissemination of terrorist content online to both spread fear and recruit new followers.

2.3 Contemporary terrorism and cyber-terrorism reality

Nowadays, terrorism in all its forms is a significant threat to democracy and the security of individual citizens.

In 2020, according to the 2021 EU Terrorism Situation and Trends Report, there were a total of 57 attempted terrorist attacks in Europe (including carried out, failed, and foiled attacks) (fig. 2.1). This is slightly higher than the 55 attempts in 2019. Moreover, between 2019 and 2020, the total number of deaths and injuries in the EU doubled from 10 deaths and 27 injuries in 2019 to 27 deaths and 54 injuries in 2020 (Europol [15]).

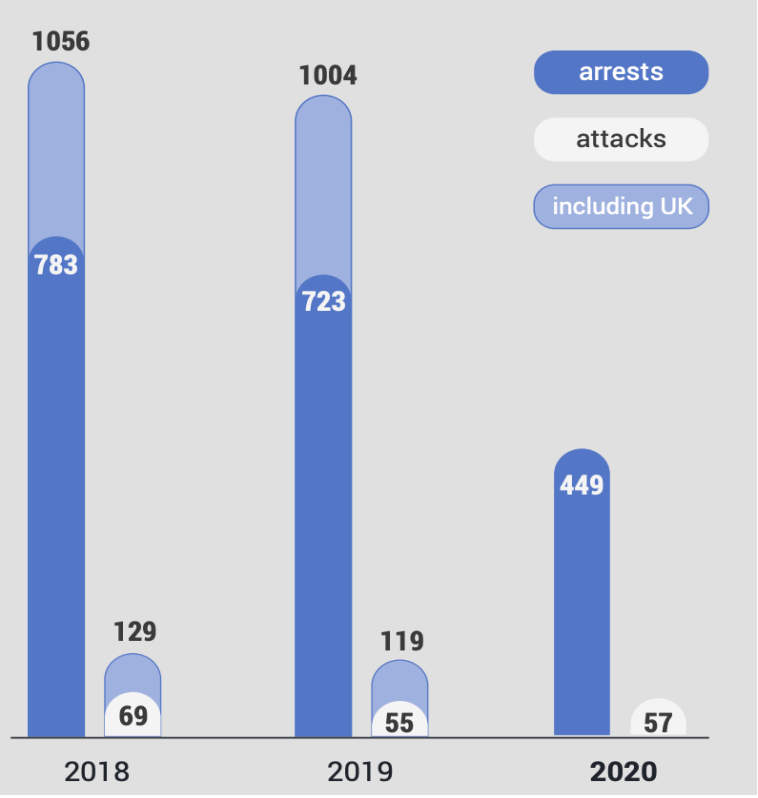

Figure 2.1: *Attacks and arrests on suspicion of terrorism in the EU*
Source: European Union Terrorism Situation and Trend report 2021

In any case, although the number of terrorist attacks in the EU remained stable

in 2020, extremists took advantage of the pandemic caused by Covid-19 to spread their ideological propaganda.

With the increase in the number of hours spent on the Internet during the pandemic, and the inability to continue their activities physically due to Covid-19 restrictions, online communities played a central role in radicalization.

As a result of efforts by messaging apps (such as Telegram, which took action in 2019 to prevent the spread of radical messages through its platform) to oppose terrorist groups, extremist propaganda has spread to other, often smaller, online platforms. For example, right-wing extremists, particularly young people, have often migrated to online gaming platforms.

These recent events, mainly due to the Covid-2019 global pandemic, have put the danger of online terrorism to modern societies even more under the magnifying glass. Indeed, it is clear that online media offered terrorism a quick and effective way to continue its activities, both propaganda and fear-mongering, even in such a crisis where physical actions and attacks were impossible to plan because of the lockdown in force. Hence, addressing terrorism on the physical territory is no longer enough because cyberspace and social media are the new favorite field of terrorists' action.

In an interview with The Guardian, Julian King, European Commissioner for the Security Union, said that almost every terrorist attack has had an online dimension in the last years. *"Either inciting or in some cases instructing, providing instruction, or glorifying"* (Boffey [4]).

Therefore, these circumstances have brought to light the need to develop and designate extraordinary measures and institutional bodies to combat the spread of terrorism in cyberspace.

Chapter 3

EU Counter-terrorism tools

3.1 The framework: an overview of European legislation on counter-terrorism and violent radicalization

Given the ever-present danger posed by terrorism, the European Union has increased its fight against this phenomenon in recent decades. Over the past two decades, the EU has implemented Directives and Acts intending to hinder terrorism, culminating in the recent days with the approval in April 2021 of the new European Regulation on countering the dissemination of terrorist content online.

To understand why the need to formulate this new Regulation was felt, it is helpful to trace a history of previous European directives adopted to counter terrorist acts.

After the devastating attacks of September 11, 2001, the European Union took note of the need to promote measures to prevent and combat international terrorism. The EU realized the need to act on two different fronts. The first one, of a repressive nature, aimed to foster the harmonization of criminal law norms in all Member States and strengthen the mechanism for judicial cooperation

and information exchange. The second was directed to implementing security and socio-cultural policies for disarming the very powerful weapon of violent radicalization.

On the first front, a series of crucial instruments were immediately adopted to ensure an effective judicial response to terrorism and transnational organized crime, including Framework Decision 2002/584/JHA on the European Arrest Warrant (European Union [14]), and Council Framework Decision 2002/475/JHA on combating terrorism, in which common standards of incrimination of terrorist conduct were established (E. Parliament and European Union [24]). In particular, with the latter, the importance of a common strategy for countering and preventing jihadist terrorism was recognized at the European level for the first time.

In the aftermath of the March 2004 attacks in Madrid and the July 2005 attacks in London, Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offenses was also adopted. The Decision requires each Member State to transmit relevant information to Eurojust, Europol, and the other Member States and designate an authority as Eurojust's national correspondent for terrorism-related matters. This discipline has been reinforced by the recent entry into force of the November 14, 2018 Regulation on Eurojust. This Regulation binds the Member States directly and concerns their obligations to fully and promptly transmit to Eurojust the information held by the competent national authorities.

On the side of countering radicalization and violent extremism, after the terrorist attacks in Madrid and London mentioned above, the Commission considered it necessary to direct strategies for preventing and countering terrorism not only through criminal law instruments, but also through measures inspired by the socio-historical, religious and ideological dimensions of the phenomenon. These measures are aimed at preventing any form of violent radicalization by supporting Member States in strategic areas, such as the development of effective

counter-narrative policies through the web and media, education and youth participation in social life, employment, issues related to inclusion and integration within a community, equality of opportunity, non-discrimination and intercultural dialogue.

Moreover, the prevention of terrorism and violent extremism has been identified in the European Security Agenda for 2015-2020 as the most urgent challenge, along with the fight against organized crime and cybercrime (Schiopu and Bobin [27]).

With particular reference to combating radicalization and proselytization occurring through the illegal use of the Internet, Directive 2017/541 introduced an obligation for Member States to take measures aimed at preventing online propaganda through the timely removal of online content that constitutes a public incitement to commit a terrorist offense (Caiola [7]).

3.2 European Union bodies playing a role in the fight against terrorism

The need to keep the guard up against the threat of terrorism has led the European Union to provide three bodies that offer indispensable support in the fight against terrorism. These are Europol, Eurojust, and the EU Counter-terrorism Coordinator.

3.2.1 Europol

The European Agency Europol function is to collect and analyze information and provide operational support in the investigation activities of member states. In recent years, its action has been essential in prosecuting cross-border crimes, especially with regard to drug trafficking and the prosecution of persons involved in terrorist activities. Within its framework, the Europol Information System

(EIS) was established: a database in which all information and data of suspects are collected.

Despite the successes that have been pursued, much remains to be done for Europol's role to become more effective. In particular, more cooperation with national authorities is needed, as their weak trust in Europol has a negative impact on information flow and data exchange.

3.2.2 Eurojust

The Eurojust Agency, since it was established, has among its tasks to facilitate counter-terrorism activities. In pursuit of this purpose, Eurojust coordinates investigations and prosecutions by national authorities dealing with cases of terrorism and severe forms of organized crime and, more generally, matters of judicial cooperation. Its work is carried out mainly at the operational level, providing information and strategic assistance through real teams of experts. Eurojust is also involved in establishing joint investigation teams that carry out fundamental investigations in cross-border criminal cases. No less significant is the action of coordinating parallel prosecutions involving judicial authorities of different member states and sharing experience gained in the field by organizing workshops and preparing reports and reports. However, Eurojust's activity is not limited to the operational level. In fact, it also plays a crucial role at the strategic level by sharing its experiences in supporting national authorities in counter-terrorism cases, as well as the results of its analyses, with practitioners and legislators at the European and national levels.

3.2.3 EU Counter-Terrorism Coordinator

Since the Madrid terrorist attacks in 2004, the European Union has had a Counter-Terrorism Coordinator. In July 2021, Ilkka Salmi has been named to serve in this position. He is responsible (as the *nomen juris* indicates) for

coordinating and monitoring the various activities that the European Union undertakes to combat terrorism. With this in mind, he works closely with the preparatory bodies of the Council, the Commission, and the European External Action Service (EEAS). In addition, very relevant is his power to make policy recommendations and signal to the Council the priorities to be pursued, and to monitor the implementation of the decisions taken. Finally, significant is its "external" role since it has the task of establishing forms of cooperation with third countries in the fight against terrorism, especially through a constant exchange of information.

These three European bodies cooperate at the institutional level to monitor terrorism trends over the years and to facilitate the work of European legislative authorities, which, thanks to the material provided by the three bodies, can formulate and implement more effective resolutions.
However, these agencies leave public awareness totally in the background. None of them sees it as one of their tasks to gather information regarding public opinion on terrorism and to plan "counter-propaganda" actions directed at the public. Therefore, at the institutional level, there are no teams dedicated to monitoring public opinion, particularly that manifested online. There are no bodies dedicated to assessing how to increase general approval for specific legislation. This lack makes it more difficult to protect people from being influenced by extremist ideologies, especially when they are spread through social media. This levity in considering people's perception of terrorism is also found in the new European Regulation designed precisely to limit the dissemination of terrorist content online.

Chapter 4

The need for new rules: The EU Regulation on addressing the dissemination of terrorist content online

4.1 Regulation content

Now, we can move on to an analysis of the new European Regulation on addressing the dissemination of terrorist content online (TERREG).
Following the provisional agreement between the Council and the European Parliament in December 2020 on a new Regulation regarding the dissemination of terrorist content and the Council's approval of the text on March 16, 2021, this Regulation was adopted by the Parliament on April 28, 2021.
The Regulation defines the responsibilities of the Member States and the obligations of hosting service providers (including social platforms such as Facebook, Twitter, YouTube, etc.) to effectively detect and remove online terrorist content from their platforms to counter the misuse of hosting services for the dissemination of terrorist content online.

De facto, the presence of terrorist content online has proven to be a catalyst for the radicalization of individuals that can lead to terrorist acts. Hence, it has serious negative consequences for users, and society as well as for online service providers hosting such content, as it undermines the trust of their users and harms their business models. Hosting service providers have special responsibilities to society in terms of protecting their services from misuse by terrorists and contributing to countering the spread of terrorist content through their online services.

Therefore, the legislation will apply to hosting service providers offering services in the Union, regardless of their principal place of business, to the extent that they disseminate information to the public. This also includes content that expresses controversial views in a public debate on sensitive political issues.

Thus, the competent authority in each Member State will have the power to issue a removal order requiring platforms to remove or block access to terrorist content throughout the EU. The removal of terrorist content is expected within one hour after receipt of the removal order.

Consequently, platforms will have to take specific, reasonable, and proportionate measures to protect their services from the dissemination of terrorist content. However, the choice of such measures is left to each of them. The Regulation clarifies that the hosting service provider could take various measures to combat the spread of terrorist content, including automated measures. In addition, if the competent authority finds that the specific measures put in place are insufficient, it may require the adoption of additional appropriate, and effective measures.

In order to ensure transparency, platforms will have to publish annual reports on measures implemented. Finally, member states will have to establish penalties applicable to violations of the Regulation by hosting service providers.

4.2 Regulation "concerns and challenges"

The adoption of this Regulation has brought with it numerous issues and criticisms.

The ensuing debate, among other things, stems from the fact that the European Union has failed to stress the need for this Regulation in people's eyes. In essence, the European Union, as much as it has been very active in dealing with the problem of the spread of terrorist content online, has not been as active in implementing strategies to raise public awareness of this issue.

At the same time, it has been shown that, over the years, individuals have become increasingly sensitive to issues related to the handling of their personal data (Custers et al. [11]). In particular, it has been shown that social media users have become less willing to make their data accessible to third parties. This is because users' trust in online service providers and the government bodies that regulate them has declined.

The main problem that has been identified with the implementation of the new European Regulation is that it incentivizes online platforms to use automated tools, such as filters on uploads, to remove content deemed to be "terrorist". An automated moderation system cannot distinguish between what is parody, satire, educational material, and truly terrorist content. As a result, content about news or evidence of war crimes or mistreatment of minorities will most likely be systematically removed, thus undermining our ability to inform or express ourselves freely.

Most worryingly, any EU country can issue an order to delete online content hosted anywhere in the EU within an hour without judicial oversight or control. This could pave the way for authoritarian regimes, such as those in Poland and Hungary, to silence their critics abroad by issuing content deletion orders beyond their borders, thus effectively extending their jurisdiction. Since this must happen within an hour, online platforms will have no choice but to comply with

these orders to avoid fines or legal problems. At the same time, the Regulation fails to resolve disagreements among EU states over what constitutes terrorism, irony, art, or news reporting.

For these reasons, on March 25, 2021, several civil society organizations had urged MEPs to vote against the adoption of the Regulation in an open letter. They pointed out that the Regulation "still contains dangerous measures that will ultimately weaken the protection of fundamental rights in the EU" (Letter [18]). They also said that the Regulation puts algorithms in charge of deciding what counts as free speech by giving more power to current opaque and unaccountable content moderation practices used by dominant platforms.

In this regard, according to Eliška Pírková, Europe Policy Analyst at Access Now, "to comply with the Regulation, many platforms will be able to use automated decision-making systems to remove content, which is problematic. Machine learning systems for detecting and identifying potentially illegal content are blind to context and make mistakes for which users' fundamental rights and freedoms pay the price." Indeed, while the Regulation does not compel the use of such systems, it does not prohibit it either.

To sum up, some concerns regarding fundamental rights remain. The Regulation continuously stresses the importance of implementing the legal instrument while preserving fundamental rights, such as the freedom of expression and the right to privacy. These remarks are contained both in the recitals and in many provisions of the legal text. It also provides that human oversight and verification should be in place where automated tools are used to detect terrorist content online. However, the Member States are entitled to designate their national competent authorities. Nevertheless, while the Regulation states that such competent authorities must carry out their duties in an objective and non-discriminatory manner, the suggestion of imposing a judicial review of the removal orders was not incorporated in the Regulation.

Therefore, these critical issues stem precisely from the fact that insufficient

attention has been paid to public opinion on terrorism. People not perceiving the seriousness of the phenomenon do not understand the need to implement a Regulation that invades so much of their privacy and potentially puts a brake on their freedom of expression.

Hence, underlying this paper is the idea that a more aware public opinion of the risk that terrorism in general, and cyber-terrorism specifically, poses can facilitate the counter-terrorism actions deemed necessary by the European Union.

For this reason, the next chapter analyses the sentiment of Twitter users in relation to terrorism and TERREG to explain why they did not welcome the implementation of the latter.

Chapter 5

Twitter users' sentiment analysis

5.1 Methodology

Granted that the study of public opinion can be a useful key for European leaders to implement efficient and widely supported counter-terrorism measures online, and considering that, to date, the European Union has not actively acted to raise awareness in this regard, the following chapter aims to give space to people's opinion through an analysis of Twitter users' sentiment. Specifically, it is intended to bring to light both how the social debate on terrorism has changed over the past ten years and what is the opinion of users regarding the TERREG Regulation.

Twitter turns out to be a highly relevant field of inquiry for two reasons: the first is that the Regulation whose public approval is to be analyzed has an impact precisely on the content posted by users of this social and their personal data. The second reason is that, as inferred from other studies, Twitter is the social media that, among all, lends itself most to political and institutional debate (Nusselder [23]).

Moreover, keeping in mind that, nowadays, social media can be considered the mirror of society (Suleiman et al. [33]; Manzoor [20]), through the consideration of how much the number of tweets has varied over the years, it is possible to

estimate how much the public's perception of the danger of terrorism has varied according to specific historical events.

To achieve this goal, this study combine quantitative and qualitative analysis. First, through a quantitative analysis of the number of tweets that have been posted from 2012 until May 2022, we intend to observe how the social debate on the topic of terrorism has varied over time. This time range encapsulates the most salient events of recent years in terms of terrorism. In 2014 the whole world witnessed the self-proclaimed Islamic State. In 2015, two of the most significant terrorist attacks occurred on European soil in recent years: the Madrid bombing and the attack on the Charlie Hebdo newspaper in Paris. In 2016, following the Brussels attack, the Extraordinary Council on Justice and Home Affairs stressed the need to agree on a code of conduct on hate speech that would involve private operators at the forefront. This led to the birth of the "Code of Conduct on the Unlawful Incitement of Hate Online" due to collaboration between the European Commission, Member States, and large IT companies (Facebook, Google, YouTube, Twitter, and Microsoft). In addition, 2019 saw the military defeat of Isis with the fall of its last bastion in Syria on March 23 of that year. However, this did not mean the end of attacks in Europe. In November 2020, a further attack occurred in Vienna. The need, therefore, to curb the power, especially dissemination, of terrorist groups led the European Parliament and the Council to approve in 2021 the Regulation on addressing the dissemination of terrorist content online.

That said, analyzing the magnitude of the media debate on Twitter allows us to understand how the salience of terrorism, particularly of the risk it poses to citizens around the world, has changed over the years.

In detail, the research was carried out as follows: through the use of keywords and hashtags such as "*#stopterrorism,*" "*#fighterrorism,*" "*#againstterrorism,*" and "*#antiterrorism,*" we downloaded all tweets from Twitter users who have commented on this phenomenon over the past ten years.

Using the same principle, I downloaded all tweets that contained the words or hashtags "*#cyberterrorism,*" "*#onlineterrorism,*" "*#stopcyberterrorism,*" and "*#stoponlineterrorism*" in this same time frame. In this way, it is possible to compare the trend of tweets related to the phenomenon of terrorism in general and those related to cyber-terrorism.

Second, we move from a quantitative to a more qualitative analysis. In fact, through a content analysis of tweets about the new European Regulation, we intend to analyze public sentiment about the same. Specifically, I downloaded all tweets published from September 12, 2018, the date the Commission proposed the EU Regulation, until May 31, 2022, containing the terms "online terrorism/terrorist, cyber-terrorism" and then selected only those that contained the words "EU Regulation" in turn. In addition, I downloaded all tweets containing the hashtag #TERREG ((official hashtag to refer to the Regulation in question). This principle was used to download tweets related to this topic in the five most widely spoken languages in the European territory: German, French, English, Italian, and Spanish.

Then each tweet was ranked according to three categories "positive," "negative," and "neutral."

This allowed consideration of the extent to which the European Regulation enjoys general approval and whether that approval has varied over time.

Furthermore, to better understand the motivations of the people who opposed the Regulation, I selected all the negative comments and analyzed their content in more detail to identify the root of their disagreement.

5.2 Findings

This type of analysis, which brings together a quantitative and a qualitative investigation, allows us to get a clear idea of the evolving social debate on terrorism and how external factors are influencing it.

5.2.1 Twitter users' discussion on terrorism

The data provided by the analysis regarding the number of tweets posted over the past decade on terrorism and cyber-terrorism specifically highlight how the debate on the social platform has varied considerably over the years. The graph depicted in Figure 5.1 shows the trend in the flow of tweets posted on the topic since January 2012.

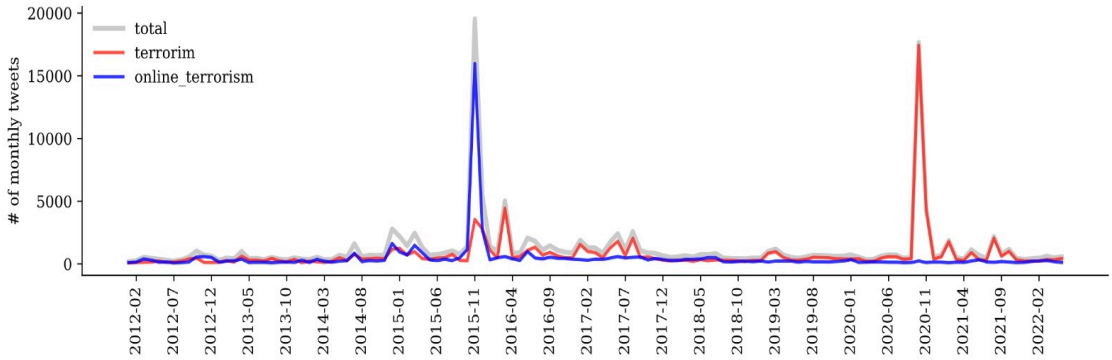

Figure 5.1: *Timeline tweets on Terrorism and Cyber-terrorism*
Source: author's elaboration on Twitter data

The graph shows a first noticeable rise in the curves representing both tweets related to terrorism in general and those related to cyberterrorism specifically corresponding to January 2015. On January 7, 2015, Isis attacked the headquarters of the Paris satirical newspaper Charlie Hebdo causing a significant shock throughout the world population. A swirling spike in the turns is subsequently recorded in November 2015. Indeed, that month saw one of the most meaningful terrorist attacks on European soil in recent years. A series of attacks in the French capital left a total of 130 people dead. The Brussels attack followed this in March 2016, then the Berlin attack in December 2016, the London and Paris attacks in June 2017, and the Barcelona attack in August of the same year, corresponding to the other peaks on the red curve that can be seen in Fig. 5.1. Following a period of calm, November 2020 saw the largest number of tweets posted on the topic of terrorism. Not coincidentally, in that month

Europe was again the stage for a terrorist attack that specifically hit the heart of the Austrian capital. Finally, the last increase in tweets is recorded in August 2021 when the Kabul airport was the victim of an attack by Isis.
From observing the graph in Fig. 5.1, it is evident that external events such as terrorist attacks in recent years are a powerful stimulus for social discussion. From this graphical representation, it would appear that Twitter discussion related to both terrorism and cyber-terrorism tends to cancel out during times of the year that are not marked by these tragic events. However, if we choose to represent the data through a logarithmic function, we can see more clearly the constant oscillation of the two curves (Fig. 5.2).

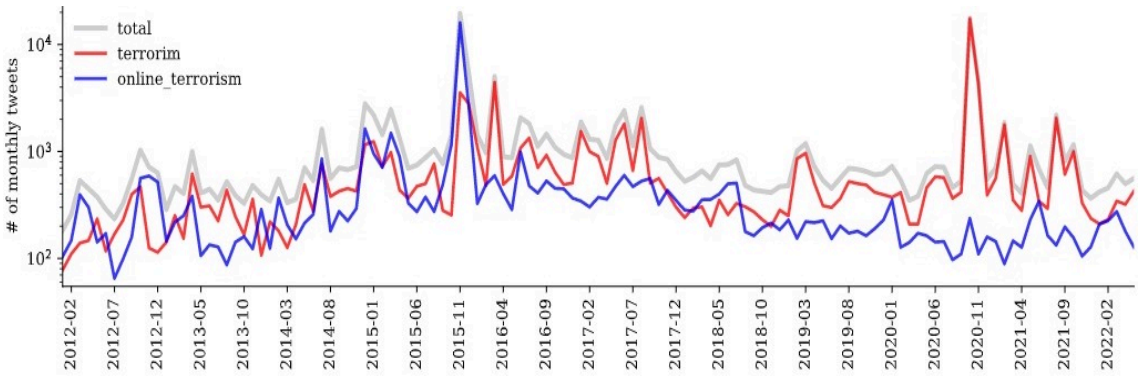

Figure 5.2: *Log. function of tweets on Terrorism and Cyber-terrorism*
Source: author's elaboration on Twitter data

Through this depiction, it is clear that terrorism is an ever-present topic on Twitter. This shows that terrorism is a topic that constantly occupies people's minds as it is an ever-present threat that, despite the efforts undertaken, is struggling to be eradicated. In addition, it can be seen that the two curves represented tweets about terrorism and those about cyberterrorism tend to diverge in recent years. In particular, the number of tweets posted on the topic of cyberterrorism is gradually decreasing. This tendency is most visible in the graph depicted in fig. 5.3. It shows that in the overall discourse on terrorism, cyberterrorism occupies a decreasing percentage. This demonstrate

that the public to date is not sufficiently aware of this issue, tending at times to underestimate it.

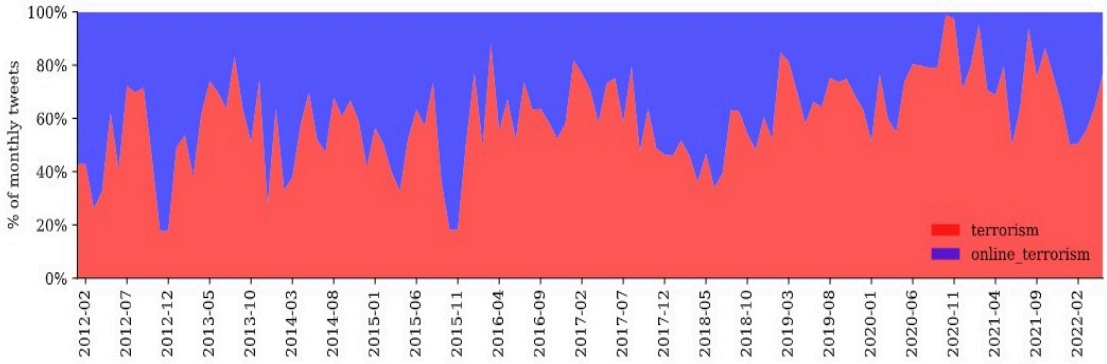

Figure 5.3: *Percentage of tweets on Terrorism and Cyber-terrorism*
Source: author's elaboration on Twitter data

5.2.2 Twitter users' sentiment on the new EU Regulation

The second part of my research focuses on people's opinion in relation to the TERREG Regulation. Of the 3857 tweets analyzed, less than 5% consider the Regulation introduced by the European Union to be a positive factor for society. On the contrary, the majority of tweets (75.8%) do not agree with the implementation of this Regulation, and 19.2% of them do not have a definite opinion about it yet (Fig. 5.4). From these numbers, it is easy to infer that public opinion did not welcome the introduction of the new European Regulation. Even when Twitter users recognized the importance of combating the dissemination of content propagandizing radical ideals, they did not likewise consider the control measures that the Regulation introduces to be necessary or at least effective.

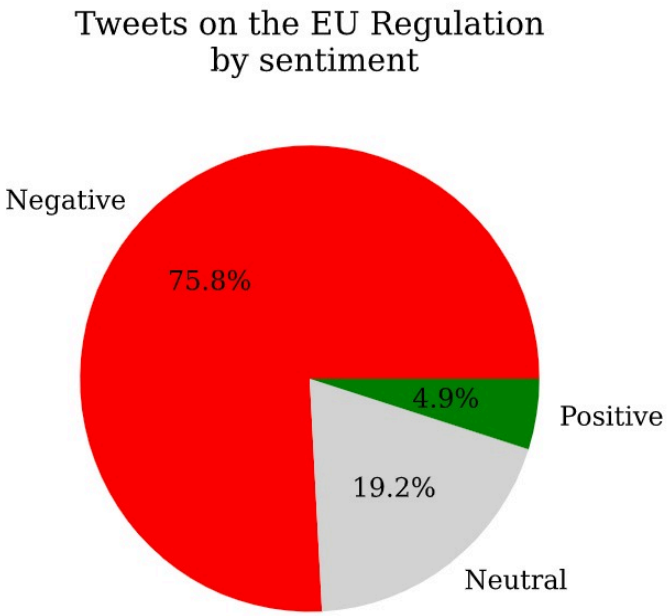

Figure 5.4: *Percentages of tweets on the EU Regulation*
Source: author's elaboration on Twitter data

In addition, public opinion has remained the same over the years (Fig. 5.5). From the time the Regulation was proposed until today, the number of negative tweets has consistently remained higher than the number of positive tweets. Notably, even during the periods when the Regulation was most "publicized" on social media by the official accounts of the European institutions in March 2019, November 2020 (months when the trilogues between the Commission and parliament took place), and April 2021 when the Regulation was approved, the general sentiment of users remained strongly negative.

These data show that the EU has not been efficient in communicating the urgency of such Internet regulatory measures and has not paid enough attention to the needs of its citizens.

The general unhappiness aroused by this Regulation may be a severe problem for the EU, which has set itself the goal of returning to discuss the effectiveness of these measures in 2024, two years after their implementation. Indeed, on that occasion, the European Parliament and the Council may decide to revoke

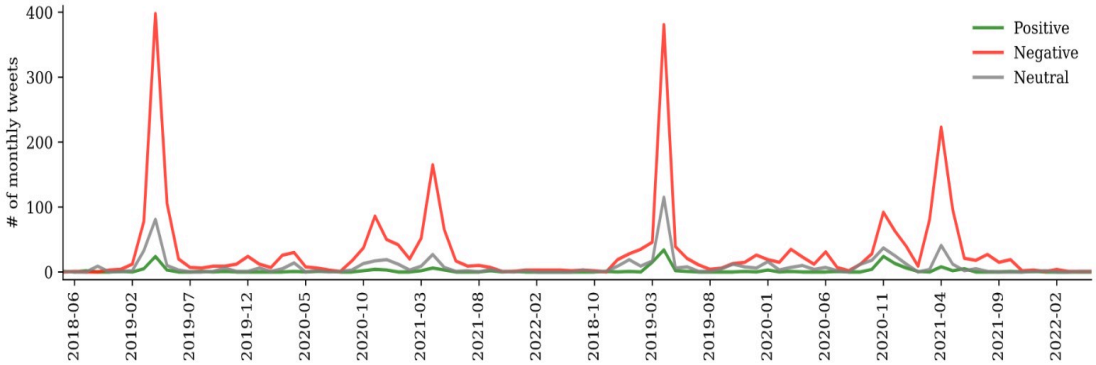

Figure 5.5: *Timeline of tweets on the EU Regulation*
Source: author's elaboration on Twitter data

the Regulation if they conclude that it has done more harm than good to the European community.

Therefore, it becomes interesting to understand what reasons people had for opposing the Regulation under consideration. Analysis of the content of the negative tweets allows us to take a step in this direction. The argument brought forward by the majority of opponents is that this Regulation violates people's fundamental rights. Specifically, they believe that the measures introduced by TERREG excessively restrict their freedom of expression online and their right to privacy. Another recurring theme in the negative tweets concerns criticism of the European Union. In fact, some users argue that the EU does not represent the interests of its citizens because it is too focused on achieving economic and political goals. The third group of users is represented by those who exploit TERREG only to criticize the actions of a particular party and support another. Finally, a small minority criticizes the European Regulation because they believe that limiting the spread of radical content online does not serve to defeat the threat of terrorism. Figure 5.6 shows the percentages of these four main matrices that fuel the negative sentiment of Twitter users.

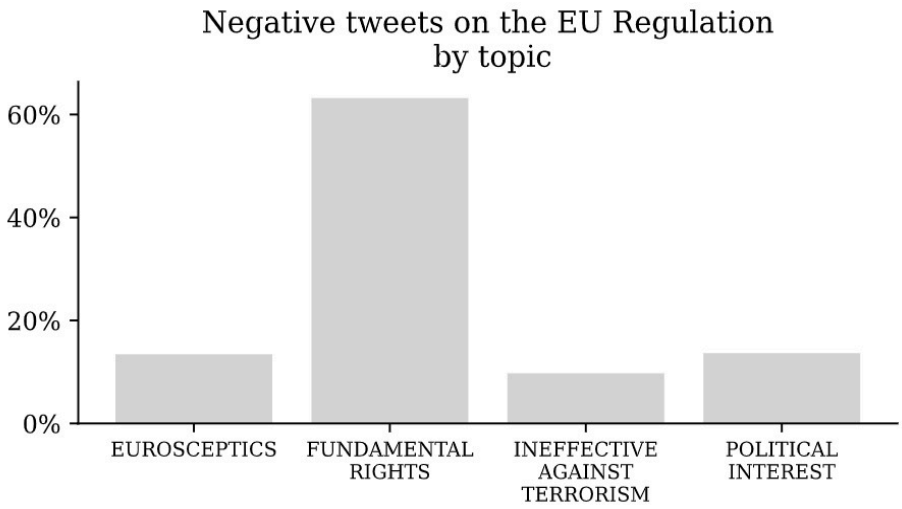

Figure 5.6: *The main matrices of negative sentiment*
Source: author's elaboration on Twitter data

From the graph in fig.5.6, it is evident that although it is possible to identify four different streams of thought behind the negative tweets, the argument of violation of citizens' fundamental rights is by far the most present.

Conclusion

Terrorism is a concern that has plagued our society for centuries. It is constantly evolving. By renewing itself and transforming its strategies of action, it continues to test the defensive mechanisms of our governments. Indeed, contemporary terrorism has appropriated all the innovations of the modern world. "Money and financial speculation, information technologies and aeronautics, the production of spectacle and media networks: they have assimilated all of modernity and globalization, while maintaining their aim to destroy it" (Baudrillard [3]). As we have seen, the advent of digitization and, in particular, that of social media has been another turning point for terrorist action. Terrorists have seen in social platforms the possibility of spreading widespread fear, recruiting new followers, and facilitating communication among members of the terrorist group. All in immediate ways and at exponential levels, managing to reach previously unimaginable numbers of people.

This has led democratic institutions to deal with this new form of terrorism, better identified as Cyber-terrorism. At the European level, the European Union, over the years, has tried to refine its counter-terrorism strategies more and more. It has not only introduced directives and acts to counter terrorism but has also established institutional bodies responsible for monitoring terrorist activities on European territory and managing cooperation between all member states and government bodies. Moreover, just to protect its citizens from cyber-terrorism, the Commission and the European Parliament approved in April 2021 a Regulation aimed at countering the dissemination of terrorist content online.

In addition, because terrorism by definition aims to target the people, it represents a salient topic for public opinion.

As demonstrated by data on the Twitter debate about terrorism and cyber-terrorism, users of the Social Network have never left the discussion over the past decade. There is a consistent awareness among Twitter users of the salience of this phenomenon. As might be expected, salience tends to increase in proximity to the terrorist attacks that have put our democracy on high alert in recent years.

However, what is most interesting is that although people are sensitive to the threat posed by terrorism and cyber-terrorism, this sensitivity loses relevance when dealing with the control measures introduced by the European Regulation to address the dissemination of terrorist content online. The analysis of the sentiment of tweets about TERREG showed that about 75% of them are critical of the Regulation.

This percentage finds an explanation if we look at the main reasons that led these people to oppose the Regulation. As we saw in the previous chapter, the primary matrix at the root of these tweets lies in the debate about users' fundamental rights (freedom of expression and the right to privacy). In this case, the opposition gets strength from a much larger argument that fuels the discussion between those who want to regulate the digital world and those who instead are advocates of a free Internet. That argument is: to place limitations on the Internet means to place limitations on individuals' freedom of expression and, at the same time, invade their privacy. This critical issue completely shifts users' focus from the "danger of terrorism" to the "danger of filters." Consequently, even if the pursued goal of the European Regulation is "noble," it is unable to gain public support. Accordingly, having neglected the latter when drafting the Regulation could be a fatal move for the EU, which may be forced to withdraw TERREG during the evaluation of its effectiveness scheduled for 2024.

A second interesting matrix behind the opposition to the Regulations also originates from a debate that goes beyond terrorism, namely the one between "Europeans" and "Euroskeptics." Many have simply used TERREG to criticize a European Union that they feel no longer represents them. They have taken a stand against an EU that, in their view, has no interest in its citizens but caters only to a small elite of individuals. Their argument is based on the fact that they see European institutions as more concerned with pursuing the economic and political interests of the Union and its member states than interested in safeguarding the rights of the society they represent.

As expected, no one opposed the Regulation because they thought terrorism was not an issue. And very few said that these restrictions would not serve to defeat terrorist groups. Instead, the most popular view was that these restrictions, in addition to filtering out terrorist content, would limit users' freedom of speech. This view stems from the fact that the EU has not sufficiently considered that when dealing with social media and its regulation, one is immersed in a much larger context and touches on issues that transcend the specific situation. The EU did not dwell sufficiently on what the implications of this Regulation would be for users, completely neglecting what their opinion on the matter might have been. Hence, a greater focus on the fundamental rights of citizens and more public awareness of the urgent need to curb cyber-terrorism would have helped the EU to ensure that people's attention remained on terrorism and was not lost in broader issues.

In conclusion, we should not think that politics and user freedom are mutually exclusive. Rather, it is true that in this occasion the right balance has not been achieved. In this regard, it might benefit the EU to shift the focus from a purely "State view" to one more interested in society and its citizens.

Bibliography

[1] RW Apple Jr. "Thatcher urges the press to help 'starve'terrorists". In: *The New York Times* 16 (1985).

[2] Imran Awan. "Cyber threats and cyber terrorism: The internet as a tool for extremism". In: *Policing Cyber Hate, Cyber Threats, and Cyber Terrorism* (2012), pp. 21–38.

[3] Jean Baudrillard. *The spirit of terrorism*. Verso Books, 2013.

[4] Daniel Boffey. "Remove terror content or be fined millions, EU tells social media firms". In: *The Guardian* (2018).

[5] Mitko Bogdanoski and Drage Petreski. "Cyber terrorism–global security threat". In: *Contemporary Macedonian Defense-International Scientific Defense, Security and Peace Journal* 13.24 (2013), pp. 59–73.

[6] Oldřich Bureš. "Perceptions of the terrorist threat among EU member states". In: *Studies* 46.1 (2008), p. 7.

[7] Antonio Caiola. "The European Parliament and the Directive on combating terrorism". In: *ERA Forum*. Vol. 18. 3. Springer. 2017, pp. 409–424.

[8] Gerard Chaliand and Arnaud Blin. *Storia del terrorismo: dall'antichità ad Al Qaeda*. Utet Università, 2007.

[9] Keren Cohen-Louck. "Perception of the threat of terrorism". In: *Journal of interpersonal violence* 34.5 (2019), pp. 887–911.

[10] Audrey Kurth Cronin. *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press, 2019.

[11] Bart Custers, Simone van Der Hof, Bart Schermer, Sandra Appleby-Arnold, and Noellie Brockdorff. "Informed consent in social media use-the gap between user expectations and EU personal data protection law". In: *SCRIPTed* 10 (2013), p. 435.

[12] Catherine Evans Davies. "Twitter as political discourse". In: *Discourse Approaches to Politics, Society and Culture (DAPSAC)* (2015), p. 93.

[13] Eugenia Dumitriu. "The EU's definition of terrorism: the council framework decision on combating terrorism". In: *German law journal* 5.5 (2004), pp. 585–602.

[14] Council of the European Union. "Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States". In: *Official Journal of the European Union* 50.18.07. 2002 (2002), pp. 3–18.

[15] TESAT Europol. "European Union Terrorism Situation and Trend report". In: *European Police Office* (2021).

[16] HM Government. *National cyber security strategy 2016-2021*. 2016.

[17] Arne Hintz, Lina Dencik, and Karin Wahl-Jorgensen. *Digital citizenship in a datafied society*. John Wiley & Sons, 2018.

[18] Open Letter. "Joint Letter to EU Parliament: Vote Against Proposed Terrorist Content Online Regulation". In: *Human Rights Watch Archives* (2021).

[19] Ariel Victoria Lieberman. "Terrorism, the internet, and propaganda: A deadly combination". In: *J. Nat'l Sec. L. & Pol'y* 9 (2017), p. 95.

[20] Amir Manzoor. "Social Media as Mirror of Society". In: *Handbook of Research on Advanced Data Mining Techniques and Applications for Business Intelligence*. IGI Global, 2017, pp. 128–141.

[21] Uche M Mbanaso and Eman S Dandaura. "The cyberspace: Redefining a new world". In: *IOSR Journal of Computer Engineering* 17.3 (2015), pp. 17–24.

[22] Timothy Nguyen. "Twitter: a Platform for Political Discourse or Social Networking". In: *Global Tides* 5.1 (2011), p. 11.

[23] André Nusselder. "Twitter and the personalization of politics". In: *Psychoanalysis, Culture & Society* 18.1 (2013), pp. 91–100.

[24] European Parliament and Council of the European Union. *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.

[25] The European Parliament and the Council of the European Union. "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on addressing the dissemination of terrorist content online". In: *Official Journal of the European Union* (2021), pp. 1–31.

[26] Ben Saul. "Definition of "terrorism" in the UN Security Council: 1985–2004". In: *Chinese Journal of International Law* 4.1 (2005), pp. 141–166.

[27] Aura Schiopu and Florin Bobin. "European Agenda on Security for 2015-2020, Instrument Supporting the Joint Action of the Member States against the New Challenges". In: *Eur. J. Pub. Ord. & Nat'l Sec.* (2015), p. 33.

[28] Alex Schmid. "Terrorism-the definitional problem". In: *Case W. Res. J. Int'l L.* 36 (2004), p. 375.

[29] Timothy Shanahan. "The definition of terrorism". In: *Routledge handbook of critical terrorism studies* (2016), pp. 103–113.

[30] Charanjit Singh and Wangwei Lin. "Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising". In: *Journal of Money Laundering Control* (2020).

[31] Vipin Singhal. "Cyberterrorism: An Overview". In: *Available at SSRN 2427059* (2014).

[32] Daniele Spoladore. "La comunicazione politica sui social network: un'analisi linguistica". In: *Italiano LinguaDue* 6.1 (2014), pp. 202–231.

[33] Alhaji Ahmad Suleiman, Abdullahi Kamba Manir, and Usman Mohammed. "UNDERSTANDING SOCIAL MEDIA AS MIRROR TO CONTEMPORARY SOCIETY". In: *British International Journal of Education and Social Sciences* 8.7 (2021), pp. 1–13.

[34] UNICRI and UNCCT. *COUNTERING TERRORISM ONLINE WITH ARTIFICIAL INTELLIGENCE*. United Nations Office of Counter-Terrorism, 2021, pp. 1–50.

[35] Gabriel Weimann. *Terrorism in cyberspace: The next generation*. Columbia University Press, 2015.