universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Conceptual foundations for the analysis of cyberterrorism in the European Union: Privacy and Security“

verfasst von / submitted by

Marco Aurelio Navarro Roux

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 884
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Master of Arts in Human Rights
Betreut von / Supervisor:	Dr. Anne Charbord

„*Terrorism is fundamentally the denial and destruction of human rights.*

The fight against terrorism must uphold those values, or it will never succeed.“

Antonio Guterres

Secretary- General of the United Nations

Statement at the opening of the first United Nations High-level Conference of Heads of Counter- Terrorism Agencies of Member States.

New York, 28 June 2018

Acknowledgments

I feel fortunate to have been a part of this two-year Master of Arts in Human Rights programme, ending with this thesis on Countering Cyber-Terrorism: Surveillance and the right to privacy in the context of the European Union. I feel privileged and thankful to have had the opportunity to study in such a spectacular university, and especially in this incredible and exciting programme with some of the best and brightest experts in the field. Thank you for this experience.

For their constant motivation and inspirational teachings, I would like to thank the Director of the Master of Arts in Human Rights, Dr. Manfred Nowak, the Coordinator Ms. Marijana Grandits, as well as Mr. Georges Younes and Ms. Sabine Mann. I am also grateful to my fellow students and every member of the Human Rights family of the University of Vienna. Their time, energy and knowledge enriched my academic work and understandings.

I would also like to extend my special gratitude and appreciation to my thesis supervisor, Dr. Anne Charbord, for her constructive advice and encouragement that provided me with the necessary direction and focus on my study. Her guidance helped me throughout the research and writing process of this thesis.

I wish to thank all the Staff members of the Terrorism Prevention Branch of the United Nations Office of Drugs and Crime, especially the Implementation Support Section 1 (ISS1) for allowing me the privilege to contribute to the inspirational work they do around the world and their commitment to the fight against terrorism.

In addition, I would like to thank my family (Dad, Mom, Etzel y Rafa) and friends for their unconditional love and guidance; and to my fellow colleagues for their constant support and encouragement. The warmth that everyone has showed has made up for all the Viennese winter days. My heartfelt thanks to my dear friends Ms. Nathalie Zamaira, Mr. Felix Steigmann and Mr. Jean-David Ott, who have, in their own ways, kept me going on my path, have stood by me when things got rough and for ensuring that good times keep flowing.

Finally, I dedicate this Master Thesis to my baby twins, Marco and Cesar. You have made me stronger, better and more fulfilled than I could have ever imagined. You are always in my mind.

Note from the author

The choice to research on "Countering Cyberterrorism: Surveillance and the protection of the right to privacy in the context of the European Union" is the result of a long period of reflection and self-analysis. Terrorism has become a persistent threat to international peace and security, and a permanent alert in people´s lives. During my time living in Europe, I have witnessed the fear and anxiety that has repeatedly struck Europe, triggered by terrorism (e.g. Paris attacks in November 2015 or Brussels in March 2016). Yet, it often seems as if governments have forgotten that the fight against terrorism is in fact, a fight for the very values of human rights.

Additionally, my professional experience at the Terrorism Prevention Branch (TPB) of the United Nations Office of Drugs and Crime (UNODC) encouraged me to delve more deeply in the topic. The six-month internship at TPB was an ideal opportunity to understand and familiarize myself with the international legal framework under which the fight against terrorism is being carried out and the many challenges faced in dealing with such a complex topic. TPB was created to provide counter terrorism technical assistance to United Nations Member States by supporting and strengthening their capacity while promoting Human Rights and the rule of law.

Terrorists can use different channels to operate and attacks can have diverse impacts. As we continue to move into a society more reliant on technology, the threat posed to nations from terrorists is no longer only physical, but it also expands to our digital world. Cyber-terrorism is a serious issue for domestic and international security. At the same time, with the rise in the use of communication technologies, privacy has become a challenging issue in modern age. To prevent and counter cyberterrorism, governments have become more inclined to use tools for surveillance or espionage in different forms that may infringe individuals´ rights, especially the right to privacy. The protection of privacy, however, represents a fundamental principle for all democratic societies obeying the rule of law.

The knowledge I gained during my internship at TPB, as well as the human rights-based approach I used to write this thesis contributed to my overall understanding of the modern threats and concrete challenges faced by European Union member states to ensure citizens a secure and terror free digital Europe while protecting the right to privacy.

Abstract

Privacy is a human right enshrined in the Universal Declaration of Human Rights and many international treaties. The need for privacy is inherent to every human being. The notion of privacy, however, is complex; it has many dimensions and many legal implications. The protection of privacy is not only physical or territorial; it is increasingly becoming an online challenge.

The right to security is also a broad notion that links with other human rights. It is essential for the wellbeing of any person, society and even humanity. With the fast-paced increase of the use of Internet in our everyday lives, and the increasing dependence on its access, new threats to security emerge, such as cyberterrorism. Since cyberterrorism is carried out through cyber space, it is extremely difficult to prevent, investigate and counter.

Surveillance is often used as an instrument to investigate individuals and organizations in order to prevent and combat terrorist attacks and terrorist groups, including those in the cyberspace. However, this instrument has a direct impact on the right to privacy. Modern technology allows law enforcement, intelligence agencies and private companies to collect and store data about individuals and infiltrate into every aspect of their lives, without suspicion of crime. Mass surveillance consists of the recording and indiscriminate storage of human actions.

This Master thesis aims to analyse the challenges that arise in the pursuit of the protection of the right to privacy, when countering and preventing cyberterrorism through surveillance programmes in the European Union.

Keywords:
Cyberterrorism, surveillance, counter terrorism, the use of Internet for terrorist purposes, right to privacy, right to security, European Union

Kurzfassung

Die Privatsphäre ist ein Menschenrecht, das in der Allgemeinen Erklärung der Menschenrechte und vielen anderen internationalen Verträgen verankert ist. Das Bedürfnis nach Privatsphäre wohnt jedem Menschen inne. Das Verständnis von Privatsphäre ist jedoch komplex; er hat viele Dimensionen und viele rechtliche Implikationen. Zudem ist der Schutz der Privatsphäre nicht nur auf physischer oder territorialer Ebene relevant, sondern wird zunehmend zu einer Online-Herausforderung.

Auch das Recht auf Sicherheit, das mit anderen Menschenrechten in Verbindung steht, ist breit gefächert. So ist es für das Wohlergehen jedes Menschen, jeder Gesellschaft und sogar der Menschheit im Ganzen von wesentlicher Bedeutung.

Mit der rasanten Zunahme der alltäglichen Internetnutzung und der zunehmenden Abhängigkeit vom Zugang zu dieser entstehen neue Bedrohungen für die Sicherheit, wie etwa Cyberterrorismus. Da der Cyberterrorismus über den Cyberspace stattfindet, ist es äußerst schwierig, ihn zu verhindern, zu bekämpfen und Ermittlungen einzuleiten.

Überwachung wird häufig als Instrument zur Ausforschung von Einzelpersonen und Organisationen eingesetzt, um Terroranschläge zu verhindern, und terroristische Gruppen, auch im Cyberspace, zu bekämpfen. Dies hat jedoch direkte Auswirkungen auf das Recht auf Privatsphäre. Moderne Technologien ermöglichen es Strafverfolgungsbehörden, Geheimdiensten und privaten Unternehmen, Daten über Einzelpersonen zu sammeln, zu speichern und so in jeden Aspekt ihres Lebens einzudringen, auch ohne den Verdacht einer Straftat. Massenüberwachung ist die Erfassung und wahllose Speicherung menschlicher Handlungen.

Diese Masterarbeit zielt darauf ab, die Herausforderungen hinsichtlich des Rechts auf Privatsphäre zu analysieren, die sich aus der Bekämpfung und Prävention von Cyberterrorismus durch Überwachungsmaßnahmen in der Europäischen Union ergeben.

Schlagwörter:
Cyberterrorismus, Überwachung, Terrorismusbekämpfung, Internetnutzung für terroristische Zwecke, Recht auf Privatsphäre, Recht auf Sicherheit, Europäische Union

List of Abbreviations and Acronyms

- AFSJ: Area of Freedom, Security and Justice
- AI: Artificial Intelligence
- APT: Advanced Persistent Threat
- CBRN: Chemical, Biological, Radiological and Nuclear (Terrorism)
- CCPR: International Covenant on Civil and Political Rights
- CFR: Charter of Fundamental Rights of the European Union
- CFSP: Common Foreign and Security Policy
- CoE: Council of Europe
- CSDP: Common Security and Defence Policy
- CTED: Counter- Terrorism Executive Directorate
- CTC: Counter-Terrorism Committee
- CTITF: Counter- Terrorism Implementation Task Force
- EC3: European Cybercrime Centre
- ECTC: European Counter Terrorism Centre
- ECJ: European Court of Justice
- EMPACT: European Multidisciplinary Platform Against Criminal Threats
- ENISA: European Union Agency for Network and Information Security
- EP: European Parliament
- EPCIP: European Programme for Critical Infrastructure Protection
- EU: European Union
- EUCTF: European Cybercrime Task Force
- EU IRU: European Union Internet Referral Unit
- EUROPOL: European Union Agency for Law Enforcement Cooperation
- GDPR: General Data Protection Regulation
- GIFTC: Global Internet Forum to Counter Terrorism
- GII: Global Information Infrastructure
- GSA: Global Security Agenda
- GSI: Global Security Index
- GSMA: Global System for Mobile Communications Association
- HTTPS: Hyper Text Transfer Protocol Secure

- ICC: International Criminal Court
- ICT: Information and Communication Technologies
- ICSANT: International Convention for the Suppression of Acts of Nuclear Terrorism
- IED: Improvised Explosive Device
- IOCTA: Internet Organised Crime Threat Assessment
- INTERPOL: International Criminal- Police Organization
- IP: Internet Protocol
- ISP: Internet Service Providers
- ITU: International Telecommunications Union
- NATO: North Atlantic Treaty Organization
- NGOs: Non-Governmental Organisations
- OPCW: Organisation for the Prohibition of Chemical Weapons
- OSCE: Organisation for Security and Cooperation of Europe
- OSP: Online Service Providers
- TCP: Transmission Control Protocol
- TFEL: Treaty on the Functioning of the European Union
- TPB: Terrorism Prevention Branch
- UN: United Nations
- UNCRC: United Nations Convention on the Rights of the Child
- UNESCO: United Nations Educational, Scientific and Cultural Organisation
- UNGCTS: United Nations Global Counter- Terrorism Strategy
- UNODC: United Nations Office on Drugs and Crime
- URL: Union Resource Locator
- VPN: Virtual Private Network
- WMD: Weapons of Mass Destruction

Table of Contents

„Conceptual foundations for the analysis of cyberterrorism in the European Union: Privacy and Security“ 1
Acknowledgments 5
Note from the author 7
Abstract 9
Kurzfassung 10
List of Abbreviations and Acronyms 12
Table of Contents 15
Methodology 17
1. Introduction 19
2. The Right to Privacy 33
2.1 Defining Privacy: its origins and its importance 40
2.2 The use of the internet and threats to privacy 42
3. The use of the internet for terrorist purposes 47
3.1 Cyberspace 52
3.2 Cyberattacks 56
3.3 Cyberterrorism 59
3.4 Countering Cyberterrorism 65
4. Policy and Legislative Framework 88
5. Conclusions 89
References 94
Legal texts: 100
European Union Instruments 101
Resolutions: 103
Journal Articles: 103
Online Newspapers Articles: 106
Thesis 107
Other 108

Methodology

The methodology used for this thesis is based on the document analysis of theoretical data by the means of research. Document analysis has a tendency to reveal in-depth insight of the reasons and motivations behind decision-making and allows for a thoughtful analysis from different perspectives and notions. This theoretical analysis largely contributes to an exploratory research and it is used to gain an understanding of underlying opinions, to acquire new insight, to collect and analyse evidence, and present findings that resolve issues. The reason to use a qualitative method of data collection was motivated by the fact that the present research aims to understand the challenges of the protection of the right to privacy in the European Union when countering cyberterrorism, which are hardly accessible through the quantitative method of data collection. Diverse academic material, international organisation´s publications, news media, as well as international and regional legal frameworks and standards were used to support and discuss my arguments.

This thesis aims to answer the research question "To what extent could surveillance programmes used by European Union Member States to counter cyberterrorism be implemented without infringing the right to privacy?" I will divide the answer to the question in two main parts: 1) the use of internet to create terrorist attacks and the methods used to counter it, such as surveillance, and 2) the existing European legal framework used to counter cyberterrorism, including its gaps and challenges, if any, at domestic levels in the context of the European Union countries. These include, national subjectivity in the evaluation of proportionality of restrictions to the right to privacy when dealing with the collective right to national security. Ultimately, I aim to analyse how the European Union pursues respect for the right to privacy when preventing and countering cyberterrorism.

1. Introduction

> *In countering terrorism, Human Rights protections are not secondary, they are not irrelevant and they remain integral to the long term success of counter-terrorism measures.*[1]

The notion of human rights lays on the idea that all individuals, no matter who they are, how they are or where they are born are inherently entitled to the same basic rights and freedoms. Indeed, human rights are the basic rights and freedoms based on shared values of dignity, fairness, equality and respect. They are often expressed and guaranteed by law in forms of constitutions, treaties, general principles, customary international law, and other sources of international law.[2] Human rights, however, are not privileges and they cannot be granted or revoked. They are inalienable and universal.[3]

Privacy is a fundamental human right recognised in the Universal Declaration of Human Rights (UDHR), the International Covenant of Civil and Political Rights (ICCPR) and in a great number of international and regional treaties at a European Union (EU) level, like the European Convention on Human Rights (ECHR). Therefore, the protection of the right to privacy represents a basic and fundamental principle for all democratic societies obeying the rule of law.

Privacy, however, is a complex notion with many dimensions, and legally, it has many implications. Nonetheless, there are many on-going discussions about the concept of privacy and its importance for humanity and human development[4]. According to professor emeritus of psychology from Duquesne University, Constance T. Fisher in her

---

[1] Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Remarks on promotion and protection of human rights at the Third Committee*, 23rd meeting – General Assembly, 72nd Session, New York, 18 October 2017. Available from: http://webtv.un.org/topics-issues/non-governmental-organizations/action-internationale-pour-la-paix-et-le-d%C3%A9veloppement-dans-la-r%C3%A9gion-des-grands-lacs/watch/fionnuala-n%C3%AD-aol%C3%A1in-special-rapporteur-on-promotion-and-protection-of-human-rights-at-the-third-committee-23rd-meeting-general-assembly-72nd-session/5613073854001/?term=&page=6&sort=date (accessed 30 June 2019).

[2] United Nations Human Rights Office of the High Commissioner [website]. Available from: https://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx (accessed 20 June 2019).

[3] Universal Declaration of Human Rights, Article 1.- "All human beings are born free and equal in dignity and rights."

[4] William C. Bier, ed., *Privacy: A vanishing value?,* Fordham University Press, New York, 1980, p. 4.

research on *Privacy and Human Development*, "privacy is a facet of the complex structure of growing and maturing" and it provides "an opportunity to get in touch with one's self while not worrying centrally about other people's judgment".[5]

With the rise in the use of communication technologies, privacy has become a challenging issue in modern age. The right to privacy relates to the protection of private life and it extends to the digital world. Ben Emmerson, former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, defined privacy as a fundamental human right that provides individuals with "an area of autonomous development, interaction and liberty."[6]

In the same vein, the right to security is essential to the wellbeing of any person, societies and even humanity. Under the idea that, if society, with the government as a central force, can guarantee that our homes, communities, and lives are safe, if we are confident that we will not, at any random moment, be killed or imprison without a just reason, then we are free to do something of ourselves, and pursuit a peaceful and happy life. In general terms, all people share the ambition to have a just and fair life, in their private and public life, and desire to live free from fear of attack, loss of life, arbitrary arrest, coercive interrogation or torture. For that reason, the right to security is enshrined in international human rights treaties and constitutions around the world. Security is also a wide and complex notion, with many implications. Moreover, the right to security links with other human rights such as freedom, association and even life. Without security, other rights cannot be guaranteed. Human rights cannot be treated in isolation; they are dependent on one another. Certainly, just as the right to security, the right to life is also protected under international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR)[7]. The right to life has been characterised as *'the*

[5] William C. Bier, ed., *Privacy: A vanishing value?,* Fordham University Press, New York, 1980, p. 43.
[6] Humans Rights Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 2009, p. 5. Available from: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed 23 June 2019).
[7] United Nations Human Rights Office of the High Commissioner, *International Covenant on Civil and Political Rights*, General Assembly, General Assembly resolution 2200A (XXI), 16 December 1966, article 6. Available from: https://www.ohchr.org/en/professionalinterest/pages/CCPR.aspx (accessed 30 June 2019).

supreme right' because "without its effective guarantee, all other Human Rights would be without meaning."[8]

Terrorist attacks directly impact on human rights, especially the right to security[9]. The term "terrorism" has its origin in the Latin verb "*terrer"*, that means, "to frighten". It later evolved into the French word *"terroriste*" in the late 18th century, originally applied during the period of the French Revolution known as The Reign of Terror, to the supporters of the Jacobins, who advocated repression and violence in their search for the principles of democracy and equality. [10] Throughout modern history, "[t]errorism has deviated from its original meaning of State- sponsored violence designed to induce fear and terror in order to control and dominate an otherwise anarchical society, to describe the exact opposite: political violence directed against the State."[11]

The research question of this thesis is "To what extent could surveillance programmes used by European Union Member States to counter cyberterrorism be implemented without infringing the right to privacy?"

The thesis intends to answer the research question by analysing two main paints: 1) the use of the internet to create terrorist attacks and the methods used to counter it, such as surveillance, and 2) the existing European legal framework for countering cyberterrorism, including the gaps and challenges faced in practice, if any, at domestic levels, within the context of European Union countries. Specially, the analysis on the use of surveillance as a counter cyberterrorism measure to protect the right to security and its infringement on the right to privacy.

I will examine diverse challenges that the European Union may face in order to respect and protect the right to privacy when preventing and combating terrorism in the cyberspace, focusing on surveillance as a counter terrorism strategy. The question to respond is: do we have to choose between privacy and security? Or, is the right to privacy as important as the right to security? The proportionality of Internet surveillance touches

[8] M. Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, N.P. Engel, 2005, p. 121.
[9] Security Council, *Threats to international peace and security caused by terrorist acts, Resolution 1566*, 2004.
[10] English Oxford Dictionary [website], *definition of "terrorist*", available from: https://www.lexico.com/en/definition/terrorism (accessed 25 June 2019).
[11] Alan Greene, *Defining terrorism: One size fits all*?, International and Comparative Law Quarterly, Cambridge University Press, Vol. 66, Issue 2, 20 February 2017, p. 412.

on fundamental values of any democratic society, raising serious questions for EU policies. Hence, a human rights-based approach[12] is essential when preventing and combating all forms of terrorism.

Although it is a persistent threat in today´s world, there is no universal agreement on the definition of terrorism. However, it is generally acknowledged that terrorism can take many forms, and that it attacks the values that lie at the heart of the Charter of the United Nations and other international instruments. Terrorism, in whatever form, aims at the destruction of human rights and the rule of law.

Terrorism has become a persistent threat to international peace and security, and it has developed into a permanent alert in people´s lives. Global initiatives to counter terrorist narratives are executed by numerous different actors on the supranational, international, regional and national levels. Even though there may be many ways to approach the fight against terrorism, the respect for human rights in any effective counter-terrorism strategy is essential and States must uphold their international agreements and obligations.

> *Too often, governments have forgotten that the fight against terrorism is in fact a fight for the values of human rights. Where terrorism is fought through means that violate human rights, or that undermine fundamental freedoms as a result is that more individuals are ready and willing to resort to the unacceptable use of terrorist violence.*[13]

Although terrorism is a global threat, the focus of this research is on the European Union (EU). The EU is a unique and complex economic and political union, result of a

[12] Defined by the Office of the United Nations High Commissioner for Human Rights as: "A human rights-based approach is a conceptual framework for the process of human development that is normatively based on international standards and operationally directed to promoting and protecting human rights. It seeks to analyse inequalities which lie at the heart of development problems and redress discriminatory practices and unjust distributions of power that impede development progress." *Frequently asked questions on a human rights- based approach to development cooperation,* United Nations Publication, New York and Geneva, 2006. Available from: https://www.ohchr.org/Documents/Publications/FAQen.pdf (accessed 31 July 2019).

[13] Manfred Nowak and Anne Charbord, *Using Human Rights to Counter Terrorism*, Elgar Studies in Human Rights, Edward Elgar Publishing, 2018, p. 3.

long historical process of negotiations between its member States. This supranational entity is composed of 28 neighbouring countries, with a total population of over 508 million inhabitants[14], who aim at maintaining peace, stability and prosperity in the region, through the Union.[15] Different bodies, with the support of treaties and the representation of its citizens and member States, govern the Union. There are also other different entities that overlap within the scope of the EU, such as the Organisation for Security and Co-operation in Europe (OSCE) with 57 participating States and the Council of Europe, composed of 47 member States, to which all 28 members States of the EU are party.

The EU has implemented strong legislations and supported operational cooperation to prevent and to counter crime and terrorism in all its forms, including the cyberspace. Example of this is the EU´s Counter- Terrorism Strategy.[16] However, member states still have the primary responsibility for combating terrorism.

The security of the EU is endangered by terrorism and new hybrid cyber threats. The internet has changed the way global terrorism functions. Internet can be used not just for carrying out attacks, but also as a communicative or instrumental tool, and for recruitment and mobilization purposes, with a worldwide reach. "Terrorists, for instance, can learn from the Internet about the schedules and locations of targets such as transportation facilities, nuclear power plants, public buildings, airports and ports, and even counterterrorism measures."[17] No single country can face these emerging threats alone. Therefore, when it comes to security, all EU member states have a linked interest. To respond more effectively, the EU shares a Common Security and Defence Policy (CSDP) that englobes different aspects of a common security strategy,[18] as well as a Common Foreign and Security Policy (CFSP) designed to preserve peace, strengthen international security, promote international cooperation, and consolidate democracy, the

[14] *Living in the EU*, European Union [website]. Available from: http://www.europa.eu/european-union/about-eu/figures/livig_eu (accessed 26 July 2019).
[15] See John McCormick, *Understanding the European Union: A concise Introduction*, 7th Edition, Palgrave, London, 2017.
[16] *The European Union Counter- Terrorism Strategy*, Council of the European Union, Brussels, 30 November 2005, No. of doc. 14469/4/05 REV 4.
[17] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, January 2006, p. 11.
[18] *CSDO structure, instruments, and agencies*, The Common Security and Defence Policy, European Union [website], 08 July 2016. Available from: http://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/csdp-structure-instuments-and-agencies_en (accessed 28 July 2019).

rule of law and respect for human rights and fundamental freedoms at home and abroad.[19] The new European Agenda on Security "prioritises terrorism, organised crime and cybercrime as interlinked areas with a strong cross-border dimension."[20] Although the EU works to create conditions which allow member states to collaborate more closely with each other on its defence, this collaboration is not always easy. Security is a primary attribution of states. Having to rely on foreign institutions to provide its citizens with security can be conflicting for national governments. However, the increasing interdependence of states and the emergence of new threats, with which countries are unable to cope alone, has led to international cooperation.

In recent years, new terrorist groups have emerged, and with them, new ways of perpetrating terror. States have had to adopt broader and firmer counter-terrorism measures to confront terrorists and ensure security. But sometimes, the protection of the collective rights of citizens, such as the right to security, may cause infringement to individual´s rights, for instance to the right to privacy. "With every attack, new measures are considered, to the point that they now permeate nearly every aspect of life, from browsing the web, to donating to a good cause, entering a shop or buying a plane ticket."[21] It seems that, there is little room for privacy when state investigators can see who individuals communicate with, what they read or watch online, and where they move around as shown by their mobile use. Yet, how much privacy must be yielded to ensure security?

Terrorism is a broad term; it can take different forms, be carried out through different channels and have diverse consequences. However, it may commonly be understood as acts of violence that take many forms, usually targeting civilians in the pursuit of political or ideological aims, to produce harm and fear.[22] Terrorism has

[19] *Foreign and Security Policy*, European Union [website]. Available from: http://europa.eu/european-union/topics/foreign-security-policy_en (accessed 27 July 2019).
[20] *European Agenda on Security*, Migration and Home Affairs, European Commission [website]. Available from: http://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (accessed 28 July 2019).
[21] Manfred Nowak and Anne Chardbord, *Using Human Rights to Counter Terrorism*, Elgar Studies in Human Rights, Edward Elgar Publishing, 2018, p. 2.
[22] Office of the United Nations High Commissioner for Human Rights. Human Rights, Terrorism and Counter- Terrorism. *Fact Sheet No. 32*. Available from: http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf (accessed 20 February 2019).

evolved. With the use of modern technologies, terrorists have found new, more complex ways to carry out attacks. Correspondingly, the operational logistics behind terrorist attacks have also evolved. With the use of modern technologies, terrorists are now able to carry out more sophisticated attacks. Terrorist groups can now be more geographically dispersed and work remotely, coordinate with others, have a non-hierarchical structure and target greater objectives.[23]

The world entered the age of web-enabled technologies and services. In this age, Internet has revolutionised the way we live by improving many aspects of our everyday life with countless benefits, such as the sharing of information and ideas. For that reason, the internet has been recognized as a fundamental human right.[24] It must also be recognized, however, that this technology can also be exploited for crimes and terrorism purposes.

Internet is an ever-growing technology with a worldwide, almost limitless, audience and a sort of life of its own. The internet can make it simple for any individual to communicate with relative anonymity, quickly and effectively across borders. People can make all sorts of online transactions that can convert into physical results, such as an online purchase or the planning a holiday trip. This global interconnectivity can be done in a matter of seconds. However, people can also take advantage and abuse the power of the cyberspace to attack and induce fear on others.

The number of people interconnected through the internet keeps growing at a fast pace. With the massive increase of internet use, other threats emerge, such as

[23] Bruce Riedel, *The Grave New World: Terrorism in the 21st Century* [website], Brookings, 9 December 2011. Available from: https://www.brookings.edu/articles/the-grave-new-world-terrorism-in-the-21st-century/ (accessed 16 June 2019).

[24] In 27 June 2016 the United Nations General Assembly issued a Resolution indicating the importance of "applying a comprehensive human rights- based approach when providing an expanding access to the internet and for the internet to be open, accessible and nurtured". Also, This resolution recognizes that "for the Internet to remain global, open and interoperable it is imperative that States address security concerns in accordance with their human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy". The resolution, however, did not receive universal backing, with countries like Russia and China rejecting it. Resolution available: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (accessed 22 February 2019).
Also see, International Covenant on Civil and Political Rights, General Assembly resolution 2200(A) (XXI), art.19, para. 2.

cyberterrorism. In the cyberspace, terrorists and terrorist groups can communicate, plan, recruit, fund, carry out attacks, and spread their messages to the whole world.[25]

> *As our communications infrastructure grows more powerful and user-friendly, we increasingly speak, listen, and act thru cyberspace. And such activity generates records, dutifully recorded, stored, saved, and exchanged by computers.*[26]

In that sense, the advancements in technology that can benefit humanity, may also challenge the right to security if misused. In response to these activities, policing and intelligence agencies have parallelly developed new capabilities and gained legal powers to put internet users under surveillance.

Cyberterrorism poses a great definitional dilemma. Dorothy Denning, a leading scholar on cybercrime and cybersecurity, describes cyberterrorism as attacks against computer systems designed "to intimidate or coerce a government or its people in furtherance of political or social objectives", it is violent or causes "enough harm to generate fear".[27] Thus, we can most precisely identify it by its aim to spread fear and coercion.

According to The European Union Agency for Law Enforcement Training (CEPOL), an agency dedicated to develop, implement and coordinate training for law enforcement officials from European Union member states, cyber-terrorism "involves the use of computers and/or related technologies with the intention of causing harm or damage, in order to coerce a civilian population and influence policy of target government or otherwise affect its conduct."[28] In accordance to that definition, attacks imply targeting critical infrastructure and should not be confused with hacktivism or cyber-warfare.

---

[25] United Nations Office on Drugs and Crime, *The use of internet for terrorist purposes*, United Nations, New York, September 2012, p. 3.
[26] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, p. 1195, 1998.
[27] Dorothy Denning, *Cybersecurity´s Next Phase: Cyber Deterrance*, Scientific American, 2016, p.4.
[28] *WEBINAR 65/2018 Cyber-terrorism: A treat for the European Union and its response*, European Union Agency for Law enforcement Training [website], 2018. Available from: https://www.cepol.europa.eu/education-training/what-we-teach/webinars/webinar-652018-cyber-–-terrorism-threat-european-union-its (accessed 17 July 2019).

Cyberwarfare is the integration of cyberattacks into military doctrine and military operations: "Cyberwar is typically conceptualised as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force."[29] Cyber operations can add significantly to military campaigns by amplifying dynamic effects on the battlefield. Military forces have made significant use of digital technologies to modernize their armaments and operations. In a 2011 report on *Cybersecurity and Cyberwarfare of National Doctrines* by the US Centre for Strategic and International Studies, 33 states were identified to have included cyberwarfare in their military planning and organisation,[30] more than half of them are member states of the EU.

A nation´s critical infrastructure is an essential part of its security. Even though cyberterrorism is carried out in the cyber space, it can have physical implications. Most of modern-day critical infrastructure is interconnected and functioning through the internet. The attack of critical infrastructure poses a tremendous danger to peace and security and has highly been underestimated.

> *Internet-based attacks or cyberterrorism have the capacity to damage physical property and human life, if for example, the attacked computer systems are responsible for the administration of nuclear power stations, dams, flight control systems, hospital computers, or military weapon systems.*[31]

Cyberterrorism is a serious issue for domestic and international security. The sole nature of interconnectivity of the internet surpasses borders and places everyone at risk.

[29] Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*, Congressional Research Service, Washington D.C., 27 March 2015, No. of doc. R43955, P. 4. Available from: https://digital.library.unt.edu/ark:/67531/metadc810730/citation/#top (accessed 29 July 2019).

[30] James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare*, Centre for Strategic and International Studies, Washington, D.C., 2011. Available from: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (accessed 29 July 2019).

[31] Sieber Ulrich, *International cooperation against terrorist use of the internet*, Revue internationale de droit pénal, Vol. 77, no. 3, 2006, p. 396. Available from: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm (accessed 27 June 2019).

Therefore, cyberterrorism is transnational by its very nature, making it not only extremely difficult for police agencies to place on a jurisdiction, but also to prevent it and counteract.

> *Cyberspace is an open environment, which poses a serious challenge to policy-makers. Its governance is shared by governments, the private sector and the civil society. Cyber security efforts thus require the involvement of various stakeholders, in particular since the private sector owns the vast majority of hardware, software and information infrastructure*. [32]

The investigation and prosecution of cyberterrorism is complex and challenging due to the technical nature of the internet. To counter and prevent cyberterrorism, some governments may, directly or indirectly, use tools for surveillance or espionage that, in different forms, may challenge individuals´ right to privacy, presumption of innocence, right to a fair trial, and freedom of expression and association. Under the alleged reason of security, surveillance can be carried out broadly and indiscriminately, placing human rights under threat and undermining privacy.

Mass surveillance means that all human actions are being monitored, recorded and stored.[33] This meaning that everything anyone does could potentially be observed with the use of different methods. "The need for the specific recognition and protection of the right to privacy is exacerbated by the development of new technologies that facilitate the invasion and interference with an individual´s privacy".[34] Therefore, technological advancements allow for more sophisticated ways to easily intrude into people´s private life.

Information people store in their laptops and mobile phones may include bank account numbers and transactions, receipts of online purchases, *Netflix* (online movie and

[32] European Parliamentary Research Service, *Briefing: Cyber security in the European Union*, European Parliament, 2001, p.2. Available from: http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf
[33] Michael O´Flaherty, Report: *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, European Union Agency for Fundamental Rights, 2007, p.9.
[34] Alexandra Rengel. *Privacy in the 21st Century*, Martinus Nijhoff Publishers, Leiden, The Netherlands, 2013, p. 41.

television screening apps) and *Spotify (*online music screening) accounts, memberships to online magazines and news outlets, selfies, pictures of family and friends, *uber* accounts (taxi service apps) with a detailed history of the places visited, and much more. Some information is stored in computers in the form of *cookies.* A *cookie* is a small, sometimes encrypted, text file composed of letters and numbers that is downloaded into the hard drive of your device when you access most websites. There are different types of *cookies*, with different levels of sophistication. They can contain all sorts of information that can remember and trace all your activities in the cyberspace.[35] Tracking *cookies* and *spyware* collect data about people's – and their friends' - search history, age, location, interests, products purchased online, items they liked and did not purchase or even the amount of time spent on each website. Mobile phone pictures may seem harmless; however, they can be used to identify people through face recognition programmes[36]. Some common social media pages like *Facebook* already use facial recognition tools to tag personal contacts in photos.[37] Modern cameras and mobile phones contain metadata in their files such as the location, time and date when pictures or videos were taken.[38] Metadata are also used to store other types of files, such as *Word* and *Excel* documents which, for example, tend to save changes made to the files using the "auto save" feature. Mobile phone calls are vulnerable to interception and conversations can be picked up and saved by third parties. Smart watches can measure a person's heart rate and pulse that may indicate if the persona has high or low blood pressure and transfer this information to a personalised online profile to keep a record of the condition. These are some examples of potential threats to people's privacy trough surveillance.

---

[35] See *All about cookies*, All about cookies.org [website]. Available from: https://www.allaboutcookies.org/cookies/ (accessed 31 July 2019) or *About cookies*, BBC [website], 10 October 2012. Available from: http://www.bbc.co.uk/webwise/guides/about-cookies (accessed 31 July 2019).

[36] See for example Cutting-edge facial recognition goes mainstream, European Commission [website], 11 March 2015. Available from: https://cordis.europa.eu/project/rcn/108790/brief/en (accessed 27 July 2019). Or, Maxime Jacob, Facial recognition gains grounds in Europe, among big-brother fears, Euractiv Network France, 20 October 2017. Available from: https://www.euractiv.com/section/data-protection/news/facial-recognition-gains-grounds-in-europe-among-big-brother-fears/ (accessed 27 July 2019).

[37] Leo Kelion, *Facebook seeks facial recognition consent in EU and Canada*, BBC News [website], 18 April 2018. Available from: https://www.bbc.com/news/technology-43797128 (accessed 27 July 2019).

[38] K. Murphy, *Web Photos that Reveal Secrets, Like Where You Live*, New York Times, August 11, 2010. Available from: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (accessed 28 June 2019).

In today´s digital world, people have full access to the internet everywhere they go, and every move can potentially be tracked down by localization systems (GPS) in mobile phones, cars, computers, tablets and intelligent watches, just to name a few. Surveillance tools are often used to investigate individuals and organizations to prevent and combat terrorist attacks and terrorist groups, including those in the cyberspace.[39]

> *These instruments must address the specific legal and forensic challenges posed by the internet, they must make use of new Internet-based investigation techniques, and, at the same time they must balance the need for effective prosecution against the obligation to protect citizens' civil liberties.* [40]

In the regional context, communication companies within the European Union are obliged by states to retain peoples´ information for long periods of time that may vary from country to country, for its possible future access.[41] For police and law enforcement institutions, collecting data from an individual is not difficult. Private communication companies are obliged by governments to hand any individual´s data when they consider it necessary. The growing practice of some intelligence agencies to gather bulk information about citizens using telephone and internet networks, as part of their counter terrorism efforts, has been a source of privacy related concern in the European Union.[42] Law enforcement and intelligence agencies may search through personal information, emails, contacts and even survey tertiary individuals anywhere in the world. In other words, they can monitor not only the information and contacts stored in the suspects' communication devices, but also their contacts' contacts, and so on. This extreme

[39] *Surveillance and interception of communication*, United Nations Office on Drugs and Crime [website]. Available from: https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/surveillance-and-interception.html (accessed 27 April 2019).
[40] Sieber Ulrich, *International cooperation against terrorist use of the internet*, Revue internationale de droit pénal, Vol. 77, no. 3, 2006, p. 396. Available from: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm (accessed 28 June 2019).
[41] *Data Retention across the EU*, European Union Agency for Fundamental Rights, 2017. Available from: https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention (accessed 29 May 2019).
[42] Council of Europe, Parliamentary Assembly, 2015(b), paras 1- 3.

intrusion into people's lives poses inherent threats into the private life of individuals, as will be further discussed in Chapter 2 of this research, on the right to privacy.

Conventional weapons are no longer the main method of terrorist attacks, and the importance of cyber-defence must be considered to fully respect human rights and the rule of law. I believe that to provide effective defence and security, the European Union will have to become an online alliance, capable of reacting regionally and not just nationally. Undeniably, since information is stored in the cyber domain and internet is a global tool that can be accessed anywhere in the world, connecting people across borders, jurisdictions of law enforcement may often surpass national borders. Cyberspace's "borderless nature enabled individuals and groups to exploit 'loopholes of jurisdiction' and take advantage of specific countries' difficulties to response adequately, due to legal reasons or because authorities do not have the necessary technical expertise or resources […]."[43] Therefore, a correct joint regional strategy may help prevent and counter cyberterrorism without violating human rights. However, if that cooperation does not hold human rights principles at its core, cooperation could have the exact opposite effect.

Due weight must be given to both -privacy and security- when countering cyberterrorism. "The counter terrorism measures, and the protection of human rights are not separate goals."[44] Privacy, freedom of expression, the free flow of information, and even the right to security itself are at risk by cyber-security policies intended to counter cyberterrorism.

[43] J. Vogel, *Towards a Global Convention against Cybercrime*, First World Conference of Penal Law in the XXI Century, Guadalajara, Mexico, 18 – 23 November 2007. Available from: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf (accessed 1 august 2019).

[44] Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Press Conference on the Preliminary findings of the visit to Belgium,* Brussels, 31 May 2018. Available from: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23164&LangID=E (accessed 30 June 2019). Also see United Nations General Assembly, *The United Nations Global Counter- Terrorism Strategy*, Resolution 60/288, 20 September 2006.

> *We all believe that security is a human right and we understand that in a long term it´s the protection and promotion of human rights that is the most effective mean to prevent terrorism in the first place, and to ensure the safety and transparency, and accountability of the societies we live in. These are not conflicting goals, they are compatible and mutual reinforced goals.*[45]

States have a difficult job in balancing competing human rights. As stated by Martin Scheinin, former special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the balance must be found within the human rights framework itself.[46] The right to security requires States to provide reasonable and appropriate measures (within the scope of those available to public authorities), to protect a person's physical security and integrity. They are obliged to do all that is reasonably possible to avoid life-threatening risks caused by terrorist threats, including those in the cyberspace, while safeguarding the fundamental rights of all individuals.

[45] Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Press Conference on the Preliminary findings of the visit to Belgium*, Brussels, 31 May 2018. Available from: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23164&LangID=E (accessed 30 June 2019).

[46] Martin Scheinin, *Statement by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 16th session of the Human Rights Council, Item 3, United Nations, Geneva, 7 March 2011. Available from: https://www.ohchr.org/Documents/Issues/Terrorism/statementHRC16SRCT_HR7March2011.pdf (accessed 2 august 2019).

2. The Right to Privacy

> *In modern society, the deliberation around privacy is a debate about modern freedoms.*[47]

Privacy is a fundamental human right and its unique necessity is universal and inherent to every human being. It is essential for human development as individuals and as members of a society. Privacy serves as the foundation upon which other human rights are built.[48] However, the concept of privacy is complex; it has many dimensions and distinct meanings in different cultures, societal contexts and periods throughout history. "Privacy has many meanings and many levels of meaning."[49] Indeed, it is recognised in the 1948 Universal Declaration of Human Rights (article 12),[50] in the International Covenant of Civil and Political Rights (article 17), the UN Convention on Migrant Workers and Members of their Families (article 14),[51] the UN Convention on the Rights of the Child (article 16),[52] European Convention on Human Rights (ECHR) (article 8),[53]

---

[47] *What is privacy?*, Privacy International Organisation [website]. Available from: https://privacyinternational.org/explainer/56/what-privacy (accessed 1 July 2019).

[48] Oliver Diggelmann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, Human Rights Law Review, Volume 14, Issue 3, Oxford University Press, September 2014, P. 442.

[49] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p.4.

[50] UDHR, Article 12: No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[51] CMWMF, Article 14: No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

[52] CRC, Article 16: 1. No child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks.

[53] ECHR, Article 8: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

and in a great number of other international and regional treaties. Though, despite the universality of the notion of privacy, there is no universal definition.[54]

> *Privacy is essential to human dignity and autonomy in all societies, enabling individuals to create barriers to protect themselves from interference in their lives, such as access to their bodies, places and things, as well as their information and communication.*[55]

Paradoxically, the right to privacy became an internationally recognised human right before it was in fact, a well- established national fundamental right in any state's constitution. "In the years after World War II, when the human rights system was devised, states constitutions protected only certain aspects of privacy. Such guarantees concerned, for example, the inviolability of the home and of correspondence and the classical problem of unreasonable searches of the body."[56] It appears that, although there was some recognition of the importance of privacy, its actual acknowledgment as a universal human right went beyond the national guarantees, settling a precedent with an underestimated potential that well along evolved into a multifaceted integral guarantee to the right to respect one´s private life.

At a regional level, the drafting of the ECHR within the framework of the Council of Europe began in August 1949, around half a year after the adoption of the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly, which was a clear important point of reference.[57] As Winston Churchill, British Prime Minister at that time, stated in his speech during the 'Europa Congress' the 7th of May 1984 in

[54] T. Mendel, A. Puddephatt, B. Wagner, et al, *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, 2012, p.4.
[55] J. Cannataci, B., Zhao, G. Torres Vives, S. Monteleone, et al., *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*, United Nations Educational, Scientific and Cultural Organization, Paris, 2016, p.32.
[56] Oliver Diggelmann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, Human Rights Law Review, Volume 14, Issue 3, Oxford University Press, September 2014, P. 441.
[57] Council of Europe, *The Conscience of Europe: 50 Years of the European Court of Human Rights*, Third Millennium Publishing Limited, London, 0ctober 2010, p. 16.

The Hague, The Netherlands: *"*In the centre of our movement stands the idea of a Charter of Human Rights, guarded by freedom and sustained by law*."*[58]

During the drafting of the ECHR, "in the Consultative Assembly, many members expressly pointed to the encroachments on the sanctity of the home during World War II."[59] The atrocities committed during the war represented a well-founded reaction and common motivation to include a provision on privacy headed by the umbrella term of 'private life', that also concerned 'family life'.[60] The inclusion of this provision concerning the abstract but vital notion of privacy, gave room for a long process of negotiations and divers' proposals by member states. On the 7th of August of 1950, an agreement for a European Convention of the Protection of Human Rights and Fundamental Freedoms was reached. The Convention was then adopted on 4 November 1950,[61] resulting into what I believe is a broad, open-ended article that is divided into two parts which includes an exception to the right itself in its second part of the article. Article 8 of the ECHR titled:

> *Right to respect for private and family life:*
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.* [62]

---

[58] Council of Europe, *Winston Churchill Speech to the Congress of Europe (The Hague, 7 May 1948)*, Documents, Records and Archives [website]. Text of speech available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168069828d (accessed 1 august 2019).
[59] Oliver Diggelmann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, Human Rights Law Review, Volume 14, Issue 3, Oxford University Press, September 2014, p. 457.
[60] Diggelmann, Ibid, 441.
[61] Martinus Nijhoff, *Collected Edition of the 'Travaux Préparatoires' of the European Convention on Human Rights*, Council of Europe, Vol. V, The Hague, 1979, p. 126.
[62] Article 8 of the European Convention on Human Rights. Available from: http://www.echr.coe.int/Documents/Conventio_ENG.pdf (accessed 22 July 2019).

There is a link between identity and property, as well as property and privacy. The notion of property does not necessarily entail a physical object, but it can form part of private life.[63] The intrusion into one's property may represent a violation into one's privacy, but property can also be represented in forms other than the physical, such as information, ideas or cultural identity.[64] People, societies and the interaction between individual's property and privacy has evolved over time. In the digital age, our concept of privacy has also evolved, and the way of infringement into our private space has expanded into the cyber domain. Technological advancements have introduced new threats, but also means for fighting those threats. "The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances.[65]"

Under International Human Rights Law (IHRL), the rules that protect privacy, on the one hand, limit the powers of states and private institutions over people's autonomy. And, on the other hand, those rules give individuals the ability to assert their rights when they are susceptible to a significant power imbalance.

There is no argument to support the idea that privacy is not under attack. With modern day technologies, violations to private life are increasingly becoming a concern. The capabilities that now exist for espionage and surveillance, for example, are unprecedented. The same tools used for maintaining a secure space can be intrusive and infringe on an individual's rights. "Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communication and metadata to hacking and database mining."[66] Law enforcement and intelligence agencies have been able to pay increasing attention to the use of the internet for criminal purposes, especially by terrorist suspects.

Therefore, nations have started to look for ways to balance privacy and security at home and abroad. However, there is an enormous discrepancy between the velocity in which technologies evolve and the pace in which laws to regulate them are produced. As

---

[63] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p. 8.
[64] Corien Prins, *Property and Privacy: European Perspectives and the Commodification of Our Identity*, Information Law Series, Vol. 16, 2006, p. 234.
[65] *What is privacy?*, Privacy International Organisation [website]. Available from: https://privacyinternational.org/explainer/56/what-privacy (accessed 1 July 2019).
[66] *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, European Union Agency for Fundamental Rights, 2017, p.9.

a result, the mechanisms for the protection of human rights are left vulnerable, exposing people to abuse, and reducing privacy.

In some countries, laws have not kept up with technology, leaving significant gaps in protection for its citizens. In other countries, law enforcement and intelligence agencies have been granted significant exceptions by their legislations.[67] Even in some of the most democratic countries with strong privacy laws, there are widespread violations related to surveillance of communications where police services maintain extensive files of citizens not accused or suspect of any crime, under the pretext of security. [68]

On the 12th of September of 2018, the Commission of the European Union launched a proposal for a regulation on 'preventing the dissemination of terrorist content online' to complement Directive 2017/541 on combating terrorism. [69] The aim of the proposal was to ensure that internet platforms offering their services in the European Union were "subject to clear rules to prevent their services from being misused to disseminate terrorist content.[70]" Correspondingly, it provided a definition of terrorist content[71] (although broad) followed by a set of operational measures to be taken by companies and member states for its proper implementation. In my point of view, even

[67] Privacy International, *Liberty, and Open Rights Group joined other organisations across the EU to file complaints over Member States' non- compliance with mass surveillance rulings*, Privacy International [website], 25 June 2018. Available from: https://privacyinternational.org/press-release/2119/privacy-international-liberty-and-open-rights-group-joined-other-organisations (accessed 31 July 2019).

[68] *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Member States' Legal Frameworks*, European Union Agency for Fundamental Rights, November 2015, p.8.

[69] 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.

[70] European Commission, *State of the Union 2018: Commission proposes new rules to get terrorist content off the web*, Strasbourg, 12 September 2018. Available from: http://europa.eu/rapid/press-release_IP-18-5561_en.htm (accessed 1 July 2019).

[71] European Commission, proposal for a regulation of the European parliament and of the council on preventing the dissemination of terrorist content online:
Article 2 (5): 'terrorist content' means one or more of the following information:

(a) inciting or advocating, including by glorification, the commission of terrorist offences, t hereby causing a danger that such acts be committed;
(b) encouraging the contribution to terrorist offences;
(c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2 (3) of Directive (EU) 2017/541;
(d) instructing on methods or techniques for the purpose of committing terrorist offences.

Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 29 July 2019).

though the regulation "takes into account the burden on hosting service providers and safeguards, including the protection of freedom of expression and information as well as other fundamental rights"[72], the regulation placed significant pressure on a variety of information and communications technology companies to monitor users' activities. In other words, it endorses a mass surveillance by private companies, with the intention of removing content in ways that could pose risks for people´s freedom of expression and privacy.[73]

European privacy law is complex, developing under a range of separate instruments, often ad hoc, by different national and regional EU judicial and other bodies. In the EU legal framework, the right to privacy and the right to data protection are two closely related, but distinct rights recognised in the Charter of Fundamental Rights of the European Union (articles 7 and 8), the Treaty on the Functioning of the EU (article 16), and separately in two legal instruments of the Council of Europe[74], to which all EU Member States are parties. Both rights, however, are subject to limitations imposed by the principle of proportionality and the case law of the European Court of Justice (ECJ).

Proportionality is a well-established principle in the legal order of the EU member States and the case law of the ECJ. It allows for limitations in the exercise for fundamental rights if they are provided by law and respect the core of those rights.[75] The Charter of Fundamental Rights of the EU in its article 52 (1) states that:

[72] European Commission, *proposal for a regulation of the European parliament and of the council on preventing the dissemination of terrorist content online*, Brussels, 12 September 2018, p. 5. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 29 July 2019).

[73] *GNI Statement on Europe´s proposed regulation on preventing the dissemination of terrorist content online*, Global Network Initiative, 15 January 2019. Available from: https://globalnetworkinitiative.org/wp-content/uploads/2019/01/GNI-Statement-Proposed-EU-Regulation-on-Terrorist-Content.pdf (accessed 29 June 2019).

[74] The Council of Europe is not a European Union institution, but all EU member States are party to it

[75] European Court of Human Rights, *Derogation in time of emergency*, Press Unit [website], August 2018. Available from: https://echr.coe.int/Documents/FS_Derogation_ENG.PDF (accessed 28 July 2019).

> *subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedom of others.*[76]

Therefore, when dealing with terrorist issues, the principle of proportionality is commonly pointed out. The underlying idea is that in order to provide security in case of an emergency, other human rights are restricted or placed at a second level as a way for law enforcement officials and intelligence agencies to act rapidly and without obstacles. In a broader sense, certain individual freedoms, such as privacy, freedom of expression or association, are paused in order to maintain peace and security.

With internet as a mainstream tool for communication, policing has become increasingly pre-emptive. Law enforcement and intelligence agencies have developed new surveillance capabilities and have been given legal powers that allow them to monitor anyone and everyone. Those capabilities have been intended to particularly target terrorist suspects and organizations, but unwillingly have compromised the rights of common people by basically spying on everyone through mass surveillance. "In the context of the fight against terrorism, this means individuals are targeted for being suspected 'extremists' or for being suspected of being 'opposed to our constitutional legal order' even before committing any criminal (let alone terrorist) offence."[77] It is difficult to capture a criminal that has not yet committed a crime. In this pre-emptive scenario, law enforcement officials look for specific clues through the analysis of mass bulk surveillance. Officials may have indications of possible suspects of cyberterrorism by monitoring everything that happens in the cyberspace.

[76] *Charter of the Fundamental Rights of the European Union* [website], European Union. Available from: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 28 May 2019).
[77] Ian Brown and Douwe Kroff, *Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology, Vol. 6, Issue 2, 2009, p. 131.

2.1 Defining Privacy: its origins and its importance

As explained earlier, privacy is fundamentally dynamic; it can change its meaning depending on the context and environment.[78] The term, therefore, is itself an obstacle to a clear thought of privacy. However, the notion of privacy has roots deep in history, in every culture, in every corner of the world and it is expressed in different forms.[79] Just as the world has endured changes, privacy has never stopped evolving. Ultimately, we all need privacy.

> *Privacy is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others that may wish to extend control.*[80]

In other words, privacy helps individuals create barriers and manage boundaries to protect themselves from unwarranted interferences in their lives. It allows people to negotiate and govern who they are and how they want to interact with the world around them. "It is a maintenance of a personal life-space within which the individual has a chance to be the individual, to exercise and experience his own uniqueness."[81]

Professor Jerry Kang explains in his article *Information Privacy in Cyberspace Transactions*, that a great number of ideas related to the notion of privacy can be organised and divided into three clusters: space, decision and information. These clusters are not completely separated and can be at times interconnected. The first cluster concerns the physical space, in reference to the extent to which an individual´s physical space is protected from undesired invasion. The second cluster of privacy has to do with making

[78] Julie E. Cohen, *What Privacy is for*, Harvard Law Review, Vol. 126, 2013, p. 1906.
[79] Ferdinand Schoeman, *Privacy and Social Freedom*, Cambridge University Press, Cambridge, 1992, p. 116.
[80] *What is privacy?*, Privacy International Organisation. Available from: https://privacyinternational.org/explainer/56/what-privacy (accessed 1 July 2019).
[81] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p. 19.

a choice, referring to an individual´s ability to make certain significant decisions without external interference or through personal autonomy. This conception of privacy centres in a person's freedom to make choices without state interference within actual space or territorial boundaries. The third cluster views privacy as mainly concerned with information privacy, or the flow of personal information. It refers to an individual´s control over the processing of personal information, including attainment, disclosure and its use in different forms and for different purposes. In this third sense, the right to privacy refers to the ability of individuals to determine who has information about them and how that information is used. [82]

For the purpose of this research the definition of privacy will be borrowed from the book published in 2016 by United Nations Educational, Scientific and Cultural Organisation (UNESCO), *Privacy, Free Expression and Transparency: Redefining their new boundaries in the new age*. Although there are many diverse interpretations of the notion of privacy, many scholars and international institutions that deal with this topic use this definition by UNESCO as a base reference because of its modern adaptability. In that sense, privacy is defined as "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' without interaction from others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[83]

Privacy and secrecy are different but linked notions. I believe recognising that secrecy is an important part of one's privacy would contribute to the understanding of what needs to be protected, for whom, and under what circumstances. The right to secrecy "involves keeping to oneself information which one feels would render one´s vulnerable to some kind of damage, either practical damage or damage to self- esteem."[84] I believe that the invasion of both, privacy and secrecy affects individuality and behaviour. People tend to keep certain aspects of their life in secrecy. They may be intimate or compromising. Hence, the walls of secrecy collapse at the infringement of one´s privacy.

[82] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1999 p.1203.
[83] J. Cannataci, B., Zhao, G. Torres Vives, S. Monteleone, et al., *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*, United Nations Educational, Scientific and Cultural Organization, Paris, 2016, p.32.
[8484] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p 19.

The issue is not whether people´s choice to secrecy is good or bad and to whom, but whether its disappearance should be a tolerated reality.

Modern day technologies allow companies and governments the possibility to monitor every conversation, each commercial transaction, and every location people attend. "Many […] take for granted the fact that they or their actions can easily be traced, especially with mobile devices."[85] This capacity to breach in our everyday lives, directly affects our privacy and can have negative effects on individuals, groups and even societies, as it can be abusive, exclude and discriminate. It can also have repercussions on how individuals think and how they express about their relationships between individuals, markets, society, the state, etcetera. "The threat to privacy originates in a complex social system which needs information to survive and which is forever expanding the scope and intimacy of data regarded as relevant."[86] There is little room for privacy when each and every move is being monitored.

2.2 The use of the internet and threats to privacy

As stated earlier, the protection of privacy is not only physical or territorial, but has increasingly become an online challenge. The greatest challenge to privacy legislation from an international perspective arises because, while the Internet is virtually borderless, legislative approaches and levels of technological capabilities differ from country to country. Also, "[t]he Internet is not a purely public space. It is composed of many layers of private as well as social and public realms."[87] Therefore, cyberspace cannot be easily

[85] European Parliamentary Research Service, *Mass Surveillance. Part 2 – Technology Foresight, options for longer- term security and privacy improvements*, European Parliament, p. 44. Available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf (accessed 30 July 2019).
[86] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p. 19.
[87] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations, doc. No. A/69/397, 23 September 2014, p7.

regulated, less so without international cooperation. Thus, as the use of digital technologies evolves, the protection of personal data is increasingly relevant.

Despite being upheld as a fundamental human right, the right to privacy had commonly been unaddressed within the UN human rights monitoring mechanisms, with a few exceptions as the 2010 report of the UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[88]

Ben Emerson, in his capacity of the second UN Special Rapporteur on the promotion and protection of human rights while countering terrorism from 2011 to 2017, examined the human rights consequences of the change in nature of international terrorism. He made as one of his main focus during his six-year tenure, the use of mass digital surveillance for terrorism purposes.[89] He urged governments engaged in mass surveillance of the internet for counter- terrorism purposes to update their national legislations in line with international human rights law for new technology surveillance measures. He also called on all states involved on mass digital surveillance technology to provide a detailed and evidence-based public justification for the systemic interference with the privacy rights of the online community by referencing their international legal obligations.[90] He emphasised that "[m]easures that interfere with the right to privacy must be authorised by accessible and precise domestic law that pursues a legitimate aim, is proportionate and necessary."[91]

[88] Martin Scheinin, *2010 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, (A/HRC/16/51/Add.1), 14 February 2010. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/107/07/PDF/G1110707.pdf?OpenElement (accessed 27 June 2019).
[89] Manfred Nowak and Anne Charbord, *Using Human Rights to Counter Terrorism*, Elgar Studies in Human Rights, Edward Elgar Publishing, 2018, p.6.
[90] See Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations, doc. No. A/69/397, 23 September 2014.
[91] Ben Emerson, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Speech during the presentation of his report to the UN General Assembly on the use of mass digital surveillance for counter-terrorism purposes, and the implications of bulk access technologies for the right to privacy*, New York, 23 October 2014. Available from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200 (accessed 30 July 2019).

Hence, real attention grew worldwide towards the importance of protecting the right to privacy after the Snowden revelations in 2013.[92] Edward Snowden was a former United Stated intelligence employee who gave detailed evidence to the public through the publishing in important news outlet sources, of the gross surveillance practices conducted by the National Security Agency (NSA) worldwide.[93] "The surveillance practices revealed by Snowden show clearly if not completely that governments […] engaged in astonishingly large scale monitoring of populations, and also how they do it."[94] The leaks created significant political momentum to address the practices of mass surveillance and their strengthening by modern communications technology, such as the use of *Big Data*, and strong complicity between states and private companies. "Bid Data intensifies certain surveillance trends associated with information technology and networks, and thus is implicated in fresh but fluid configurations."[95] Massive quantities of data about people and their activities are generated extensively and intensively by Big Data practices. The revelations triggered governments and citizens to question the power of surveillance technologies and their wide interference into intimate and private information. It became clear that governments and intelligence agencies do not only use surveillance to monitor its people 'looking for criminals', but also use these practices to monitor each another's governments and institutions[96], including EU government leaders.[97]

---

[92] Nikhil Kalyanpur and Abraham Newman, *Today, a new EU law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened*, The Washington Post [website], 25 May 2018. Available from: https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/?noredirect=on&utm_term=.2744a04e52b3 (accessed 20 June 2019).

[93] Ewen MaCaskill and Gabriel Dance, *NSA Files: Decoded*, The guardian [website], 1 November 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (accessed 2 August 2019).

[94] David Lyon, *Surveillance, Snowden, and Big Data: Capacities, consequences, critique,* Big Data & Society, SAGE, July- December 2014, p. 2. Available from: https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861 (accessed 2 August 2019).

[95] Lyon, Ibid, p. 1.

[96] See Ewen MacAskill and Gabriel Dance, *NSA Files: Decoded/ Edward Snowden's surveillance revelations explained,* The Guardian [website], 1 November 2013. Available from: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (accessed 28 July 2019).

[97] See for example: *NSA tapped German Chancellery for* decades, WikiLeaks claims, The Guardian [website], Berlin, 8 July 2015. Available from: https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel (accessed 29 July 2019). Also: *Snowden NSA: Germany drops Merkel phone- tapping probe*, BBC News [website], London, 12 June 2015. Available from: https://www.bbc.com/news/world-europe-33106044 (accessed 29 July 2019).

At the EU level, the Directive on Privacy and Electronic Communications, also known as the ePrivacy Directive, safeguards the confidentiality of electronic communications in the EU. The directive is a key instrument to protect privacy by including specific rules on data protection in the area of telecommunications in public electronic networks. It deals with several important issues, such as confidentiality of information, treatment of traffic data, spam and cookies. The legislation aims to protect online privacy when browsing on the internet, mobile phones, wearable intelligent technology or other internet connected devices. It was last updated in 2009, with the aim to provide clearer rules for customers' rights to privacy. [98] One of the biggest modifications was the inclusion of a required prior consent from users regarding *cookies*[99], often called as the *cookie law* for that reason (and is the reason why *cookie* consent popups appear on many websites in Europe). Although it became national law with a gradual implementation in EU countries, the ePrivacy Directive has never properly been enforced across the EU due the different capabilities within its member States. "Rules have been poorly enforced and lawmakers have not been able to keep up with development in technologies." [100] Indeed, just as it was the case with the predecessor General Data Protection Regulation (GDPR).

Personal data is an asset and it belongs to the individual who produces it. Without the right laws there is little to protect citizens against having data misused, vulnerable to theft and stored in unknown places. "Once gathered and coded, the information is stored in great data banks and, most important, is retrievable within seconds on command by anyone with access to the button."[101] In recent years, the European Parliament has pushed for laws that favour and balance privacy and regulate the use of personal information, data protection and surveillance.

[98] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and electronic communications).
[99] European Commission, *Digital privacy*, Digital Single Market Policy [website], 27 June 2019. Available from: https://ec.europa.eu/digital-single-market/en/online-privacy (accessed 28 July 2019).
[100] *EU Privacy and Electronic Communications (ePrivacy Directive*), Electronic Privacy Information Center [website]. Available from: https://epic.org/international/eu_privacy_and_electronic_comm.html (accessed 29 July 2019).
[101] William C. Bier, ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980, p. 16.

All European Union Member States are parties to the European Convention on Human Rights and Fundamental Freedoms and the International Convention on Civil and Political Rights (ICCPR), amongst many other treaties in which the right to privacy is enshrined. Yet, increasingly, we are not being informed about the monitoring we are being placed under. Even though it is invasive, lacks accountability and in broadly places democratic life at risk, secret surveillance is rapidly becoming the standard. "Perhaps the most significant challenge to privacy is that the right can be compromised without the individual being aware."[102]

Surveillance, by its very nature, impacts on personal privacy and threatens the most fundamental values underpinning the European political settlement, at both national and international level.

[102] *What is privacy?*, Privacy International Organisation. Available from: https://privacyinternational.org/explainer/56/what-privacy (accessed 1 July 2019).

3. The use of the internet for terrorist purposes

The internet is a worldwide data network that exchanges information through a protocol called Transmission Control Protocol/ Internet Protocol (TCP/IP). To explain it in simple terms, the TCP breaks down information into small packets and numbers them sequentially for later reassembly. The IP addresses each packet with its intended destination. The physical technology of the internet is made-up of communications lines, which send, receive and process the information transmitted. The information on the internet is stored in hard drives of servers around the world. The internet provides numerous communicative functions, such as file transfers, remote login, e-mail, video conferencing, news, and hypertext, or as we known it, the World Wide Web.[103]

The benefits of the internet are numerous, starting with its incomparable possibility for sharing information and ideas. It is an instrument that promotes freedom of expression and information, which are recognised as a fundamental human rights in article 19 (2) of the ICCPR.[104] While there are still some debates regarding the access to internet as a commodity or a utility[105], it can be agreed that in Europe it is no longer a luxury, but has rather become part of everyday life across European households. "An estimated 189.8 million people had a broadband internet connection in Europe in 2016."[106]

[103] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1999, p.1221.
[104] International Covenant on Civil and Political Rights, General Assembly Resolution 2200 A (XXI), art. 19, para. 2: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the for of art, or through any other media of his choice."
[105] The debate matters for the purpose of acknowledging the access to Internet as a human right or not.
1. "Commodities are subject to regulatory pressure, but their pricing and availability is governed more by the powers of supply and demand than by federal authorities." 2. "Utilities, while still run by companies, are heavily regulated and their services are doled out evenly to all customers. "
J. Harpaz, *The Internet: A Commodity or Utility?*, Forbes [website], 2015. Available from: https://www.forbes.com/sites/joeharpaz/2015/01/27/the-internet-commodity-or-utility/#414e998e6eff (accessed 20 March 2019).
[106] S. O´Dea, *Internet Usage in Europe- Statistics & Facts*, Statista [website], 20 May 2019. Available from: https://www.statista.com/topics/3853/internet-usage-in-europe/ (accessed 25 June 2019).

The public use of the internet has transformed virtually every aspect of life. It has revolutionised the ways in which people communicate, obtain information, make commercial transactions, and much more. Although the benefits of the internet to modern society are countless, it must also be recognised that the same technology that facilitates communication can also be exploited by terrorists.

Internet also revolutionized the way terrorist operate. The interactive capabilities of the internet have allowed all terrorist groups to have established some sort of presence on the internet.[107] For example, "[a]bout 90% of terrorist activity on the internet is using social networking tools […]."[108] Internet has become a platform for terrorists to spread their message, to communicate with one another and to gain sympathizers.[109] They are no longer confined to specific regional boundaries. The very essence of terrorism is the promotion of fear by attracting attention, and to achieve that, terrorists must find ways to expose themselves and their views through publicizing their attacks into the world.

> *Computer-mediated communication is ideal for terrorists: it is decentralized, cannot be subject to control or restriction, is not censored, and allows free access to anyone who wants it. The typical, loosely knit network of cells, divisions, and subgroups of modern terrorist organizations, finds the Internet both ideal and vital for inter- and intra- group networking.*[110]

Also, though the use of IT, terrorists have diversified their targets and operations, and have developed ways to attack computer networks, including those on the internet, becoming what is known as cyberterrorism. According to the 2012 United Nations Office on Drugs and Crime (UNODC) publication *The use of Internet for Terrorist purposes*, the internet *"*can be used for glorification of terrorists acts, incitement to commit acts of terrorism radicalization and recruitment of terrorists, dissemination of illegal content,

---

[107] Mark Last and Abraham Kandel, eds., *Web Intelligence and Security: Advances in Data and Text Mining Techniques for Detecting and Preventing Terrorist Activities on the Web*, IOS Press, The Netherlands, November 2009, p. 20.
[108] Last and Kandel, eds., Ibid, p. 19.
[109] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, United States Institute for Peace, Washington D.C., 2006, p.6.
[110] Weimann. Ibid. P.3.

facilitating communication between terrorist actors and the training of potential recruits.*"*[111] Terrorists can also use social media, encrypted channels and the dark web to spread propaganda, recruit new followers and coordinate attacks. In other words, terrorists can make use social media to promote themselves, just like companies and brands do. Terrorist organisations also use online platforms to radicalise people across the globe. Those recruits may then travel to join the organisation groups in person or commit terrorist attacks in their support, from their home countries.

Most of the innovative digital companies, such as social networks are based on individuals willingly sharing their personal data on the internet. "Around 70% of the world's digital content is generated by individuals and most of these data are stored by large private companies on content-sharing websites such as YouTube."[112] Just as any other individual, terrorists can make use of these platforms to easily reach the public directly and make their existence, their achievements and goals known at an international scale.

Nevertheless, all of the activities carried out online can unwillingly leave behind traces that, when gathered, can project 'biometric data.' When analysed, biometric data can show a lot about a person. That data are traceable and can be collected, stored and exchanged by interoperable data systems.[113] It can illustrate who and how the person is by considering all its activity online. Governments trying to respond to terrorism and security threats consider biometrics as a very attractive tool. Through the analysis of this data it is possible to identify an individual's physical and behavioural characteristics[114].

In today´s world, the frontline against terrorism is increasingly in the cyberspace. Modern conflicts are no longer confined in the physical world; they have spread into the cyberspace. With the use of online platforms, terrorist are able to carry out activities beyond border and spread fear.

---

[111] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, United Nations, New York, 2012, p. 3.
[112] Ioannis A. Tsoukalas and Panagiotis D. Siozos, Privacy and Anonymity in the Information Society – Challenges for the European Union, The Scientific World Journal, 1 March 2011, Vol. 11, p. 459.
[113] Tsoukalas and Siozos, Ibid, p. 459.
[114] J. E. Mills and Sookeun Byun, *Cybercrimes against Consumers: Could Biometric Technology Be the Solution?*, IEEE Internet Computing, July-Aug 2006, vol. 10, no. 4, p. 64.

Computer systems are fundamental to carry out many essential everyday functions, for example, the operation of Critical Infrastructures (CIs). The dependence of CIs on Information Technology (TI) systems makes them potential targets for groups interested in acts that may produce physical harm or even the loss of life. Terrorist groups can exploit the internet and other computing technologies and software as supporting tools to their actions in the physical world.

In this regard, several measures have been taken with the aim to tackle the use the internet for terrorist purposes by the international community, but also by the European Union. For instance, in 2015, the European Commission created the EU Internet Forum as an attempt to stop the misuse of the internet by terrorist groups. The forum acts as a platform between the online industry, civil society and the EU. It works in two ways: 1) It aimed at reducing the amount of terrorist content available on the internet, for which it liaises with other EU institutions such as Europol[115]; and 2) it aimed to empower civil society partners to amplify counter terrorism narratives.[116] According to the commission, these collective measures by the EU have substantially reduced the presence of abuse in the internet of international terrorist groups. The encouragement of participation from all stakeholders also promotes for checks-and-balances, conditions that allow for a greater protection of human rights.

> *Nevertheless, while terrorist content by some terrorist groups is on the decline, other violent extremist groups are seeking to increase their online presence. Tackling this challenge, while protecting the Union´s fundamental values of freedom of speech, remains at the forefront of our EU counter terrorism efforts.* [117]

---

[115] *EU Internet Forum: Progress on removal of terrorist content online*, European Commission [website], San Francisco, 10 March 2017. Available from: http://europa.eu/rapid/press-release_IP-17-544_en.htm (accessed 4 July 2019).

[116] *EU Internet Forum: Civil Society empowerment programme*, European Commission [website], 2017. Available from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en (accessed 4 July 2019).

[117] *EU Internet Forum: Progress on removal of terrorist content online*, European Commission [website], San Francisco, 10 March 2017. Available from: http://europa.eu/rapid/press-release_IP-17-544_en.htm (accessed 4 July 2019).

Online privacy and data protection have become an issue of major political concern. The portion of the internet, known as the Dark Web or the Darknet, forms part of the deep cyberspace where sites and users can interact in anonymity by encrypted engines. It works as a "worldwide decentralised network of hundreds of computers, whose owners configure them and contribute internet bandwidth to create a series of routing points or nodes."[118] There are no names in the Dark Web, which allows for the publication of websites and dissemination of information without revealing any information from the publisher, such as identity or location. The Dark Web is inaccessible for traditional investigative or navigation tools and technologies. Therefore, offering anonymity and protection to users from those who keep track of what people do online.[119]

While the Dark Web was neither created nor intended for illegal purposes, it does allow access to a variety of illegal transactions: illegal markets, hidden meetings or encounters and criminal databases. The dark web makes use of applications and network protocols for encryption and anonymization that obstructs law enforcement to investigate illegal activity. Due to the privacy advantages of the Dark Web, it has become an ideal environment for the preparation and implementation of illegal activities targeted at both physical and virtual atmospheres. However, it also serves as a platform for refuge for those who may be persecuted or for whose ideas may be threatened or suppressed. It has allowed for individuals to reclaim privacy and protect their identities in the cyberspace. "On the Darknet, human rights and political activists enjoy privacy, a safe haven where they can avoid surveillance."[120]

[118] Andreas Zaunseder, *The darknet is not a hellhole, it's an answer to internet privacy,* The Conversation, United Kingdom, 16 August 2018. Available from: https://theconversation.com/the-darknet-is-not-a-hellhole-its-an-answer-to-internet-privacy-101420 (accessed 2 August 2019).
[119] Dave Piscitello, *The Dark Web: The Land of Hidden Services*, Internet Corporation for Assigned Names and Numbers [website], 27 June 2017. Available from: https://www.icann.org/news/blog/the-dark-web-the-land-of-hidden-services (accessed 2 August 2019).
[120] Cath Senker, *Cybercrime & the Dark Net: Revealing the hidden underworld of the internet*, Arctus Publishing Limited, London, 2016, p. 4.

3.1 Cyberspace

The notion of "cyberspace" praises to the emerging 'Global Information Infrastructure' (GII). "The GII, like all information infrastructures, moves information from sender to receiver through some medium. Physically, in cyberspace, information usually moves through a hybrid of wireline and wireless pathways."[121] Digitally, cyberspace transfers, processes, and stores information faster, cheaper and more efficiently than any other information structure that has ever existed. "Cyberspace is an environment comprised entirely of 0's and 1's: simple binary switches that are either off or on. No in-between. No halfway. No shades of grey."[122] Once information is transported, it is processed to provide some communicative functionality. I believe that as digital infrastructure keeps upgrading, and technological literacy expands, the use of the cyberspace for communication transactions will grow even further and it will diversify.

The notion of physical space "is a basic concept which underlines our understanding of the world around us, the entities within it, and our own and other people's movements through it."[123] Cyberspace, as the physical space, is also a concept which features those same understandings but rather its translation into "the world of electronic communications, the entities which populate it and our movements through it."[124] The physical world is reflected into the digital one, thus it is people who created it and feed it. "Cyberspace is also home to virtual worlds that parallel the behavioural settings and rules of places and social networks in physical space, and some that don't."[125]

---

[121] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1998, p.1220.
[122] Beth E. Kolko, Lisa Nakamura, Gilbert B. Rodman, ed., *Race in Cyberspace*, Routledge, New York and London, 2000, p.1.
[123] Rebecca Bryant, *What kind of Space is Cyberspace*?, Minerva- An Internet Journal of Philosophy Vol. 5, 2001, p. 140. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.125.5433&rep=rep1&type=pdf (accessed 31 July 2019.
[124] Bryant, Ibid, p. 141.
[125] Donald G. Janelle and David C. Hodge, eds., *Information, Places and Cyberspace: Issues in Accessibility*, Springer, New York, 2000, P.4.

Cyberspace directly affects every aspect of society including economic, social, cultural and political developments, and the rate of immersion into the web keeps increasing. "Cyberspace may be seen as an electronic linkage of computers and their users that facilitates interaction through shared hardware, software, and protocols for communication."[126] Flowing through this web is information, which makes useful our telephones, radios, televisions, satellite dishes, localization systems, weather monitors, radars, and all computer networks.[127] Our dependency on cyberspace is unprecedented and affects our everyday lives. We increasingly speak, listen and act through cyberspace. The physical objects of traditional communication, such as letters, books or newspapers, are gradually being superseded by new electronic objects. "[T]he data collected in these various domains can be aggregated to produce telling profiles of who we are, as revealed by what we do and say. The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observations of our selves possible."[128] On the one hand, cyberspace is a place for innovation, interaction and economic growth, and on the other hand, criminals, spies and terrorists use cyberspace as a place for their activities.

> *Cyberspace will never be immune to attack—no more than our streets will be immune to crime. But with stronger cybersecurity, increased use of active cyber defenses, and international cyber norms, we can hope to at least keep a lid on the problem.*[129]

In recent years, the cyberspace has become a focal point in security issues. From a privacy perspective, the crucial characteristic of cyber-activity is the rich flow of personal information it generates. Concepts and terms such as "hybrid operations", "cyber-crime", "cyber-threat", "cyber-defence" and "cyberterrorism" have emerged in discussions and debates regarding security. As a result, actions to safeguard states and

---

[126] Donald G. Janelle and David C. Hodge, eds., *Information, Places and Cyberspace: Issues in Accessibility*, Springer, New York, 2000, P.4.
[127] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1998, p.1221.
[128] Kang, Ibid, p.1199.
[129] Dorothy Denning, *Cybersecurity´s Next Phase: Cyber Deterrence*, The Conversation, Scientific American [website], 13 December 2016. Available from: https://www.scientificamerican.com/article/cybersecuritys-next-phase-cyber-deterrence/# (accessed 2 July 2019).

their people from those threats that attempt to compromise core EU values as human dignity, democracy, the rule of law, equality and respect for human rights, have also developed. With the increased use of technology worldwide, terrorist threats can take the form of and can be carried out through the cyber domain.

The anonymity and freedom of movement in the cyberspace are incomparable. "The internet has made information exchange easier and more efficient, but it has also created a new space in which criminals and terrorists can operate almost undetected."[130] Therefore, tackling cyber-threats pose a big challenge for police and law enforcement agencies. Websites, domains and even IP addresses can easily be created and/or moved outside any given jurisdiction to a location with different laws or unwilling to cooperate with law enforcement.

> *In cyberspace there are no borders because traditionally understood, although ICT infrastructure is located in specific countries, it is immaterial, but operates on the basis of the actually existing infrastructure, generating an electromagnetic field. Using this feature, you can get tangible material benefits.*[131]

Even though states regulate Internet Service Providers (ISP), states share internet governance with the private sector. "Almost all software and hardware, entire networks and, in many cases, even critical infrastructure, are owned by private firms."[132] However, governments have been trying to increase their role in the cyberspace, but due to its very nature, the web remains largely unregulated or self-regulated, and jurisdictions are not clearly defined.

---

[130] R. Gandhi, A. Sharma, W. Manhoney, W. Sousan, Q. Zhu, P. Laplante, *Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Politica*l, IEEE Technology and Society Magazine, Vol. 30, Issue 1, Spring 2011, 7 March 2011, p.28. Available from: https://ieeexplore.ieee.org/document/5725605/authors#authors (accessed 2 august 2019).

[131] Isabela Oleksiewicz, *Challenges of EU Security on the example of cyberterrorism policy*, Journal of International Trade, Logistics and Law, Vol. 1, Num. 1, 2015, p. 27.

[132] European Parliamentary Research Service [website], *Briefing: Cyber security in the European Union*, 2013, p.2. Available from: http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf (accessed 12 June 2019).

In the European Union, its individual member states are responsible for their own cyber-capacities, and security. Member states have a wide variety of levels of maturity and development, with different threats, priorities and capabilities.[133] Nevertheless, all of them are bound not just by treaties that recognise human rights at an international level, but also by being parties to the European Convention of Human Rights in the regional level. Further, the protection of privacy represents a core human right for democracies obeying the rule of law.

Despite limits to its competence, the EU has sought to collaborate in a comprehensive platform for common cyber security efforts by its member states. Through the Cybersecurity Act,[134] the European Union Agency for Cybersecurity (ENISA) was strengthen by appointing to the agency the permanent mandate of supporting the EU in achieving a common high level of security. ENISA also contributes as a 'capacity builder' for member states as well as a crucial source of independent advice and guidance for policy-implementation. [135]

The Act also established the first EU- wide cybersecurity certification framework.[136] By doing this, the EU aims to tackle network security issues and set up standardised general procedures for the protection of critical infrastructure in Europe. Moreover, the EU has also established regulations concerning criminal offences in the cyber domain and promoted the cooperation of law enforcement agencies through Europol, that includes the creation of the European Cybercrime Centre.[137] Nevertheless, there are still further steps to take in cyber regulations. Providing security still represents

---

[133] Jaap de Hoop Scheffer, Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans, Andrea Renda, *Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force*, Centre por European Policy Studies, Brussels, November 2018, p.18.

[134] *The cybersecurity Act at a Glance*, European Commission [website], 6 August 2019. Available from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance (accessed 1 august 2019).

[135] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC (accessed 1 August 2019).

[136] *The EU cybersecurity certification framework*, European Commission [website], 24 July 2019. Available from: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed 1 August 2019).

[137] European Parliamentary Research Service [website], *Briefing: Cyber security in the European Union*, 2013, p.2. Available from: http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf (accessed 12 June 2019).

the main responsibility of national governments. It seems that, governments do not like sharing information and that their differences in legislations create a challenge for a collaborative approach when dealing with cyberterrorism.

3.2 Cyberattacks

Equally to terrorist attacks, cyberattacks can be socially or politically motivated but they are carried out primarily through the internet. Attacks can be random or specifically targeted, and can aim at the general public, national or corporate organisations. Cyberattacks are carried out through the spread of malicious programs (viruses), unauthorised web access, fake websites, and other means of stealing personal or institutional information from targets of attack, causing far- reaching damage.[138]

As IT capabilities increase, cyberattacks continually becoming more sophisticated. Most of society's critical or vital infrastructure are notable, for example, water, energy, railway networks, airports or banking, nowadays none of these could really function without the internet.[139] Also, the absence or lack of regulation and a general increasing focus of profitability and productivity has forced more companies and utilities to move their operations to the internet, for the sake of improved efficiency and reduced costs. "The Internet thus is not only becoming the backbone of all kinds of societal processes, it is also, more importantly, becoming the backbone of backbones. This makes society extremely vulnerable to failures or attacks to internet infrastructure."[140] In that sense, cyberattacks pose an increasing number of threats to a wide range of targets.

---

[138] *What constitutes a cyberattack?*, Information Management, NEC Corporation [website]. Available from: https://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html (accessed 19 July 2019).

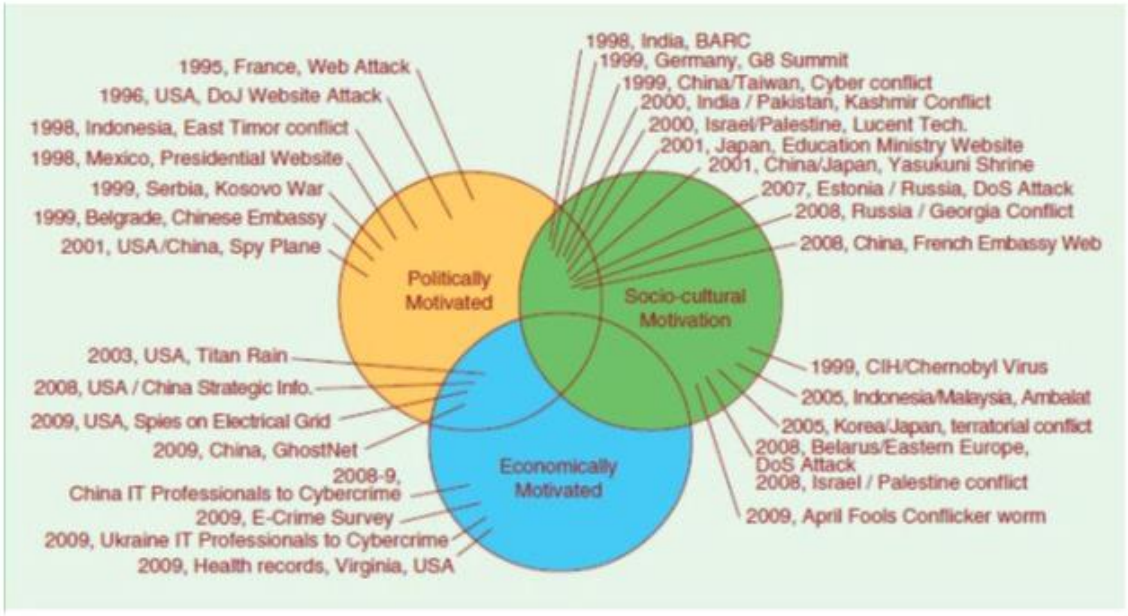
[139] *Critical infrastructure*, Migration and Home Affairs, European Commission [website], Available from: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (accessed 7 July 2019).

[140] Babak Akhgar and Ben Brewster, *Combating Cybercrime and Cyberterrorism: Challenges, trends and priorities*, Advanced Sciences and Technologies for Security Applications, Springer, Switzerland, 2016, p.5.

As defined by the United Nations Office on Drugs and Crime´s 2012 publication on *The Use of Internet for Terrorist Purposes*, a

> *Cyberattack generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers of underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, phlooding, or other means of unauthorised or malicious access.*[141]

Furthermore, cyberattacks may have the characteristics of an act of terrorism, (the desire to create fear with the aim of political, social or economic objectives). Although, not all cyberattacks are intended to disrupt peace or promote fear.



142

[141] United Nations Office on Drugs and Crime, *The Use of Internet for Terrorist Purposes*, United Nations, New York, 2012, p. 12.

[142] Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P., Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, IEEE Technology and Society Magazine, Vol. 30, Issue 1, Spring 2011, 28 -38. See also, *Cyber Terrorism: understanding and preventing acts of terror within our cyber space*, Medium Corporation, 7 June 2017. Available from: https://littlefield.com/cyber-terrorism-

Figure 1. An example of cyberattacks around the world and their distribution across cultural, social, economic and political motivations.

Cyberattacks can manifest in different forms, and it is through these forms that it can be understoood weather the attack is of crime or terror. The analysis of cyberattacks display a wide variety of possible techniques:

> *[T]errorist could bypass the integrity, confidentiality, and availability of computer systems and data, either by hacking computers, deceiving victims, or spreading viruses and worms, thus manipulating systems, or by bringing about mass queries and other large-scale attacks on victim´s computer systems.*[143]

If the attacked IT systems are connected to other critical systems and infrastructure, it can result in both the disruption of services, as well as physical harm and loss of life. Physical damage could be reached by, for example, attacking the computers of electrical supply systems, hospitals, food production, pharmaceutical companies, air and railroad or other transport control systems, hydroelectric dams, military control systems and their weapons controls, or even nuclear power stations.[144]

understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb (accessed 1 august 2019).

[143] Ulrich Sieber, *International Cooperation against terrorist use of the internet*, Revue Internationale de Droit Pénale, Vol. 77, no. 3, 2006, p. 395 – 449, available from: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm#no19 (accessed 3 July 2019).

[144] Ulrich Sieber and P. Brunst, *Cyberterrorism and other use of internet for terrorist purposes: Threat Analysis and Evaluation of International Conventions*, Council of Europe Publishing, Strasbourg, 2007, p 12.

3.3 Cyberterrorism

The new generation of terrorists is now growing in the digital world. As technologies evolve, hacking tools will certainly become more powerful, simpler to use and easier to access. Cyberterrorism poses a emerging threat to peace and stability.

An agreement on a common definition of cyberterrorism among the nations is much needed. However, the international community has not been able to succeed in a commonly accepted comprehensive definition of "terrorism" itself. Although there are many reasons for this, it can be reduced as:

> *Firstly, States fundamentally disagree as to the distinction between freedom fighters and terrorists. Secondly, States disagree as to weather a definition of terrorism in international law should cover State acts or not. These differences are politically and ideologically driven, with a State's perspective on the issue predicted by its own self- interests.*[145]

However, there are treaty- based definitions for terrorist crimes that can be found in the 19-international counter- terrorism legal instruments, of which around two-thirds of all UN member states have either ratified or acceded to at least 10 of the 19 instruments. There is no longer any country that has neither signed nor become party to at least one of them.[146] These international instruments, as well as a great number of important Security Council resolutions, e.g. Resolutions 1267 (1999)[147], 1373 (2001)[148] and 1540 (2004),[149] 1566 (2004), make up what the United Nations Office on Drugs and Crime (UNODC)

[145] Alan Greene, *Defining terrorism: One size fits all*?, International and Comparative Law Quarterly, Cambridge University Press, Vol. 66, Issue 2, 20 February 2017, p. 412.
[146] Counter- Terrorism Committee, *International legal instruments*, Security Council. Available from: https://www.un.org/sc/ctc/resources/international-legal-instruments/ (accessed 28 July 2019).
[147] S/RES/1267 (1999) Establishes Security Council Committee; imposes limited air embargo and financial embargo on the Taliban (paras 4 & 6). Available from: https://www.un.org/securitycouncil/s/res/1267-%281999%29 (accessed 31 July 2019).
[148] S/RES/1373 (2001) On threats to international peace and security caused by terrorist acts. Available from: https://www.refworld.org/docid/3c4e94552a.html (accessed 31 July 2019).
[149] S/RES/1540 (2004) Regarding non- proliferations of weapons of mass destruction. Available from: http://unscr.com/en/resolutions/doc/1540 (accessed 31 July 2019).

calls the universal legal regime against terrorism. In addition, offences related to terrorism may exist in national legislations.

The 1994 General Assembly's Declaration on Measures to Eliminate International Terrorism, resolution 49/60, stated that terrorism includes "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes," and that such acts "are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them."[150]

On 16 February 2011, the Special Tribunal for Lebanon, the world's first international court with jurisdiction over the crime of terrorism, issued its Interlocutory Decision on the applicable law, where it recognised a definition of 'transnational terrorism' within customary international law.[151] Making it the first time that an international tribunal has confirmed a general definition of terrorism under international law.[152] However, "[t]he Tribunal's ruling, together with its underlying legal basis, were significantly criticized and not widely accepted, including for not meeting the necessary legal threshold tests in terms of state practice and *opinion juris*."[153] The ruling stated:

> *As we shall see, a number of treaties, UN resolutions, and the legislative and judicial practice of States evince the formation of general 'opinio juris' in the international community, accompanied by a practice consistent with such 'opinio', to the effect that a customary rule of international law regarding the international crime of terrorism, at least in time of peace, has indeed emerged. This customary rule requires the following three key elements: (i) the perpetration of a criminal act (such as murder, kidnapping, hostage- taking, arson, and so on), or threatening such an act; (ii) the intent to spread fear among*

[150] General Assembly Resolution A/RES/49/60, *Measures to eliminate international terrorism*, 17 February 1995, p. 4, no. 3. Available from: https://undocs.org/en/A/RES/49/60 (accessed 30 July 2019).
[151] *The cases: Key Developments (Case Timeline*), Special Tribunal for Lebanon. Available from: https://www.stl-tsl.org/en/the-cases/stl-11-01/key-developments (accessed 31 July 2019).
[152] Michael Scharf, *Special Tribunal for Lebanon issues Landmark Ruling on Definition of Terrorism*, School of law of Case Western Reserve University, 22 February 2011. Available from: https://law.case.edu/Academics/Centers-and-Institutes/Cox-International-Law-Center/Grotian-Moment/ArtMID/804/ArticleID/158 (accessed 30 July 2019).
[153] *E4J University Module Series: Counter- Terrorism*, United Nations Office on Drugs and Crime, July 2018. Available from: https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html (accessed 30 July 2019).

the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it; (iii) when the act involves a transnational element.[154]

The European Union presents its approach to define terrorism. Instead of referring to the criminal elements of offence surrounding it in the Council Framework Decision of 13 June 2002, on combating terrorism, article 1- Terrorist offences and fundamental rights and practices, states:

> 1. *Each Member State shall take the necessary measures to ensure that the international acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or a international organisation where committed with the aim of:*
> *- seriously intimidating a population, or*
> *- unduly compelling a Government or international organisation to perform or abstain from performing any act, or*
> *- seriously destabilising or destroying the fundamental political, constitutional, economic or social structure of a country or an international organisation,*
> *Shall be deemed a terrorist offence: […]*[155]

Cyberterrorism is a frightening and specific new form of terrorism. It is a combination of cyberspace and terrorism meaning that such activity is associated not only with the hostile use of Internet Technologies (IT) and actions in the virtual or online sphere, but it is also characterised by all constitutive elements for the terrorist activity, except that it happens online. There are a number of reasons that may explain why the

[154] Special Tribunal for Lebanon, *Major rulings issued by the Special Tribunal for Lebanon*, Leidschendam, The Netherlands, 2001, p. 87, no. 85. Available from: https://www.stl-tsl.org/sites/default/files/documents/legal-documents/stl-casebooks/STL_Casebook_201_EN.pdf (accessed 31 July 2019).
[155] See *Council Framework Decision on combating terrorism*, Council of the European Union, 13 June 2002. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN (accessed 30 July 2019).

term ‘cyberterrorism’ has not been internationally legally defined, including the difficulty in identifying the parameters of what should be constructed applicable activities. When considering what cyberterrorism actually means, we must first understand the motivations behind cyberattacks. I consider that, attempting to define the phenomenon, simply by attaching the word “cyber” to the broad definition of “terrorism” does not yield a meaningful result. Rather, it is necessary to develop a separate, independent definition. As a starting point, it is helpful to refer to the proposal for the International Convention to Enhance Protection from Cybercrime and Terrorism, also called the Stanford Draft, which was developed by a group of experts and scholars in the field. It provides a definition of cyberterrorism, although it has not been able to revive much interest by the global community, yet. The Draft requires states party cooperation through mutual legal assistance and law enforcement provisions. States party are also obligated to exchange information, assist in gatherings and preserving evidence, arrest alleged offenders, prosecute or extradite them, and to implement agreed international standards dealing with security and law enforcement.[156] According to article 1 of the draft convention:

> *cyberterrorism means international use, or threat of use, without legally recognised authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm.* [157]

Since ITs are ever evolving instruments, cyberterrorism is by its very nature considered to be a dynamic phenomenon. A terrorist´s ability to control, disrupt or alter the command and monitoring functions performed by vital infrastructure´s systems could threaten national and, possibly, regional security. According to the former Director of the Georgetown Institute for Information Assurance, Dorothy E. Denning’s article “*Is Cyber terror next?*”, the term refers to the

[156] Abraham D. Sofaer, Gregory D. Grove and Gorge D. Willson, *A proposal for an International Convention To Enhance Protection from Cybercrime and Terrorism*, The Information Warfare Site, 2001. Available from: http://iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm (accessed 15 July 2019).
[157] Sofaer, Grove and Willson, Ibid.

> *unlawful attacks and threats against computers, networks and the information that may be stored in them with the intention to intimidate and/or coerce the government or its people in order to achieve certain political or social benefits.*[158]

In addition, for an attack to qualify as a cyberterrorism attack, its drive must be "made as a result of violence against people or property or at least cause significant damage in order to induce fear". [159]

Derived from the above arguments, certain attributions that cyberattacks may have can be defined to be considered cyberterrorism. The incident can be divided in three aspects that must be present in the attack. 1) The attack must be intentional, as a result of a conscious calculation from the perpetrator, and aimed at attaining a political, economic, religious or social impact, in the same way a physical terrorist attack would. 2) The incident must entail some level of violence or threat of violence, which could take the form of property violence and cause significant civil disorder, harm or fear of harm. 3) The perpetrator (s) cannot be state actors, but rather sub-national actors. In other words, the attack must be outside the context of cyberwarfare, that is, the act must be outside of the parameters of international humanitarian law that prohibit deliberately targeting civilians or non- combatants.[160]

Simply put, cyberterrorists attack their targets electronically. It is an attack executed via information systems to significantly interfere with the political, social or economic operative of groups or organisations of a nation or induces physical violence and creates panic and fear.

---

[158] Dorothy E. Denning, *Is cyber terror next?* (essay), Social Science Research Council [website], New York,1 November 2001. Available from: http://essays.ssrc.org/sept11/essays/denning.htm (accessed 6 July 2019).
[159] Dorothy E. Denning, *Is Cyber terror next*?, Social Science Research Council [website], 1 November 2001. Available from: http://essays.ssrc.org/sept11/essays/denning.htm (accessed 6 July 2019).
[160] Max Roser, Mohamed Nagdy and Hannah Ritchie, *Terrorism*, Our World in Data, January 2018. Available from: https://ourworldindata.org/terrorism (accessed 29 July 2019).

In the public discussions on cyberterrorism, there are numerous possible scenarios in which terrorists might abuse the internet to commit diverse types of attacks.[161] There are many speculations of how terrorists or terrorists groups might be able to cause harm to society´s infrastructures and its people, by attacking systems and networks. "For example, if telecommunications and emergency services had been completely dismantled in a time of a crisis, the effects of that sort of infrastructure attack could potentially be catastrophic."[162] Through the use of IT, terrorists have the capacity to perform coordinated global cyberattacks and evade surveillance. According to present studies and theories, "cyberterrorism could attack anything that is important to modern society and that is connected to the Internet or accessible via other communication lines."[163]

In the regional context, the European Commission and High Representative of the EU for Foreign Affairs and Security Policy presented on 2013 the *EU Cyber Security strategy: An open, safe and secure Cyberspace*. This strategy declared that the EU´s core values applied as much in the digital as in the physical world. Which means that the same laws and norms that apply in other areas of our everyday lives apply also in the cyber domain. [164] In broad terms, this policy raised the level of importance of crimes committed in the cyber domain. Cyberterrorist attacks are as important and dangerous as any terrorist attacks carried out in the physical world. Also, the strategy recognises the role of the private sector in the significant partial ownership and operation of cyberspace and calls for national governments to "safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet."[165]

---

[161] See for example: Thomas Oriti, *Cyberterrorists targeting healthcare systems*, critical infrastructure, ABC News [website], 23 October 2017. Available from: https://www.abc.net.au/news/2017-10-23/forget-explosives,-terrorists-are-coming-after-cyber-systems/9076786 (accessed 27 July 2019) or *Global nuclear facilities 'at risk' of cyber attack*, BBC News [website], 5 October 2015. Available from: https://www.bbc.com/news/technology-34423419 (accessed 27 July 2019).

[162] Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In brief*, Congressional Research Service, Washington D.C., 27 March 2015, p.9.

[163] *Organised Crime Situation Report 2004. Focus on the threat of cybercrime*, Council of Europe, Strasbourg, 23 December 2004, p. 127. Available from: https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf (accessed 16 July 2019).

[164] *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*, European Commission and High Representative of the EU for Foreign Affairs and Security Policy, Brussels, 7 February 2013, para. 2.

[165] Ibid, p.2.

Most countries around the world rely on their foreign agreements and domestic policies, military structures and legal and budgetary capabilities, to develop their own cyber-capacities on security. In this regard, there is a delicate balance between what constitutes states´ sovereignty and the EU's power and responsibly to protect its citizens, that becomes an even greater challenge to apply in the cyberspace. On the one hand, EU member states are responsible for their own cyber capacities, facing a wide stages of cyber-maturity and development, different priorities, threats and capabilities. On the other hand, all member states are bound by EU regulations, regardless of their advancement in online security. In that regard, the EU works to develop a comprehensive cyber defence regulation within a Common Security and Defence Policy (CSDP).[166] The CSDP offers a framework for enhanced cooperation among member states by sharing military capabilities and supports the strengthening of the European defence industry. The EU Cyber Defence Policy Framework (CDPF) was last updated in 2018 as a response to the changing security challenges. The framework helps clarify the roles of different European actors and focuses in strengthening the cyber protection of the EU´s security and defence infrastructure.[167]

3.4 Countering Cyberterrorism

Countering Cyberterrorism is not an easy task. Unless intending to claim responsibility for their actions to make a point, perpetrators can hide in the vastness of the cyberspace and lurk behind hidden IP addresses and proxy servers. This challenge relates to the security versus privacy frame. Moreover, privacy is not the only human right

[166] *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*, European Commission and High Representative of the EU for Foreign Affairs and Security Policy, Brussels, 7 February 2013, p.11.
[167] See *EU Cyber Defence Policy Framework (2018 update),* Council of the European Union, Brussels, 19 November 2018, No. of Doc. 14413/19.

at issue: freedom of expression, association, non-discrimination, and the right to an effective remedy are equally relevant in anti- cyberterrorism policy and practice.

The actions of terrorists not only directly affect individual's human rights, "but also foster an atmosphere of fear and dread that devastates peace and social order" and the measures to counter the attackers "impede the essential functions of the social order and lead to inefficiency, lower standards of living, mutual distrust, and fearful, brutish lifestyle."[168]

As the case of physical acts of terrorism, cyberterrorism uses unlawful methods for intimidation, threat of violence and the promotion of fear, thus according to international law, the response should always be directed at ensuring the rule of law. An effective response to terrorism must essentially include a strong criminal justice element: "one that is guided by a normative legal framework and embedded in the core principles of the rule of law, due process, and respect for human rights."[169] I believe that the advantages of the internet should not only serve terrorists but also those who confront them. Not only in terms of monitoring and learning about terrorists' activities, but also in launching and managing pre-emptive antiterrorist campaigns. Preventing and countering cyberterrorism must use tools that places human rights values at its core.

A key feature in many international legal instruments against terrorism is an obligation that requires states parties to establish certain identified terrorism related offences, in their national legislations, as criminal offences. "States need adequately functioning counter- terrorism legal regimes and criminal justice systems, as well as the related capacity to deal with potentially complex criminal cases and engage effectively in internationally criminal justice cooperation."[170] Therefore, perpetrators of terrorist acts, as defined in the universal legal instruments against terrorism,[171] are criminals, and should

[168] Mark D. Kielsgard, *A human rights approach to counter- terrorism*, California Western International Law Journal, Vol. 36, No. 2, Spring 2006, p. 260.
[169] *Handbook on Criminal Justice Responses to Terrorism*, United Nations Office on Drugs and Crime, New York, 2009, p. 3.
[170] Ibid, p.3.
[171] See for example, Security Council Resolution 2322 (2016) paragraph 3 : "terrorism in all its forms and manifestations constitutes one of the most serious threats to peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivation, whenever, wherever, and whomsoever committed". Or article 2: "those responsible for committing or otherwise responsible for terrorist acts, and violations of international humanitarian law or violations or abuses of human rights in this context, must be held accountable".

face proper criminal justice processes to ensure that justice is achieved but also to ensure that the rights of those accused and the victims are protected.

In addition to this core function, a criminal justice approach to terrorism should also consider effective prevention mechanisms that include: countering the funding of terrorists and terrorist organizations; interception of schemes to commit attacks; and prohibition of incitement of terror.

Transferring that same criminal justice approach into the digital world, the same rules apply; those who commit attacks, promote or incite terrorism, are also criminals, and must be treated as such. However, I believe much greater international cooperation is especially needed in relation to countering cyberterrorism due to its global nature. "Cybercrime is quintessentially transnational and will often involve jurisdictional assertions of multiple States. Agreements on jurisdiction and enforcement must be developed to avoid conflicting claims."[172]

Moreover, the internet is not a complete public space and it functions at an international scale. The development of information and communication technologies have been largely controlled by the private sector. Governments cannot fully control what takes place in the internet. The internet and the cyberspace are partially owned and operated by private companies scattered around the world.

> *The internet has been constructed as a private and non-hierarchical global network without specific location and definitely not under state control. The sheer volume of today's internet communication makes it an impossible task for state authorities with limited resources to 'check the web'. And 'normal' police and prosecution authorities often lack the technological experience and capacity to investigate and prosecute effectively in a complex data-processing environment.*[173]

[172] Abraham D. Sofaer and Seymour E. Goodman, *A Proposal for an International Convention on Cyber Crime and Terrorism*, Center for International Security and Cooperation, Stanford, August 200. Available from:https://cisac.fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a (accessed 28 July 2019).

[173] J. Vogel, *Towards a Global Convention against Cybercrime*, First World Conference of Penal Law, Penal Law in the XXI Century, 18- 23 November 2007, Guadalajara, Mexico, p. 4. Available from: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf (accessed 31 July 2019).

This makes cyberterrorism a complex, dynamic phenomenon that comprise a great deal of areas of involvement for its development. It is extremally difficult to prevent and counteract. "Capacity limitations often emerge when the police face a terrorist conspiracy, particularly one that is inter-national in nature."[174] For example, terrorists can use commercially produced equipment, and privately-owned servers, they can recruit and coordinate through private social media outlets; and operate in one country and attack in another. Therefore, stronger cooperation must take place, not just between governments, but also between the public and the private sectors. Measures adopted so far have not provided an adequate level of security.

> *While new methods of attack have been accurately predicted by experts and some large attacks have been detected in early stages, efforts to prevent or deter them have been largely unsuccessful, with increasingly damaging consequences. Information necessary to combat attacks has not been timely shared. Investigations have been slow and difficult to coordinate.*[175]

Combating cyberterrorism through indiscriminate massive surveillance dehumanises people and places them not as individuals, but as items of a database. A police database represents people as suspects and victims. "There tends to be less scope for discretionary application of power when the authority comes from a database process rather than from a person. The particular implementation of a system reflects the interests of the institution that created the database."[176] Protecting the right to privacy is not an obstacle to combating terrorism. In accordance with the commitments towards human rights made by states under European and international law, as well as their national constitutions, all measures taken by states to fight terrorism must respect human rights

[174] *Handbook on Criminal Justice Responses to Terrorism*, United Nations Office on Drugs and Crime, New York, 2009, p. 49.
[175] Abraham D. Sofaer and Seymour E. Goodman, *A Proposal for an International Convention on Cyber Crime and Terrorism*, Center for International Security and Cooperation, Stanford, August 200. Available from: https://cisac.fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a (accessed 28 July 2019).
[176] David Holmes ed., *Virtual Politics: Identity and Community in Cyberspace*, Sage Publications, London, p. 89.

and the principle of the rule of law, while excluding any form of arbitrariness, as well as any discriminatory or racist treatment, and must be subject to appropriate supervision.[177] However, all these elements are difficult to fulfil when people are not aware they are being monitored in the first place.

However, article 15[178] of the of the European Convention on Human Rights (ECHR) is a derogation clause that grants the governments of the states parties the possibility of a certain special 'relaxation' to uphold their legal duties, although only in exceptional circumstances, and only in a temporary, limited and supervised manner, from their obligation to secure certain rights and freedoms under the Convention. The article also states that certain other articles in the convention can never be derogated under this provision, such as article 2, right to life, except in respect of deaths resulting from lawful acts of war; article 3, the prohibition of torture and inhumane or degrading treatment or punishment; article 4 (paragraph 1), prohibition of slavery and servitude; and article 7, no punishment without law.

This, of course, represents a problem for privacy. Acts of terrorism, in whatever form, are a public emergency and represent an exceptional circumstance, that threatens the life of any nation and does require exigencies to prevent or contain the situation. Therefore, states feel obliged to take the most drastic actions, including derogating their usual human rights obligations applicable in 'ordinary' times. However, although acts of terrorism, including those carried out through the cyber space, may be time- limited to the act itself, cyberterrorism is not a passing phenomenon and the anti- terrorism legislations tend to become semi- permanent. "While wars or other public emergencies generally have a more-or-less clear end (even if this can be much delayed), there is no

[177] *Guidelines on human rights and the fight against terrorism*, Committee of Ministers of the Council of Europe, 11 July 2002, II.

[178] Article 15 of the ECHR- Derogation in time of emergency:

1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under [the] Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.
2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3,4 (paragraph 1) and 7 shall be made under this provision.
3. Any High Contracting Party availing itself of this derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefore. It shall also inform the Secretary General of the Council of Europe when such measures have operated and the provisions of the Convention are again being fully executed.

end in sight in the fight against terrorism."[179] So the temporality under which article 15 of the ECHR intends states to act upon, can be blurry and pose permanent challenges to certain rights when countering cyberterrorism.

> *A better way to look at questions of the compatibility of anti- cybercrime/ cyberterrorism measures with the human rights framework is the three- prong test for privacy- and free speech-invasive measures that is embedded in the European Convention on Human Rights : (1) does the measure have a legal basis, (2) does it serve a legitimate purpose (such as crime-fighting or national security), and (3) is it a necessary measure, i.e. one that meets the requirements of proportionality and subsidiary in light of the measure's foreseen benefits and effects on human rights?*[180]

In that sense, terrorism has a negative direct and indirect impact in human rights. Not only do terrorist groups deprive individuals of their human rights, but they also drive states into taking counter- terrorism measures, which also serve to diminish human rights.

As in the national level, there are a number of actors dealing with cybersecurity at a EU level. In particular, the European Network and Information Security Agency (ENISA), EUROPOL/ European Cybercrime Centre (EC3) and the European Counter Terrorism Centre (ECTC), the European Defence Agency (EDA) are the four agencies active from the perspective of Networks and Information Systems (NIS). They work to ensure and promote law enforcement, the sharing of intelligence and expertise, and defence, respectively. These agencies have management boards, where the member states are represented. They offer a platform for coordination and provide a joint direction between EU member states in cybersecurity issues.[181]

---

[179] Ian Brown and Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology, Vol. 6 Issue 2, 1 March 2009, p. 120.
[180] Babak Akhgar and Ben Brewster, eds., *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Springer, Switzerland, 2016, p.13.
[181] *Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*, High Representative of the European Union for Foreign Affairs and Security Policy, European Commission, Brussels, 7 February 2013, p. 18. Available from:

Cyberterrorism and the security of the cyber domain is not only an EU problem. Efforts to prevent and counter cyberterrorism are poorly addressed in the global arena. On the 24th of April 2019, the European Union and the United Nations signed a Framework on Counter-Terrorism[182] after several political dialogues on the matter. The purpose was to strengthen the EU-UN partnership by providing an informal framework for guidance and cooperation in counter- terrorism. Although this agreement between the entities is based on the spirit of collective efforts to counter terrorism in all forms and manifestations, it focuses mainly on the physical threat of terrorism and has no direct mention of cyberterrorism. However, it does promote collaboration, technical assistance and the mobilization of resources for the prevention and countering of all forms of terrorism while contributing to the balanced implementation of the commitments and standards against terrorism, with the respect and protection of human rights[183].

3.4.1 Investigation

The vastness and complexity of the internet allows for certain anonymity. Cybercrime acts show a wide-ranging distribution across the range of offences.[184] Cyberterrorism is a crime, but not all cyber-attacks are terrorism attacks. Investigation of crimes carried out in the cyberspace are different from those in the physical world. Although they may share some elements of technique, the tools and methods must adapt to a universe created of digital data. "While some of these investigative actions can be

https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 18 April 2019).

[182] *Framework on counter- terrorism between the United Nations and the European Union*, Brussels, 24 April 2019. Available from: https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf (accessed 31 July 2019).

[183] European Union External Action, *The European Union and the United Nations strengthen partnership on counter- terrorism* [website], Press Release, New York, 24 April 2019. Available from: https://eeas.europa.eu/headquarters/headquarters-homepage/61409/european-union-and-united-nations-strengthen-partnership-counter-terrorism_en (accessed 30 July 2019).

[184] United Nations Office on Drugs and Crime, p. 26.

achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flow."[185]

Every activity conducted online leaves behind trails. "The evidence of cybercrime acts is almost always in electronic, or digital, form." [186] This information can be traced and used to learn more about an individual, what he/she does, where he goes, his interests, the people he interacts with, etcetera. All these private data can be used for the investigation and prevention of cybercrimes and cyberterrorism.

> *Investigating cybercrime in a data processing environment is, of course, a factual challenge because the investigation objects – information systems and data – and methods differ widely from traditional objects – e.g. crime scene – and methods. However, there is also the legal challenge to balance the need for cybercrime- specific investigation powers and fundamental 'cyber rights' such as data privacy and data protection.*[187]

The specific challenge which investigators faces is the need to achieve a balance between fundamental human rights in relation to data protection and privacy, and effective law enforcement techniques necessary to tackle cyberterrorism and cybercrime. The role and functions of police, including their powers of investigation, are normally well established and limited by statutes in their domestic criminal procedure code.[188] "Some of these powers have been enhanced by special legislation, often legislation adopted as a result of a terrorist incident or threat."[189] These legislations may grant them special powers to gather information about an individual or groups of people in order to find suspects of a crime. "Despite two major rulings by the CJEU, which made blanket

---

[185] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations Publications, New York, 2013, p. 122.
[186] UNODC, Ibid, p.122.
[187] J. Vogel, *Towards a Global Convention against Cybercrime*, First World Conference of Penal Law, Penal Law in the XXI Century, 18- 23 November 2007, Guadalajara, Mexico, p. 3. Available from: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf (accessed 31 July 2019).
[188] *Handbook on Criminal Justice Responses to Terrorism*, United Nations Office on Drugs and Crime, New York, 2009, p. 41.
[189] Ibid, 41.

and indiscriminate retention of personal data unlawful, the majority of EU member states have yet to stop the form of surveillance"[190]

As cybercrime becomes more frequent, law enforcement agencies have to question themselves on what it means to 'serve' and 'protect' in the context of crime with a global digital dimension. When investigating cybercrime, each investigative measure must be assessed in its own legal practical context to determine whether its interference with the rights of its subject is justified.

> *These can include viewing, and seizing or copying, computer data from devices belonging to suspects; obtaining computer data from third parties such as internet service providers, and – where necessary- intercepting electronic communications.*[191]

The EU has assumed a leading role in countering cybercrime and cyberterrorism through its own agencies and programmes as well as through supporting external initiatives. In this matter Europol plays a key role in identifying and removing illegal terrorist content through the internet while the EU Internet Forum provides a platform to disrupt terrorist content and amplify counter- narratives on the web.[192] It can be argued that to accomplish that, digital surveillance tools are used to monitor online content. Higher capabilities and tools used by investigators to collect and analyse large amounts of (potentially personal) data may be needed to prevent and counter cyberterrorism, but at the same time they have to comply to various data protection laws in different European countries and underlying fundamental human rights. There are also a number of public and private institutions working at the European level, often in partnership with the EU member states, which facilitate in the investigation of cybercrime and cyberterrorism.

---

[190] *Privacy International, Liberty, and Open Rights Group joined other organisations across the EU to file complaints over Member States' non-compliance with mass surveillance*, Privacy International [website], 25 June 2018. Available from: https://privacyinternational.org/press-release/2119/privacy-international-liberty-and-open-rights-group-joined-other-organisations (accessed 2 august 2019).

[191] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations Publications, New York, 2013, p. 122.

[192] United Nations Office on Drugs and Crime, Module 5: Regional Counter Terrorism Approaches, E4J University Module Series: Counter- Terrorism, United Nations, July 2018.

Tech companies also play an important role through organisations such as the Global Internet Forum To Counter-Terrorism (GIFTC) and Tech Against Terrorism, which aim to empower and build the capacity of all tech companies against their platforms being used by terrorist actors.

The effective use of special investigative techniques in counter- terrorism is a global challenge. The use of special investigative techniques and forensic tools to prevent and counter cybercrime and cyberterrorism pose significant challenges for policymakers and law enforcement agencies. United Nations Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016) and 2396 (2017) call on states to respond to counter terrorist threats in a human right- compliant manner, in line with the respect of fundamental freedoms and other obligations under international law.

The information collected remotely about an individual can build a portfolio with sufficient data to form behavioural biometrics. Behavioural biometrics can make it possible to identify an individual.[193] Many online services already use a system called device *fingerprinting.*

> *This employs software to note things like the model type of a gadget employed by a particular user; its hardware configuration; its operating system; the apps which have been downloaded onto it; and other features, including sometimes the Wi-Fi networks it regularly connects through and devices like headsets it plugs into.*[194]

Biometric data offers a number of practical benefits in law enforcement and intelligence gathering contexts. The use of biometric technology is rapidly advancing and used by multiple actors in state security sectors.[195] However, states not always have proper safeguards to ensure the respect of rule of law and human rights. "Despite

[193] Giles Hogben ed., *ENISA Briefing: Behavioral Biometrics*, European Network and Information Security Agency, January 2010. Available from: https://www.enisa.europa.eu/publications/behavioural-biometrics (accessed 2 August 2019).
[194] *Online identification is getting more and more intrusive*, The Economist [website], 23 May 2019. Available from: https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive (accessed 3 August 2019).
[195] *UNOCT Consolidated Multi- Year Appeal*, United Nations Office of Counter-Terrorism, New York, 2019-2020, p. 85. Available from: https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/UNOCT_Multi-Year-Appeal_Website.pdf (accessed 3 August 2019).

recognition of the importance of rule of law-based approach to biometric use, the legal analysis of, and in particular human rights guidance to its use, remains limited and underdeveloped."[196]

The range of rights that may be implicated in the use of biometric data include freedom of movement, association and expression, due process rights, fair trial and non-discrimination. Nevertheless, the United Nations Security Council resolution 2322 (2016)[197] called on states to strengthen international law enforcement, as well as on judicial cooperation in countering terrorism, through the sharing of information that includes biometric and biographic data. Moreover, the Security Council through resolution 2396 (2017)[198], affirmed that states should develop and implement systems to collect biometric data and that its development and implementation should be undertaken in compliance with international human rights law as well as domestic law.

It is clear that tools such as biometric systems may greatly assist on the investigation of cybercrime and cyberterrorism. However, gathering data about individuals without their knowledge directly affects individuals right to privacy. Also, the retention of that data can pose future threats into a person's integrity. "Information can be misused by making us vulnerable to unlawful acts and ungenerous practices. After all, personal information is what the spying business calls 'intelligence', and such intelligence helps shift the balance of power in favour of the party who wilds it." [199]

In my view, international cooperation can also pose a threat for human rights. Not only is information about individuals being collected and stored, but also transferred to unknown places. Without proper data protection regulations, such data can reveal intimate information about an individual to the world.

---

[196] *UNOCT Consolidated Multi- Year Appeal*, United Nations Office of Counter-Terrorism, New York, 2019-2020, p. 85. Available from: https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/UNOCT_Multi-Year-Appeal_Website.pdf (accessed 3 August 2019).

[197] S/RES/1373 (2001), 28 September 2001. Available from: https://www.un.org/depts/german/sr/sr_01-02/sr1373.pdf (accessed 2 August 2019).

[198] S/RES/2396 (2017), Threars to international peace and security caused by terrorist acts- foreign terrorist fighters, 22 December 2017. Available from: https://www.un.org/sc/ctc/news/document/s-res-2396-2017-threats-international-peace-security-caused-terrorist-acts-foreign-terrorist-fighters/ (accessed 2 august 2019).

[199] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, p.1215, 1999.

Given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation and to promote a common approach to security and counter cyberterrorism human rights at its core. Although some positive steps have been taken between EU member states to increase strong cooperation, differences on many levels create challenges in this regard, such as willingness to share data and delicate information, different legal systems, language barriers, and cultural and policy differences.

3.4.2 Surveillance

Surveillance happens to everyone, every day, as people walk by street cameras, make online purchases, swipe their cards, and surf the World Wide Web. Many people are surrounded by personal devices that are almost always online. As mentioned in the previous section on investigation, those vast observations can be collected by monitoring people's behaviour through their online movements, gathering all sorts of information that could identify them. That information can be stored and shared with others.

According to the Cambridge Dictionary, surveillance can be defined as "the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected"[200]. While this definition focuses on a direct co-presence form of monitoring, it grasps a dimension of surveillance that is increasingly discussed in current debates, which are the elements of prevention and trust. "Surveillance is practice, particularly in workplaces, public spaces, and total institutions, such as prisons and the military, because those in position of authority do not trust or are seeking grounds to trust those below them."[201]

[200] *Surveillance*, Cambridge Dictionary, Cambridge University Press [website], 2019. Available from: http://dictionary.cambridge.org/dictionary/eglish/surveillance (accessed 22 July 2019).
[201] David Lyon ed., *Surveillance as a Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London and New York, 2003, p. 37

Surveillance can be accomplished with the use of several systems and techniques. One of the most common and oldest technics is to follow and watch the individual to gather direct information such as where the individual goes and what he/she does. There are two other techniques for physical surveillance: reconstructive and preconstructive surveillance.[202] Preconstructive surveillance is used to watch certain areas using circuit television cameras that record and transmit to local police agencies. The cameras take recordings of actions and events in specific targeted areas and serve as the law enforcement's eyes and ears. It can also be used to keep a record of frequents the area. Reconstructive surveillance, on the other hand, uses evidence left behind at a crime committed to reconstruct events that have taken place, like finger prints or DNA samples, for example.[203]

However, following somebody around takes a lot of time and manpower. Of course, in cyber space surveillance is not performed through traditional methods, such as a private investigator parked outside the target´s home and observing his movements with binoculars. Instead, it is done through the cyberspace itself, by collecting and examining the data trail left by the individual´s cyber activity. With the increasing use of technology and the sophistication of tools, much of the observation can be done digitally. The aim is to prevent possible crimes or attacks from people who may commit them. "Law enforcement agencies have lobbies for powers to arrest and detain people who they think may be likely to commit crimes, or at least terrorist crimes."[204]

Law enforcement and intelligence agencies are increasingly using sophisticated computer systems, especially reachable databases, to keep tabs on individuals at home, work and in their spare times through their online activity.

> *In respect of mass electronic surveillance and interception, there is increasing evidence emerging regarding the practice of States to out-source surveillance tasks to others. There is credible information to suggest that some*

[202] Robin Williams and Paul Johnson, *Circuits of Surveillance*, Surveillance Soc. Vol. 2, Issue 1, 2004. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1351150/ (accessed 3 August 2019).
[203] Williams and Johnson, Ibid.
[204] Ian Brown and Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology, Vol. 6, Issue 2, 2009, p. 126.

> *governments have systematically routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy.*[205]

Parallel to the development of communications technology, processing capability and storage capacity have also had an exponential increase. Information processing power has reached extreme speeds.

> *New surveillance technologies exploiting these capabilities include mechanisms to monitor, screen and analyse records of billions of telephone and email communications; 'bugs' and tracing technologies that can access the geographical position of mobile phones and act as a remote listening device; and hard to detect (even with antivirus tools) 'spyware', surreptitiously installed on a suspect's computer by the authorities, that can remotely and secretly monitor a suspect's online activity, passwords and email, and even computer's camera and microphone.* [206]

For the purpose of this study, I focus only on digital surveillance and the form of terrorism in question and its configuration within the cyber domain. "The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy."[207] Yet, monitoring the internet is crucial for global security.

When law enforcement agencies and government entities want to gather information about a crime, detect or prevent a crime, or investigate crimes, they use surveillance. In this regard, is also an instrument used in the cyber domain for the prevention and countering of digital crime like cyberterrorism.

> *[M]any criminal justice systems are currently better at responding to and punishing crimes after the fact than at preventing them in the first place. Often, existing criminal justice practices are ineffective when it comes to preventing*

[205] Manfred Nowak and Anne Charbord, *Using Human Rights to Counter Terrorism*, Elgar Studies in Human Rights, Edward Elgar Publishing, 2018.
[206] Ian Brown and Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology, Vol. 6, Issue 2, 2009, p. 123.
[207] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1999, p.1202.

> *terrorist conspiracies from achieving their aim. A forward-looking, preventive criminal justice strategy against terrorist violence requires a comprehensive system of substantive offences, investigative powers and techniques, evidentiary rules and international cooperation.*[208]

With the use of technologies, agencies have begun to rely on digital surveillance that can reach more effective proportions with less effort, such as tapping into the subject´s mobile phone and going through private information, emails, text messages, locations, pictures, etcetera. Such information is routinely collected during undercover surveillance. "The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observations of our selves possible."[209] It is relatively recent, however, that intelligence agencies can collect, store and analyse the majority of the world's communications.

Internet surveillance systems can be used for diverse purposes; they can assist in identifying emerging threats by applying scientific competences and computational linguistics to create algorithms that search for specific things through the use of massive datasets.[210] Those surveillance systems can, for example, alert and track emerging public health threats (Medical Information System[211]), revise news media sources around the world for emerging threats (Europe Media Monitor[212]) or to help maintain the sea secure and fight against piracy (Maritime surveillance[213]).

Digital surveillance can be performed by the collection of all the information an individual's activity creates online. A person's mobile phone connected to the internet has a Global Positioning System (GPS) that can locate where in the globe

---

[208] *Handbook on Criminal Justice Responses to Terrorism*, United Nations Office on Drugs and Crime, New York, 2009, p. 5.
[209] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, p.1202, 1999
[210] Internet Surveillance Systems, European Commission [website]. Available from: https://ec.europa.eu/jrc/en/research-topic/internet-surveillance-systems (accessed 28 July 2019).
[211] Medical Information System (MEDISYS). Available from: https://medisys.newsbrief.eu/medisys/homeedition/en/home.html (accessed 28 July 2019).
[212] See Europe Media Monitor. Available from: https://emm.newsbrief.eu/NewsBrief/clusteredition/en/latest.html (accessed 28 July 2019).
[213] See Maritime Surveillance, European Commission [website]. Available from: https://ec.europa.eu/jrc/en/research-topic/maritime-surveillance (accessed 28 July 2019).

you are at any time. Monitoring that information has the potential of interfere seriously with the right to privacy, as well as the rights to freedom of expression and association.

The need for security seems to be a self-evident truth. However, we must remember to set new rules to balance the need for security with the right to privacy. In an interview to the Information Security Media Group, a recognised French news source outlet, Europol Advisor Alan Woodward stated that already, "France has some of the most intrusive surveillance laws in the western world."[214]

Due to some of the recent terrorist attacks across Europe, member states have had a tendency to expand their surveillance powers with the excuse of preventive measures for future attacks. Former French Prime Minister Manuel Valls stated during his address to the National Assembly on 13 January 2015, to pay tribute to the 17 victims killed in the recent terrorist attacks, that the government would soon propose a new surveillance law designed to give the country´s intelligence services "all the legal means to accomplish their mission."[215] In my view, those demands for greater surveillance powers are a threat to human rights and especially the right to privacy. To compensate with public opinion, he also stated that, "An exceptional situation requires exceptional measures; But never exceptional measures that would undermine our core principals, laws and values."[216] History has taught us that legality is not a synonym of ethically. Changing the laws and making it legal for intelligence agencies to work their way around people´s privacy by making exceptions for human rights does not make it correct.

Increased attention from activists and human rights organisations has been focused on finding ways to counteract surveillance. In November 2014, Amnesty International, the Electronic Frontier Foundation and privacy investigators launched a tool designed to scan computers for traces of known surveillance spyware called *Detekt*.

---

[214] Mathew J. Schwartz, *Europe Seeks More Mass Surveillance: EU Politicians Demand More Monitoring, New Encryption Policies*, Information Security Media Group [website], 14 January 2015. Available from: http://www.bankinfosecurity.com/europe-seeks.more-mass-surveillance-a-7795 (accessed 25 July 2019).

[215] Sam Schechner and Jenny Gross, F*rance Pushes for Tighter Online Surveillance: Government Demands More Help from Tech Firms in Spotting Terrorist Communication Online*, The Wall Street Journal [website], 13 January 2015. Available from: http://www.wsj.com/articles/france-pushes-for-tighter-online-surveillance-1421186711 (accessed 24 July 2019).

[216] Sam Schechner and Jenny Gross, *France Pushes for Tighter Online Surveillance: Government Demands More Help From Tech Firms in Spotting Terrorist Communication Online*, The Wall Street Journal [website], 13 January 2015. Available from: http://www.wsj.com/articles/france-pushes-for-tighter-online-surveillance-1421186711 (accessed 24 July 2019).

The programme was able to detect at least *FinFisher*, a software known to be widely used by a number of governments around the world, including repressive regimes.[217] The idea behind this campaign was to create conscious of the normalised surveillance under which people are under and the importance of individual's privacy.

3.3.3 Data Retention and Intelligence-gathering

Hardly anyone sends a letter on paper anymore. Communication nowadays is reliant on technology. The practice of data retention involves the gathering and storing of communications data, or metadata, for extended periods of time for the purpose of future access. Metadata can tell the story about someone´s data and is able to uncover the who, when, what and how of a specific communication. Retaining data help solve or prevent a crime, but infringe into an individual's privacy by collecting information about him, in his everyday life.[218]

As cyberspace becomes the vehicle through which a person completes everyday tasks, it generates a great deal of personal information, that is recoded dutifully, and often invisibly, by computers that never stop. These can include each and every communication through any device that anyone could have had with friends, colleagues, organizations, and governmental agencies. They include interactions with businesses, financial institutions and political parties; every purchase, every transaction, every payment.[219]

Every single day, intelligence agencies collect details of thousands of our calls and messages in arrogant defiance of our courts. By invading our privacy

[217] European Parliamentary Research Service, *Mass Surveillance. Part 2 – Technology Foresight, options for longer- term security and privacy improvements*, European Parliament, p. 50. Available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf (accessed 30 July 2019).
[218] Privacy International, *A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJU'S Tele-2/Watson Judgement*, 2017. Available from: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf (accessed 20 July 2019).
[219] J. Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, p.1238, 1999.

> *they undermine our free press, our freedom of speech and our ability to explore new ideas. In a democratic society, no one is above the law- and that includes politicians in power. […] It´s time the Government stopped spying on innocent people and build a surveillance system that targets those who pose a genuine threat.*[220]

The practice of commanding the retention of communication data, or commonly known as metadata, by telecommunications companies, as prescribed by the laws of most EU member states, raises significant privacy, transparency and security concerns. Telecommunication companies and service providers are required by national laws to store large amounts of personal data on an ongoing basis for potential later access by government agencies and local authorities. Such storage and its access is regularly indiscriminate and fails to guarantee sufficient safeguards from abuse. In simple, there needs to be no real reason for the retention of personal data, no suspect of a crime, just the spying of innocent people. This is a clear infringement on the citizen´s right to privacy.

The potential dangers associated with data retention and access are significant. In a context where the gathering and exploitation of data by private companies becomes increasingly intrusive and regular, data retention poses serious risk to individual privacy and data security. The data opens the door for governments and third parties to make intimate interferences into individual's private life and to engage in profiling and other infringements. If individuals' data is not properly protected there is always a potential of unauthorized access to information by third parties, including cyber-criminals.[221]

The debate between privacy advocates and authorities in Europe centre the argument between what could be considered more important: privacy or security. According to David Anderson, an independent reviewer of terrorism legislation from Great Britain, argues in a report published in June 2015 that a) on the one side privacy

[220] Privacy International, Quoting Corey Stoughton, Advocacy Director at Liberty from, *A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJU'S Tele-2/Watson Judgement*, 2017. Available from: https://privacyinternational.org/press-release/2119/privacy-international-liberty-and-open-rights-group-joined-other-organisations (accessed 20 July 2019).

[221] Privacy International, *A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJU'S Tele-2/Watson Judgement*, 2017. Available from: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf (accessed 20 July 2019).

advocates emphasize the growing volume of electronic communications and the quality, as well as, extended techniques for the gathering that information and its analysis, as lives are progressively lived online. They campaign to reduce powers, or improved safeguards, to protect the individual from the spectre of a surveillance from the state. Also, b) authorities argue for greater support in the use of electronic communications that can have an open access, and fear the emergence of channels of communication that cannot be monitored. They also search to redress the balance in favour of the interests of national security for the prevention and detection of crime and terrorism.[222]

Current data retention regimes in Europe violate the right to privacy and other fundamental human rights, such as the freedom of speech and access to information. In particular, the Court of Justice of the European Union (CJEU) has made it particularly clear thru several court rulings[223] that general and indiscriminate retention of communications data is disproportionate and cannot be justified. The CJEU recognized that the data retention gives access to governments and third parties to make interferences about individuals, to engage in profiling and ultimately intrude on people´s lives.[224]

> *While one may voluntary divulge personal information in exchange for some goods or services, people remain largely uninformed about what happens to their information. The information becomes, quite literally, someone else's property, and is bought and sold without the individual's consent or awareness.* [225]

All EU member states are parties to the European Convention on Human Rights and Fundamental Freedoms and to the International Convention on Civil and Political Rights (ICCPR), both enshrining the right to privacy. Regional institutions like the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR) have developed human rights standards on data retention aiming to ensure that

[222] David Anderson Q.C., *A question of Trust: Report of the Investigatory Powers Review*, Williams Lea Group, London, June 2015, p.22. Available from: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

[223] For example the CJEU ruling in the Tele2/Watson Case (2016) or the Digital Rights Ireland Case (2014).

[224] CJEU ruling in the Tele2/Watson decision. (see supra note2, at para. 99).

[225] Debbie V.S. Kasper, *The Evolution (or Devolution) of Privacy*, Sociological Forum, Vol. 20, No. 1, March 2005, p. 89.

the individuals whose data is being retained are effectively empowered to protect themselves against all of the related risks.

Most countries in Europe treat separately the question of the retention of data and the actual access to the data for law enforcement or intelligence purposes. Both are, however, closely intertwined. Without proper safeguards, there is no way to guarantee that interference with fundamental rights is minimised at both phases: the retention and the access to the data. Lax legislations on data retention increase the chances of indiscriminate gathering, retaining and access to the information with an open door for abuse of power. In other words, vague rules on governmental access to retained data can lead to unlawful surveillance, including access to information of individuals who may not even be related to the subject of investigations (collateral data), misuse and other abuses of data protection standards, such as the sharing of personal data.

The protection of privacy represents a core human right for democracies obeying the rule of law. In the European Union, privacy is protected under the EU Charter of Fundamental Rights and Freedoms, in its article 7, respect for private and family life; and article 8, protection of personal data; as well as under the limitations and guarantees of article 52. The European Convention on Human Rights also recognises the right to a private and family life under article 8.

The Privacy and Electronic Communications Directive, also known as the e-Privacy Directive (ePD) (2002/58/EC), is a directive on data protection and privacy in the digital age. It deals with several important issues such as confidentiality of information, treatment of traffic data, spam and cookies. But more importantly, in article 15, states that:

> *Member States may […] adopt legislative measures providing for the retention of data for a limited period [where data retention constitutes] a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised*

use of the electronic communication system [and provided that the data retention measures are] in accordance with the general principles of Community law.[226]

The directive addresses member states to prohibit listening, tapping, storage or other sorts of interception and/or surveillance of communication and "related traffic", unless the users have previously given their consent or, as mentioned earlier, the conditions of article 15 have been met. The directive also obliges the providers of services to erase or anonymise the traffic data processed when it is no longer needed, unless, again, the conditions of article 15 have been fulfilled.

European Union member states have an obligation to ensure that their laws comply with the CJEU´s jurisprudence, and EU law more generally. However, very few Member States have actually annulled their pre-digital rights legislation and that practically no member state´ law currently comply with the Tele-2/Watson ruling. Very few governments have stepped up in pushing legal reforms.[227] In the Tele-2/Watson Case the CJEU not only confirmed the importance of its ruling in Digital Rights Ireland Case but expanded on that ruling, affirming positive requirements that national data retention legislation must fulfil in order to comply with both European and international human rights law.[228]

As mentioned earlier, even though all European Union member states share common values and interests, and are bound by regional obligations, security issues mostly fall under national jurisdiction, especially when dealing with terrorism. In this case the right to privacy is heavily challenged by State surveillance in the form of data retention with the justification of security.

[226] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 in relation to the processing of personal data and the protection of privacy in the electronic communications sector (Directive on private and electronic communications), OJ L 201, p. 37 -47, Article 15(1), 31 July 2002.
[227] See e.g. Austria, Belgium, Luxembourg, The Netherlands, Slovenia, Slovakia.
[228] David Anderson Q.C., *A question of Trust: Report of the Investigatory Powers Review*, Williams Lea Group, London, June 2015, available from: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

3.3.4 Public – Private Cooperation and Partnerships

Cyber security has become a challenging issue in recent years. There are many benefits from establishing public- private partnerships in countering cyberterrorism. First, the fight against cyberterrorism requires strong cooperation from all stakeholders; national authorities, public and private sectors. The Internet is not a complete public space, nor is it all private. However, most of the physical part of the internet such as computers, wires, servers, etcetera, are privately produced, sold and owned. Most of networks and information systems around the world are also privately operated. Therefore, a close relation between the public and private sectors is essential.[229]

It is also crucial that both spheres be involved in meaningful policy shaping. Most of the times, these "[p]artnerships are mostly used for facilitating the exchange of information on threats and trends, but also for prevention activities, and action in specific cases."[230] Legislation needs to clearly define the responsibilities, limitations of powers and the extent of human rights in respect of privacy and data protection, in the context of investigatory procedures. A balance must be achieved between the interests of investigating crime, by ensuring public safety, and citizens' rights of privacy and data protection.

Critical infrastructure represents a big security concern for sates. An attack on Cis could greatly effect the security of the state of possibly the region. Also, even though the protection of critical infrastructure falls under national competence for most countries, the majority of critical infrastructure is privately owned.

An important tool for cooperation is the EU Internet Forum. It facilitates dialogue between the Commission and tech companies to develop a safer web, both by disrupting terrorists content (Europol) and by amplifying counter terrorist narratives (CSEP).

---

[229] Madeline Carr, Public- private partnership in national cyber- security strategies, Chatham House The Royal Institute for International Affairs, Vol 92, No. 1, 8 January 2016, p. 43.

[230] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations Publications, New York, February 2013, p. xxvii. Available from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 1 august 2019).

In 2015, the European Commission created the Internet Forum in an attempt to stop the abuse of the internet by international terrorist groups. The forum acts as a platform between industry and EU, but is careful to retain focus on working with smaller internet companies that do not have the resources as the largest companies in the online social media market to prevent abuse of their platforms. The forum has two approaches: 1) it aims to reduce the amount of content available on the internet, for which it partners with Europol and the Internet Referral Unit. And 2) it empowers civil society through the Civil Society Empowerment Programme (CSEP), an initiative under the umbrella of EU internet Forum, launched in 2015. The EU also facilitates a network of frontline practitioners – the Radicalization Awareness Network (RAN), which provide analysis of existing counter terrorist efforts.

An example of cooperation is when a number of private actors have engaged in strategic communications to counter terrorism in their platform. Internet 'gatekeepers' have been accused by policy makers of facilitating terrorist narratives on their sites and have developed a number of responses. An example is the GIFTC, launched in July 2017 by Facebook, Twitter, YouTube and Microsoft[231], with the aim of making their service hostile to terrorists. The GIFTC is part of a wider initiative in partnership with the UN CTED and Tech Against Terrorism, a Swiss Foundation, whose members include a number of communication companies. The aim of the project is to provide operational support to other smaller companies, to prevent their communication technology from being exploited by terrorists.

[231] Nicholas Watt and Patrick Wintour, Facebook and Twitter have 'social responsibility' to help fight against terrorism, says David Cameron," The Guardian, 16 January 2015, Available from: https://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat (accessed 4 august 2019). See also, Richard Ford, Hole Secretary Amber Rudd will tell web giants to fight terrorism," The Times [website], 1 August 2017. Available from: https://www.thetimes.co.uk/article/home-secretary-amber-rudd-will-tell-web-giants-to-fight-terrorism-dgbhd0zg0 (accessed 4 august 2019).

4. Policy and Legislative Framework

There are three main institutions involved in EU legislation: 1) the European Parliament, which represents the citizens; 2) the Council of the European Union, which represents the governments of the individual member States; and 3) the European Commission, which represents the interests of the Union as a whole.[232] The European Council, on the other hand, is composed of the heads of governments of the members, and sets the EU´s political direction, but has no powers to pass laws.[233]

As part of the EU Cybersecurity Strategy[234] implemented in 2013 to combat cybercrime, including cyberterrorism, the EU has adopted legislation and supported operational cooperation. By creating a common legislative framework, standards are introduced that make sure all measures taken by member States to fight terrorism must respect human rights and the principle of the rule of law, while excluding any form of arbitrariness, as well as any discriminatory or racist treatment, and must be subject to appropriate supervision. [235]

The policy consequence is that rather than technology, it is the legal framework, authorities and accountability that should be regulated. This balance requires a solid political discussion on what is reasonable from a law enforcement perspective in comparison to privacy and protection against other cyber threats. Without a conclusive discussion it will remain a cat-and-mouse from a technology perspective.[236]

---

[232] *Institutions and bodies*, European Union [website]. Available from: http://europa.eu/european-union/about-eu/institutions-bodies_en (accessed 27 July 2019).
[233] See *European Council*, European Union [website]. Available from: http://europa.eu/european-union/about-eu/institutions-bodies/european-council_en (accessed 27 July 2019).
[234] See *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, High Representative of the European Union for Foreign Affairs and Security Policy, European Commission, Brussels, 7 February 2013.
[235] See the Guidelines on human rights and the fight against terrorism, adopted by the Committee of Ministers of the Council of Europe on 11 July 2002, II.
[236] European Parliamentary Research Service, *Mass Surveillance. Part 2 – Technology Foresight, options for longer- term security and privacy improvements*, European Parliament, p. 51. Available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf (accessed 30 July 2019).

5. Conclusions

Aiming to provide for an understanding of the extent to which the implementation of surveillance programmes to counter cyberterrorism in the European Union without infringing the right to privacy, the Master Thesis at hand presented a multi-dimensional contrasting outcome.

Although the notion of privacy has many layers and its definition can vary, it is essential for human development. It creates barriers and manages boundaries to protect individuals from unwarranted interferences in their lives. It relates to the protection of the private life and extends this concept into the digital cyberspace. Nonetheless, the right to privacy is a fundamental human right. It is legally well represented across international law and many European Union legal instruments. However, it is a right that can be limited when other rights are under threat such as the right to security.

The right to security is a crucial. Without security, other rights cannot be guaranteed. Security links with other human rights such as freedom of expression, association and even life. Human rights cannot be treated in isolation; they are dependent on one another. States must do everything in their power to protect peace and national security.

The frontline against terrorism is increasingly in the cyberspace. Terrorist can exploit social media, encrypted communications, spread propaganda, recruit new followers and coordinate attacks. The internet has transformed virtually every aspect of life. Its communication capabilities promote freedom of expression and information. Dependency in the cyberspace is unprecedented. People increasingly speak, listen and act through cyberspace.

Part of my research intended to discover how much freedom and privacy must be sacrificed in the quest for security. There is a strong factor of subjectivity in the evaluation of proportionality of restrictions to the right to privacy when dealing with the collective right to national security.

Proportionality is a well-established principle in the legal order of the EU that allows for limitations in the exercise for fundamental rights if they are provided by law

and respect the core of those rights.While human rights covenants recognize national security and public order as legitimate aims for restricting freedoms (privacy, expression, association), the Human Rights Council has stressed the need to ensure that invocation of national security, including counter-terrorism, is not used unjustifiably or arbitrarily.[237]

Even though cyberterrorism is a specific new form of terrorism, terrorist acts, in whatever form, are a public emergency and represent an exceptional circumstance, that threatens the life of any nation and does require exigencies to prevent or contain it. Therefore, states feel obliged to take the most drastic actions, including derogating the usual human rights obligations applicable in 'ordinary' times. However, a crucial argument is that, although acts of terrorism, may be time- limited to the act itself, cyberterrorism is not a passing phenomenon and the anti- terrorism legislations tend to become semi- permanent.

Law enforcement and intelligence agencies are increasingly using sophisticated computer systems to carry out mass surveillance. Through the use of different surveillance techniques it is possible to identify individuals. Combating cyberterrorism through indiscriminate massive surveillance dehumanises people and places them not as individuals, but as items of a database. A police database represents people, not as common users of the cyber space, but as suspects or victims.

Various EU institutions such as Europol play a significant role in identifying and removing illegal terrorist content from the internet by monitoring content online. It can be argued that in order to detect and remove terrorist material, mass surveillance is conducted. While the EU Internet Forum provides a platform amplify counter- narratives on the web.

The cost of applying cyberterrorism measures to the internet should be considered when such measures can give governments and intelligence agencies the opportunity to violate human rights with little public accountability tools that can limit the free flow of information, and restrict freedom of expression, infringe in private life and diminished liberties the same way terrorism would.

[237] A/HRC/RES/7/36.

There are several functioning but rather differentiated legal frameworks on counter- terrorism. Due to the complexity of the EU and the different levels of priorities and cyber maturity, EU member states have different stands in regard to cyber security advancements. Legislation must clearly define the responsibilities, limitations of powers and the extent of human rights in respect of privacy and data protection, in the context of investigatory procedures. A balance must be achieved between the interests of investigating crime, by ensuring public safety, and citizens' rights to privacy and data protection. In this regard, states have a wide variety of development levels, with different threats, priorities and capabilities. However, it is a fact that with the increasing dependency of information technologies, online privacy and data protection have become an online challenge and a cause for major political concern.

Technological developments have created societies that are extremely dependant to computer systems. Information technologies have taken control over the administration of important social infrastructures. As a result, the threat of cyberterrorism has become more frequent. There are many speculations of how terrorists or terrorists groups might be able to cause harm to society´s infrastructures and its people, by attacking systems and networks. Hence, States are responsible for their own cyber-capacities, and security. Also, countries rely on and domestic policies, international agreements, military structures and the legal and budgetary capabilities to develop their own cyber-capacities.

Computer networks are global and interconnected with computers all over the world. The cyber space is borderless and is often unclear which country is being used to store or transfer relevant data. A single attack in one country can affect millions of computer systems in other countries. Even in data exchange processes between two computers in a single country, the information may pass through to one or more countries, even if no direct connection is available.

The internet has been designed to resist external influence, giving it a sort of life of its own. Therefore, it has no central integrated into its network architecture, as a safe mechanism to protect it from an attack to the functioning of the entire network. Consequently, it is difficult to control illegal network operations and to identify offenders who use the internet to commit crimes.

Despite the many technology options, there is no single technological solution to help citizens better manage their privacy risks when it comes to mass surveillance and other threats against their privacy. Work needs to be done on a regulating a common framework that includes governments, private companies and civil society. There are many ways to approach terrorism, but the respect for human rights in any effective counter-terrorism strategy is essential and states must uphold their international agreements and obligations. All member states are bound by EU regulations, regardless of their advancement in online security.

An important accomplishment for preventing and countering cyberterrorism is the EU Cyber Security strategy presented by the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy. Its declaration acknowledging that the EU´s core values applied as much in the digital as in the physical world will serve as a great tool to criminalize acts terrorism in the internet. Which means that the same laws and norms that apply in other areas of our everyday lives, also apply in the cyber domain. [238] Also, the strategy recognises the role of the private sector in the significant partial ownership and operation of cyberspace and calls for national governments to safeguard the access and openness of the internet while respecting fundamental rights online.[239] Most network and information systems are privately operated; therefore, cooperation between the public and private sectors is essential.

Another important aspect that I would like to include is the fact that most people use of their mobile phones, computers and gadgets, which are active online and always present in the cyberspace, and thus, not fully aware that every online activities they make is possibly being monitored, stored and shared. Also, a considerable number of computer users are unaware that their computers may be targeted by hackers or used as remote weapon by terrorists. Raising awareness on these two topics would certainly help protect human rights and improve online safety.

To conclude, the proportionality of Internet surveillance touches on fundamental values of any democratic society, raising serious questions for EU policies. Protecting the

[238] *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*, European Commission and High Representative of the EU for Foreign Affairs and Security Policy, Brussels, 7 February 2013, para. 2.
[239] Ibid, p.2.

right to privacy is not an obstacle to combating terrorism. Terrorism if fundamentally the denial and destruction of human rights. A human rights-based approach is essential when preventing and combating all forms of terrorism. A state's lack of respect for human rights not only hinders its current fight and perpetuates the problem.

References

Books and e-books:

Anderson Q.C., David, *A question of Trust: Report of the Investigatory Powers Review*, Williams Lea Group, London, June 2015, available from: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

Angwing, Julia, *Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance*, San Martin´s Griffin, 2015.

Akhgar, Babak and Ben Brewster, *Combating Cybercrime and Cyberterrorism: Challenges, trends and priorities*, Advanced Sciences and Technologies for Security Applications, Springer, Switzerland, 2016.

Council of Europe, *Organised Crime Situation Report 2004. Focus on the threat of cybercrime*, Strasbourg, 23 December 2004, available from: https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf (accessed 16 July 2019).

Holmes, D. ed., *Virtual Politics: Identity and Community in Cyberspace*, Sage Publications, London, 1997.

Janelle, D. G., and Hodge, D. C., eds., *Information, Places and Cyberspace: Issues in Accessibility*, Springer, New York, 2000.

Kolko, B. E., Nakamura, L., Rodman, G.B., eds., *Race in Cyberspace*, Routledge, New York and London, 2000.

Last, Mark, and Abraham Kandel, eds., *Web Intelligence and Security: Advances in Data and Text Mining Techniques for Detecting and Preventing Terrorist Activities on the Web*, IOS Press, The Netherlands, November 2009.

Lyon, David, *Surveillance after Snowden*, Polity Press, Cambridge, 2015.

Lyon, David ed., *Surveillance as a Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London and New York, 2003.

McCormick, John, *Understanding the European Union: A concise Introduction*, 7th Edition, Palgrave, London, 2017.

Nowak, Manfred, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, N.P. Engel, 2005.

Nowak, Manfred and Anne Charbord, *Using Human Rights to Counter Terrorism*, Elgar Studies in Human Rights, Edward Elgar Publishing, 2018.

Office of the United Nations High Commissioner for Human Rights, *Frequently asked questions on a human rights- based approach to development cooperation,* United Nations Publication, New York and Geneva, 2006, available from: https://www.ohchr.org/Documents/Publications/FAQen.pdf (accessed 31 July 2019).

Rengel, Alexandra, *Privacy in the 21st Century*, Martinus Nijhoff Publishers, Leiden, The Netherlands, 2013.

Schoeman, Ferdinand D., *Privacy and Social Freedom*, Cambridge University Press, Cambridge, 1992.

Sieber, Ulrich and P. Brunst, *Cyberterrorism and other use of internet for terrorist purposes: Threat Analysis and Evaluation of International Conventions*, Council of Europe Publishing, Strasbourg, 2007

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations Publications, New York, February 2013, available from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 1 august 2019).

United Nations Office on Drugs and Crime, *Handbook on Criminal Justice Responses to Terrorism*, United Nations Publications, New York, 2009.

United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, United Nations Publications, New York, 2012.

United Nations Office on Drugs and Crime, *Human Rights and Criminal Justice Response to Terrorism*, United Nations Publications, New York, November 2014.

United Nations Office on Drugs and Crime, *Universal Legal Framework against Terrorism*, United Nations Publications, Vienna, October 2017.

Weimann, Gabriel, *Terror on the Internet: The New Arena, the New Challenges*, United States Institute of Peace Press, Washington, D.C., 2006

Official Publications:

Aoláin, Fionnuala Ní, *Remarks on promotion and protection of human rights at the Third Committee*, 23rd meeting – General Assembly, 72nd Session, New York, 18 October 2017, available from: http://webtv.un.org/topics-issues/non-governmental-organizations/action-internationale-pour-la-paix-et-le-d%C3%A9veloppement-dans-la-r%C3%A9gion-des-grands-lacs/watch/fionnuala-n%C3%AD-aol%C3%A1in-special-rapporteur-on-promotion-and-protection-of-human-rights-at-the-third-committee-23rd-

meeting-general-assembly-72nd-session/5613073854001/?term=&page=6&sort=date (accessed 30 June 2019).

Aoláin, Fionnuala Ní, *Press Conference on the Preliminary findings of the visit to Belgium*, Brussels, 31 May 2018, available from: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23164&LangID=E (accessed 30 June 2019).

Bier, William C. ed., *Privacy: A vanishing value?*, Fordham University Press, New York, 1980.

Cannataci, J., B., Zhao, G. Torres Vives, S. Monteleone, et al., *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*, UNESCO, Paris, 2016.

Council of the European Union, *Cyber-attacks: Council is now able to impose sanctions*, Press Release [website], 15 May 2019, available from: http://www.consilium.europa.eu/en/press-release/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ (accessed 28 July 2019).

Common Security and Defence Policy, *CSDO structure, instruments, and agencies*, European Union [website], 08 July 2016, available from: http://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/csdp-structure-instuments-and-agencies_en (accessed 28 July 2019).

Electronic Privacy Information Center, *EU Privacy and Electronic Communications (ePrivacy Directive*) [website], available from: https://epic.org/international/eu_privacy_and_electronic_comm.html (accessed 29 July 2019).

European Commission, *Digital privacy*, Digital Single Market Policy [website], 27 June 2019, available from: https://ec.europa.eu/digital-single-market/en/online-privacy (accessed 28 July 2019).

European Commission, *EU Internet Forum: Civil Society empowerment programme* [website], 2017, available from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en (accessed 4 July 2019).

European Commission, *Critical infrastructure*, Migration and Home Affairs [website], available from: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (accessed 7 July 2019).

European Commission, *Cutting-edge facial recognition goes mainstream* [website], 11 March 2015, available from: https://cordis.europa.eu/project/rcn/108790/brief/en (accessed 27 July 2019).

European Commission, *EU Internet Forum: Progress on removal of terrorist content online* [website], San Francisco, 10 March 2017, available from: http://europa.eu/rapid/press-release_IP-17-544_en.htm (accessed 4 July 2019).

European Commission, *proposal for a regulation of the European parliament and of the council on preventing the dissemination of terrorist content online*, Brussels, 12 September 2018, available from: https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 29 July 2019).

European Commission, *State of the Union 2018: Commission proposes new rules to get terrorist content off the web*, Strasbourg, 12 September 2018, available from: http://europa.eu/rapid/press-release_IP-18-5561_en.htm (accessed 1 July 2019).

European Court of Human Rights, *Derogation in Time of Emergency*, Press Unit, available from: https://echr.coe.int/Documents/FS_Derogation_ENG.PDF (accessed 29 July 2019).

European Parliamentary Research Service, *Briefing: Cyber security in the European Union* [website], 2013, available from: http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf (accessed 12 June 2019).

European Parliamentary Research Service, *Briefing: Cyber security in the European Union*, European Parliament, 2001, available from: http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf

European Parliamentary Research Service, *Mass Surveillance. Part 2 – Technology Foresight, options for longer- term security and privacy improvements*, European Parliament, available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf (accessed 30 July 2019).

European Union, *Foreign and Security Policy* [website], available from: http://europa.eu/european-union/topics/foreign-security-policy_en (accessed 27 July 2019).

European Union, *Living in the EU* [website], available from: http://www.europa.eu/european-union/about-eu/figures/livig_eu (accessed 26 July 2019).

European Union Agency for Fundamental Rights, *Data Retention across the EU*, 2017, available from: https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention (accessed 29 May 2019).

European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, 2017.

European Union Agency for Law enforcement Training, *Cyber-terrorism: A treat for the European Union and its response*, WEBINAR [website], DIC. 65/2018, 2018, available from: https://www.cepol.europa.eu/education-training/what-we-teach/webinars/webinar-652018-cyber-–-terrorism-threat-european-union-its (accessed 17 July 2019).

European Union External Action, *The European Union and the United Nations strengthening partnership on counter-terrorism* [website], New York, 24 April 2019, available from: http://eeas.europa.eu/headqarters-homepage/61409/european-union-and-united-nations-strengthen-partnership-counter-terrorism_en (accessed 23 July 2019).

Global Network Initiative, *GNI Statement on Europe´s proposed regulation on preventing the dissemination of terrorist content online*, 15 January 2019, available from: https://globalnetworkinitiative.org/wp-content/uploads/2019/01/GNI-Statement-Proposed-EU-Regulation-on-Terrorist-Content.pdf (accessed 29 June 2019).

Mendel, T, A. Puddephatt, B. Wagner, et al, *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris, 2012.

European Commission, Migration and Home Affairs, *European Agenda on Security*, [website], available from: http://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (accessed 28 July 2019).

Nijhoff, Martinus, *Collected Edition of the ´Travaux Préparatoires' of the European Convention on Human Rights*, Council of Europe, Vol. V, The Hague, 1979.

Office of the United Nations High Commissioner for Human Rights. Human Rights, Terrorism and Counter- Terrorism. *Fact Sheet No. 32*, available from: http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf (accessed 20 February 2019).

O´Dea, S., *Internet Usage in Europe- Statistics & Facts*, Statista [website], 20 May 2019, available from: https://www.statista.com/topics/3853/internet-usage-in-europe/ (accessed 25 June 2019).

O´Flaherty, Michael, *Report: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, European Union Agency for Fundamental Rights, 2007.

Privacy International, *A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJU'S Tele-2/Watson Judgement*, 2017,

available from: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf (accessed 20 July 2019).

Privacy International, *What is privacy?* [website], available from: https://privacyinternational.org/explainer/56/what-privacy (accessed 1 July 2019).

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Humans Rights Council, 2009, available from: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed 23 June 2019).

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations, September 2014, doc. No. A/69/39723.

Emerson, Ben (Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), *Speech during the presentation of his report to the UN General Assembly on the use of mass digital surveillance for counter-terrorism purposes, and the implications of bulk access technologies for the right to privacy*, New York, 23 October 2014, available from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200 (accessed 30 July 2019).

Scheinin, Martin, *2010 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, (A/HRC/16/51/Add.1), 14 February 2010, available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/107/07/PDF/G1110707.pdf?OpenElement (accessed 27 June 2019).

Theohary, Catherine A. and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*, Congressional Research Service, Washington D.C., 27 March 2015, No. of doc. R43955, available from: https://digital.library.unt.edu/ark:/67531/metadc810730/citation/#top (accessed 29 July 2019).

United Nations Human Rights Office of the High Commissioner [website], available from: https://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx (accessed 20 June 2019).

United Nations Office on Drugs and Crime, *E4J University Module Series: Counter-Terrorism*, July 2018, available from: https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html (accessed 30 July 2019).

United Nations Office on Drugs and Crime, *Surveillance and interception of communication* [website], available from:

https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/surveillance-and-interception.html (accessed 27 April 2019).

NEC Corporation, *What constitutes a cyberattack?*[website], available from: https://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html (accessed 19 July 2019).

Legal texts:

Treaties United Nations:

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) No. 999 UNTS 17.

International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 Mat 2001) No. 37517.

International Convention for the Suppression of Acts of Nuclear Terrorism (adopted 13 April 2005).

Special Tribunal for Lebanon, Major rulings issued by the Special Tribunal for Lebanon, Leidschendam, The Netherlands, 2001, available from: https://www.stl-tsl.org/sites/default/files/documents/legal-documents/stl-casebooks/STL_Casebook_201_EN.pdf (accessed 31 July 2019).

Universal Declaration of Human Rights (adopted 10 December 1948).

Resolutions of the United Nations:

United Nations General Assembly, *Universal Declaration of Human Rights, Resolution* 217, 10 December 1948.

United Nations General Assembly, *Measures to eliminate international terrorism*, Resolution A/RES/49/60, 17 February 1995, available from: https://undocs.org/en/A/RES/49/60 (accessed 31 July 2019).

United Nations General Assembly, *The United Nations Global Counter- Terrorism Strategy*, Resolution 60/288, 20 September 2006.

United Nations General Assembly, *Protecting Human Rights and Fundamental Freedoms while countering terrorism*, Resolution 64/168, 22 January 2010.

United Nations General Assembly, *The United Nations Global Counter- Terrorism Strategy Review*, Resolution A/RES/66/282Sixty-sixth session, 12 July 2012.

United Nations General Assembly, *Plan of Action to prevent Violent Extremism,* Resolution A/70/674, Seventieth session, Agenda items 16 and 117, 24 December 2015.

United Nations General Assembly, *Promotion and protection of human rights and fundamental freedoms while countering terrorism,* A/72/43280, 27 September 2017, available from: https://www.ohchr.org/Documents/Issues/Terrorism/A_72_43280_EN.pdf

United Nations General Assembly, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, Human Rights Council, A/HRC/16/51/Add.1, 14 February 2010.

United Nations Security Council, Threats to international peace and security caused by terrorist acts, *Resolution S/RES/2322*, 12 December 2016.

United Nations Security Council, *Threats to international peace and security caused by terrorist acts, Resolution 1566*, 2004.

United Nations Security Council resolution, S/RES/1267 (1999).

United Nations Security Council resolution, S/RES/1373 (2001).

United Nations Security Council resolution, S/RES/1540 (2004).

United Nations Security Council resolution, S/RES/1624 (2005).

United Nations Security Council resolution, S/RES/2178 (2014).

United Nations Security Council resolution, S/RES/2322 (2016).

United Nations Security Council resolution, S/RES/2396 (2017).

European Union Instruments

Charter of the Fundamental Rights of the European

Council of the European Union, *Convention on the Prevention of Terrorism*, Warsaw, 2005.

EU Cyber Defence Policy Framework (2018 update), Council of the European Union, Brussels, 19 November 2018, No. of Doc. 14413/19.

Council of the European Union, *The European Union Counter- Terrorism Strategy*, Brussels, 30 November 2005, No. of doc. 14469/4/05 REV 4.

Council of the European Union, *Council Framework Decision on combating terrorism*, 13 June 2002, available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN (accessed 30 July 2019).

Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace, European Commission and High Representative of the EU for Foreign Affairs and Security Policy, Brussels, 7 February 2013.

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption, 9916/17, Council of the European Union, Brussels, 7 June 2017.

Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, High Representative of the European Union for Foreign Affairs and Security Policy, European Commission, Brussels, 7 February 2013, available from: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 18 April 2019).

Framework on counter- terrorism between the United Nations and the European Union, Brussels, 24 April 2019, available from: https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf (accessed 31 July 2019).

Guidelines on human rights and the fight against terrorism, Committee of Ministers of the Council of Europe, 11 July 2002, II.

Guidelines on the Protection of Victims of terrorist acts, Committee of Ministers of the Council of Europe, 19 May 2017.

Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 17 April 2019, available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC (accessed 1 August 2019).

Resolutions:

Directive (EU) 20161148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union. The European Parliament and the Council of the European Union, Official Journal of the European Union, 6 July 2016.

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and electronic communications), 12 July 2002.

Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25 October 1995.

Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 15 March 2017.

Directive 2004/80/EC, relating to compensation to crime victims, 29 April 2004, available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004L0080&from=EN (accessed 29 July 2019).

Journal Articles:

Brown, Ian, and Douwe Kroff, *Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology, Vol. 6, Issue 2, 2009, p. 119- 134.

Bryant, R., *What kind of Space is Cyberspace*?, Minerva- An Internet Journal of Philosophy Vol. 5, 2001, p. 138- 155, available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.125.5433&rep=rep1&type=pdf (accessed 31 July 2019).

Bruce G., *Definition of Terrorism- Social and Political Effects*, Review article, Volume article, No.2, 2018.

Carr, M., *Public- private partnership in national cyber- security strategies*, International Affairs, Vol. 92, 2016, p. 43- 62.

Denning, D. E., *Cybersecurity´s Next Phase: Cyber Deterrence*, The Conversation, Scientific American [website], 13 December 2016, available from: https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090 (accessed 2 July 2019).

Cohen, Julie E., *What Privacy is for*, Harvard Law Review, Vol. 126, 2013, p. 1904-1933.

Denning, D. E., *Cybersecurity´s Next Phase: Cyber Deterrence*, Scientific American [website], 13 December 2016, available from: https://www.scientificamerican.com/article/cybersecuritys-next-phase-cyber-deterrence/# (accessed 27 July 2019).

Denning, D. E., *Is cyber terror next?* (essay), Social Science Research Council [website], New York,1 November 2001, available from: http://essays.ssrc.org/sept11/essays/denning.htm (accessed 6 July 2019).

Diggelman, Oliver and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, Human Rights Law Review, Volume 14, Issue 3, Oxford University Press, p. 4439-450, September 2014.

Flynn, E.J., *Counter- terrorism and Human Rights: the view from the United Nations*, European Human Rights Law Review, No. 1, 2005.

Friedrichs, J., *Defining the International Public Enemy: The political struggle behind the legal debate on international terrorism*, Leiden Journal of International Law, Vol. 19, 2006.

Gandhi, R., Sharma, A., Manhoney, W., Sousan, W., Zhu, Q., Laplante, P., *Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Politica*l, IEEE Technology and Society Magazine, Vol. 30, Issue 1, Spring 2011, 7 March 2011, p.28- 38, available from: https://ieeexplore.ieee.org/document/5725605/authors#authors (accessed 2 august 2019).

Greene, A., *Defining terrorism: One size fits all?*, International and Comparative Law Quarterly, Cambridge University Press, Vol. 66, Issue 2, 20 February 2017, p. 411- 440, available from: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/defining-terrorism-one-size-fits-all/0E707CD33E7F656573C777BE23C27168/core-reader# (accessed 27 May 2019).

Kang, J., *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Vol. 50, 1998, p. 1193- 1287.

Kasper, D. V. S., *The Evolution (or Devolution) of Privacy*, Sociological Forum, Vol. 20, No. 1, March 2005, p. 69- 100, available from: https://www.academia.edu/4641837/The_Evolution_or_Devolution_of_Privacy (accessed 27 July 2019).

Kielsgard, Mark D., A human Rights Approach to Counter- Terrorism, California Western International Law Journal, Vol. 36, article 2, p. 249- 302, available from: https://scholarlycommons.law.cwsl.edu/cwilj/vol36/iss2/2 (accessed 12 June 2019).

Lewis, James A. and Katrina Timlin, *Cybersecurity and Cyberwarfare*, Centre for Strategic and International Studies, Washington, D.C., 2011, available from: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (accessed 29 July 2019).

Lyon, D., *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*, Big Data & Society, SAGE, July- December 2014, p. 1- 18, available from: https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861 (accessed 2 August 2019).

Mills, J. E. and Sookeun Byun, *Cybercrimes against Consumers: Could Biometric Technology Be the Solution?, IEEE Internet Computing,* , vol. 10, no. 4, July-Aug 2006, p. 64-71.

Oleksiewicz, Isabela, *Challenges of EU Security on the example of cyberterrorism policy*, Journal of International Trade, Logistics and Law, Vol. 1, Num. 1, 2015, P. 25-30.

Prins, C., *Property and Privacy: European Perspectives and the Commodification of Our Identity*, Information Law Series, Vol. 16, September 2006, p. 223- 257, available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=929668 (accessed 1 august 2019).

Riedel B., The Grave New World: Terrorism in the 21st Century, Brokings [website], 9 December 2011, available from: https//www.brookings.edu/articles/the-grave-new-world-terrorism-in-the-21st-century/ (accessed 18 July 2019).

Roser, M., Nagdy, M. and Ritchie H., *Terrorism: our world in data* [website], available from: https://ourworldindata.org/terrorism (accessed 18 May 2019).

Sieber, Ulrich, *International cooperation against terrorist use of the internet*, Revue internationale de droit penal, Vol. 77, no. 3, 2006, p. 395-449, available from: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm (accessed 27 June 2019).

Sofaer, Abraham D., Gregory D. Grove and Gorge D. Willson, *A proposal for an International Convention To Enhance Protection from Cybercrime and Terrorism*, The Information Warfare Site, 2001, available from: http://iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm (accessed 15 July 2019).

Sofaer, A. D. and Seymour E. Goodman, *A Proposal for an International Convention on Cyber Crime and Terrorism*, Center for International Security and Cooperation, Stanford, August 200, available from: https://cisac.fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a (accessed 28 July 2019).

Tsoukalas, Ioannis A. and Panagiotis D. Siozos, Privacy and Anonymity in the Information Society – Challenges for the European Union, The Scientific World Journal, 1 March 2011, Vol. 11, P. 458 – 462.

Vogel, J., *Towards a Global Convention against Cybercrime*, First World Conference of Penal Law, Penal Law in the XXI Century, 18- 23 November 2007, Guadalajara, Mexico, p. 1- 10, available from: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf (accessed 31 July 2019).

Online Newspapers Articles:

About cookies, BBC [website], 10 October 2012, available from: http://www.bbc.co.uk/webwise/guides/about-cookies (accessed 31 July 2019).

Global nuclear facilities 'at risk' of cyber attack, BBC News [website], 5 October 2015, available from: https://www.bbc.com/news/technology-34423419 (accessed 27 July 2019).

Harpaz, J., *The Internet: A Commodity or Utility?*, Forbes [website], 2015, available from: https://www.forbes.com/sites/joeharpaz/2015/01/27/the-internet-commodity-or-utility/#414e998e6eff (accessed 20 March 2019).

Jacob, Maxime, *Facial recognition gains grounds in Europe, among big-brother fears*, Euractiv Network France, 20 October 2017, available from: https://www.euractiv.com/section/data-protection/news/facial-recognition-gains-grounds-in-europe-among-big-brother-fears/ (accessed 27 July 2019).

Kalyanpur, Nikhil and Abraham Newman, *Today, a new EU law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened*, The Washington Post [website], 25 May 2018, available from: https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/?noredirect=on&utm_term=.2744a04e52b3 (accessed 20 June 2019).

Oriti, T., *Cyberterrorists targeting healthcare systems*, critical infrastructure, ABC News [website], 23 October 2017, available from: https://www.abc.net.au/news/2017-

10-23/forget-explosives,-terrorists-are-coming-after-cyber-systems/9076786 (accessed 27 July 2019)

MacAskill, Ewen and Gabriel Dance, *NSA Files: Decoded/ Edward Snowden's surveillance revelations explained*, The Guardian [website], 1 November 2013, available from: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (accessed 28 July 2019).

Murphy, K., *Web Photos that Reveal Secrets, Like Where You Live*, New York Times, August 11, 2010, available from: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (accessed 28 June 2017).

NSA tapped German Chancellery for decades, WikiLeaks claims, The Guardian [website], Berlin, 8 July 2015, available from: https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel (accessed 29 July 2019).

Schechner, Sam and Jenny Gross, F*rance Pushes for Tighter Online Surveillance: Government Demands More Help from Tech Firms in Spotting Terrorist Communication Online*, The Wall Street Journal [website], 13 January 2015, available from: http://www.wsj.com/articles/france-pushes-for-tighter-online-surveillance-1421186711 (accessed 24 July 2019).

Schwartz, Mathew J., *Europe Seeks More Mass Surveillance: EU Politicians Demand More Monitoring, New Encryption Policies*, Information Security Media Group [website], 14 January 2015, available from: http://www.bankinfosecurity.com/europe-seeks.more-mass-surveillance-a-7795 (accessed 25 July 2019).

Snowden NSA: Germany drops Merkel phone- tapping probe, BBC News [website], London, 12 June 2015, available from: https://www.bbc.com/news/world-europe-33106044 (accessed 29 July 2019).

Thesis

Adkins, Gary, *Utilizing Cyber Espionage to Combat Terrorism*, Master Thesis. Intelligence and National Security Study Program, The University of Texas at El Paso, 2013, available from: https://academics.utep.edu/Portals/4302/Student%20research/Theses/Utilizing%20Cyber%20Espionage%20to%20Combat%20Terrorism%20(Adkins).pdf (accessed 29 may 2019).

Other

"terrorist", English Oxford Dictionary [website], available from: https://www.lexico.com/en/definition/terrorism (accessed 25 Junes 2019).

"Surveillance", Cambridge Dictionary, Cambridge University Press [website], 2019, available from: http://dictionary.cambridge.org/dictionary/eglish/surveillance (accessed 22 July 2019).

All about cookies, All about cookies.org [website], available from: https://www.allaboutcookies.org/cookies/ (accessed 31 July 2019)