Department of Political Sciences

Master degree in International Relations – Global Studies

Master Thesis in Comparative Public Law

The Law of the Cyberspace: A First Comparative Inquiry

Supervisor

Prof. Cristina Fasone

Co-Supervisor

Prof. Pietro Santo Leopoldo Falletta

Candidate

Sofia Badari

(635652)

Anno Accademico 2018/2019

List of Contents

Introduction

We live in a world in which information technology surrounds every aspect of our lives. People have never been so connected with each other, communication has never been so easy, the sharing of information has never been so simple; so easy, so simple, and so dangerous. Most of the operations we perform in our daily life rely on information technology: our phone, our email box, our profile on social networks, our pictures on the cloud, our bank account, our medical records. The informatisation and digitalization of these aspects of our lives have fostered great innovation but have exposed us to risks and vulnerabilities that can be exploited by malicious actors, creating a new form of crime: the cybercrime. It is for this reason that national governments and, above all, the international community through international organizations, whose traditional goal is to ensure peace, security and stability of the international system, should focus also on the new threats posed by information technologies and ensure the security of the cyberspace: the cybersecurity, which implies the collection of resources and processes[1] to protect the cyberspace and ensure the confidentiality, integrity and availability of information, systems and networks.[2]

The purpose of my thesis is to understand how the cyberspace can be regulated. The idea behind my research is to find out which are the aspects on which the law of the cyberspace should focus in order to make the cyberspace a safer domain. To this end, I will first analyse whether existing law principles can be applied to the cyberspace. Second, I will examine ad hoc legislations on cybersecurity matters to recognize whether they are exhaustive or present soma gaps.

I tried to answer these questions, first analysing how existing principles of international law can be applied to the cyberspace. Second, I considered how a supranational organization like the European Union and a federal State as the United States are developing their legislations in order to regulate the cyberspace. The EU and the U.S' legislations represent two good examples of the law of the cyberspace. The choice to consider the EU and the U.S is justified by the fact that both actors aim to promote peace, security and cooperation between independent

[1] Craigen D., Diakun-Thibault N., Purse R. *Defining Cybersecurity*. Technology Innovation Management Review. October 2014

[2] Kosseff J. *Defining cybersecurity law*

states which share a common territory.[3] Also both have to represent different interests and minorities which can sometimes be a problem for the application of the same legislation in different States. But at the same time, profound differences resides in their legal systems, in the focus of their legislations, in the protection of rights and in the way they try to ensure cybersecurity.[4] In order to better depict their legislations, I decided to analyse some legal documents which I claim to be essential first, for the understanding of the differences in the focus of the two legal approaches to cybersecurity; second, for identifying the gaps in the legislations, with the aim to understand how the law of the cyberspace could be exhaustive. Moreover, I consider some literature to support my argument.
To the purpose of my research, I will introduce some important terminology related to the cyberspace and the crimes performed through it, which would help me to understand the danger represented by cybercrimes and the effects that these could have on States, citizens and businesses.
Then, I will analyse how the norms of international law can be applied to the cyberspace, taking into account the reports adopted by the United Nations Groups of Governmental Experts and the Tallinn Manual 2.0, a guidebook for governments concerning the applicability of international law to cyber operations. By examining cyberoperations of different nature, I will then see whether national States have applied these provisions or not.
Subsequently, I will consider the legal measures adopted by the European Union and the United States to regulate the cyberspace. Analysing on one side the European NIS Directive, the GDPR and the most recent Cybersecurity Act. On the other side, recent U.S acts like the Cybersecurity Information Sharing Act and the Cybersecurity and Infrastructure Security Agency Act. Finally, I will tackle the disclosure of information made by the whistle-blower Edward Snowden in 2013, concerning the collection of personal data information by the U.S NSA and the debate that has arisen about the protection of data and privacy in the U.S and in the EU.

---

[3] Fabbrini S.*Compound Democracies: Why the United States and Europe Are Becoming Similar*, Oxford, Oxford University Press, 2010;
[4] Bendiek, A.*Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*

Chapter 1 - Cybercrime, a new threat

1.1 Defining the issue

Our society is changing very quickly and with it also the threats to which it is exposed. As a consequence of digitalisation, attacks have changed from kinetic to cyber. Cybercrimes affect different areas ranging from cyber-dependant crimes, payment fraud and online criminal markets to child sexual exploitation online and cyber-terrorism.[5] One key feature of cybercrimes is the use of the dark web, which is composed of websites to which anyone can have access in total anonymity because IP addresses details, which allow the identification of the users, are hidden.[6]

For instance, cyber-dependent crime is a crime that «can only be committed using computers, computers networks or other forms of information communication technology».[7] These crimes include activities like the spread of malware, a software created to cause damage to computers and computers networks, and the theft of data. A means through which hackers spread malware and steal data is with the posting of fake news. In fact, fake news aim both at spreading false stories on social media in the attempt to influence and manipulate people's opinion, often relatively to a political choice,[8] and infecting computers with malicious malware. By clicking on an article or by downloading a non-safe document, a malware can be easily installed on a computer and give access to passwords and personal information.[9] As regard to payment fraud, this type of cybercrime uses skim cards data to clone cards and then resell them on dark web markets.[10]

Concerning online criminal markets, they can be found both on the surface

---

[5] Internet Organized Crime Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation 2018. EUROPOL. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[6] Technopedia definition. https://www.techopedia.com/definition/31562/dark-web

[7] Internet Organized Crime Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation 2018. EUROPOL. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[8] Matthews, K. *What Does Fake News Have to Do with Cybersecurity?*. June 19, 2019. Security Boulevard https://securityboulevard.com/2019/06/what-does-fake-news-have-to-do-with-cybersecurity-a-lot/

[9] *How Fake News Leads to Cyber Attacks*. New England College. https://www.newenglandcollegeonline.com/resources/communications/how-fake-news-leads-to-cyber-attacks/

[10] *Id.*

web and on the dark web and imply the sale of illicit commodities like fake documents which then facilitate further criminality[11] like illegal immigration. One of the worst aspects of cybercrime is represented by child sexual exploitation. Nowadays children have access to the internet at an early age and can easily be reached by offenders. Moreover, the possibility to share and obtain material on the internet has created a huge volume of Child Sexual Exploitation Material (CSEM) which was unthinkable before the advent of the internet.[12]

Regarding cyber terrorism, it took the first steps at the beginning of the new millennium when al-Qaeda started making use of the internet for the spreading of Jihad. Jihadi websites were used for discussions and showed the activities of al-Qaeda.[13] Nowadays, despite the loss of territory of the Islamic State in the Middle East, the terrorist group remains active on the internet in order to spread propaganda, inspire terrorist's attacks and enlist foreign fighters.[14]

Besides, cybercrimes are also directed to States and private companies. In 2007, a cyber-attack enacted by Russia hit Estonia government's websites and banks. In 2010, another cyber-attack was launched against the Iranian uranium enrichment facilities using a malicious computer worm[15] called Stuxnet. In 2011, the PlayStation network was hacked, and this resulted in the loss of personal data of 77 million users. More recently, in 2016, Russia interfered in the U.S elections using cyber means.

---

[11] *How Fake News Leads to Cyber Attacks*. New England College. https://www.newenglandcollegeonline.com/resources/communications/how-fake-news-leads-to-cyber-attacks/

[12] Internet Organized Crime Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation 2018. EUROPOL. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[13] Watts C. *Messing with the enemy. Surviving in a social media world of hackers, terrorists, russians, and fake news*.

[14] *Id.*

[15] Computer worm: malware computer program that replicates itself in order to spread quickly to other computers.

1.2 International organizations dealing with cybersecurity issues

1.2.1 North Atlantic Treaty Organization (NATO)

The NATO's policy establishes that cyber defence is part of the Alliance's core task of collective defence. Since the cyberspace represents a growing threat, at the Warsaw Summit in 2016 the allies recognized cyberspace as a domain in which the organization must defend itself as it does in the other domain of land, sea and air. NATO's own network are protected by the NATO Computer Incident Response Capability (NCIRC), whereas NATO's Smart Defence Projects in cyberspace facilitate countries to cooperate in order to develop capabilities against cyber threats. Moreover, NATO organizes training and exercises for member states as the Cyber Coalition Exercise. NATO also cooperates with other institutions like the European Union, United Nations and the Organization for Security and Co-operation in Europe (OSCE) in order to ensure international security. It also works together with industries in the private sector through the NATO Industry Cyber Partnership which enhance information-sharing activities and multidimensional Smart Defence projects.[16]

1.2.2 United Nations (UN)

The UN Office of Information and Communication Technology (OICT) aims to implement effective measures to face information security concerns adopting resolutions in order to strengthen information and security.[17]

1.2.3 Organization for Security and Co-operation in Europe (OSCE)

The OSCE works on confidence-building measures (CBMs) with the aim of making the cyberspace more predictable and offering mechanism for avoiding disputes among the States originated from the use of Information Communication Technologies.[18]

---

[16] NATO, Cyber Defence. https://www.nato.int/cps/en/natohq/topics_78170.htm
[17] UN, Cybersecurity https://unite.un.org/services/information-security
[18] OSCE. Cyber/ICT Security. https://www.osce.org/cyber-ict-security

1.2.4 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

The NATO Cooperative Cyber Defence Centre of Excellence based in Tallinn, aims to support member nations and NATO with an interdisciplinary expertise in cyber defence. It is a NATO-accredited research and training facility that deals with cyber defence education, research and development. The CCDCOE has fostered the creation of the Tallinn Manual, a guidebook for national government based on international law norms that can be applied on the cyberspace.[19]

1.2.5 European Cybercrime Centre (EC3)

Europol instituted the European Cybercrime Centre (EC3) in order to strengthen the law enforcement response to cybercrimes in the European Union. Since its establishment in 2013, it has been involved in several operations that have brought to the arrest of cyber criminals and have stopped several malicious files. Every year EC3 publishes the Internet Organized Crime Threat Assessment (IOCTA), a report on cyber threats. EC3 focuses particularly on three types of cybercrimes: cyber-dependent crime, online child sexual exploitation and payment fraud.[20]

1.3 Definitions

1.3.1 Security

The traditional meaning of security is related to the sovereignty of the State,[21] in particular with the security of borders and the protection of a State from exterior threats represented by other States, and can be identified with the security of the first "dimension": the land.[22] Later, the concept of security evolved in order to gather together the security of multiple States from exterior threats, this time represented not only by State actors but also

[19] CCDCOE. https://ccdcoe.org
[20] European Cybercrime Centre https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[21] Hitoshi N. *The expanded conception of security and international law: challenges to the collective security system*s. Amsterdam Law Forum, VU University Amsterdam
[22] Williams P.D, McDonald M. (eds.), *Security Studies: an introduction*, 3rd edition, Routledge, 2018

by non-State actors such as terrorist. As a result, the concept evolved into international security. Then, the concept of security has also encompassed the concept of human security, strictly related to the protection of human rights as to protect people from threats such as genocide, war crimes, ethnic cleansing and crimes against humanity.[23] The Universal Declaration on Human Rights and Freedoms defines security as a human right, stating that everyone has the right to life, liberty and security of person.[24] In fact, the concept of 'security' is strictly liked with the protection of human rights as we can't have security if our human rights are not protected.[25] The difficulty is in balancing human rights and security so that the research of security doesn't bring to some form of violation of human rights. As a matter of fact, history has shown how some states, trying to achieve high security standards, have violated human rights.[26]

Finally, the concept of security extended in order to embrace the other dimensions: the sea, the sky, the outer space and in the end the security of the cyberspace, considered the fifth dimension.[27]

The evolving meaning of the concept of security has represented a challenge for governments and legal regimes[28] which have to find ways to govern and ensure security of these areas. For instance, military means are no more the solution for the new security threats, as a consequence, there's the need of new policy responses. Furthermore, the expansion of the security concept has provided opportunities for legal developments like the law of the sea and the air and, in the end, cybersecurity law, which will be analysed in this thesis.

---

[23] Williams P.D, McDonald M. (eds.), *Security Studies: an introduction*, 3rd edition, Routledge, 2018
[24] Universal Declaration on Human Rights and Freedoms. Article 3.
[25] Ramcharan, B. *Security and Human Rights.*
[26] Iztok, P. *Relationship between security and human rights in counter-terrorism: a case of introducing body scanners in civil aviation.* International studies. Interdiscipliary political and cultural journal, Vol. 17, No. 1/2015
[27] Williams P.D – McDonald M. (eds.), *Securoty Studies: an introduction*, 3rd edition, Routledge, 2018
[28] Hitoshi N. *The expanded conception of security and international law: challenges to the collective security system*, Amsterdam Law Forum, VU University Amsterdam

1.3.2 Cyberspace

In order to understand what the law of the cyberspace is, I have taken in consideration the definition of cyberspace. Many scholars and governmental entities[29] have tried to give a definition of cyberspace, I will consider the definition of the scholar Daniel T. Kuehl, that puts together all these views giving an exhausting explanation of what the cyberspace is.
Cyberspace is defined as «a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies».[30] The fact that cyberspace is defined as a global domain means that it can be used by everyone, no one has the monopoly or the exclusivity of the use of cyberspace. It is a tool created by human beings for human beings in order to better perform their activities. In fact, through the cyberspace we can do every sort of operation, from getting information to interact with people around the world to effectuate transactions. Thanks to the cyberspace we're always and constantly interconnected with each other, we can know what happens everywhere in the world and make operations at the fastest speed ever from a single device: our computer. Substantially, we can be everywhere staying sit in our living room.

1.3.2.1 Components and characteristics of cyberspace

The functionality of the cyberspace is possible thanks to many different components. For instance, a "computer network" is «an infrastructure of interconnected devices (…) that enables the exchange of data».[31] A "cyber infrastructure" encompasses «the communications, storage, and computing devices upon which information systems are built and operate».[32] Then, a

---

[29] Kuehl D.T. *From Cyberspace to Cyberpower: Defining the Problem*, in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009). Table 2-1. Definitions of Cyberspace
[30] *Id.*
[31] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Glossary.
[32] *Id.*

"software" is formed by «the non-physical components of a computer system and cyber infrastructure. These components encompass programs, (…) and applications (…) ».[33]
A distinctive feature of the cyberspace is that it can be used by everyone almost everywhere and it operates without broadly accepted means.[34] Besides, there's a low price of entry and actors can operate in full anonymity. The fact that cyberspace can be used by everyone is positive as it allows people to get in contact with each other, inform and express themselves. On the other hand, the fact that the cyberspace is not regulated is negative because it means that everyone can do whatever operations, even illegal ones, without being judged guilty.

1.3.2.2 Cyber power: hard and soft power

Another aspect to stress is that «smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics».[35] The ability to use the cyber space for specific goals is called "cyber power". By definition cyber power is «the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power».[36] This definition shows that cyberspace is the environment in which numerous operations can be performed and cyber power is the ability to use that environment.[37] Clearly, cyber power has a huge influence on political affairs. It is used in political campaigns or by terrorist's groups in order to recruit new combatants.
Cyber power is divided in soft and hard power.[38] Cyber soft power is put in place when a public diplomacy campaign is used to influence people's

[33] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Glossary.
[34] P.D. Williams, M. McDonald (eds.), *Security Studies: an introduction*, 3rd edition, Routledge, 2018
[35] Nye J. S. Jr. *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010
[36] Kuehl D. T., *From Cyberspace to Cyberpower: Defining the Problem*, in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009).
[37] *Id.*
[38] Nye J.S. Jr. *Supra note 35*

opinion, whereas an example of an implementation of hard power in the cyberspace is a denial of service attack, which implies the denial of access to the computers of a company or a country; or the insertion of malicious codes in the computers of a company to steal intellectual property.[39]

1.3.2.3 Cybercrimes: cyber-attack and cyber exploitation

The developments in information technologies, with the consequent increase of operations performed on the internet, such as electronic payments, led to the exploitation of the cyberspace in order to perform criminal activities, called cybercrimes.

Cybercrimes can take two forms: cyber-attacks and cyber exploitations.[40]

«Cyber-attack refers to the use of deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs transiting these systems or networks».[41]

The cyber-attack is disruptive in nature and seek to make the adversary's computer systems and networks unavailable so that they become useless.[42]

More in detail, cyber-attacks aim to cause an alteration of information provided by the computer system, which after the attack doesn't give good results; compromise the authenticity of information provided and the functionality of a target system[43]. One example could be the destruction of the data on a network in order to block the functioning of a power generation facility or generate fake internet traffic in order to deteriorate the quality of the service available on the internet.[44]

On the other hand, cyber exploitation is non-destructive in nature. It is represented by the implementation of cyber operations in order to obtain confidential information and make them available to the opponents through the mapping of the network and espionage operations.[45]

---

[39] Nye J.S. Jr. *Supra note 35*

[40] William A. Owens, Kenneth W. Dam & Herbert S. Lin. National Research Council, *Technology, Policy, Law, and Ethics regarding U.S Acquisition and Use of Cyberattack Capabilities* (eds., 2009)

[41] *Id.*

[42] Lin, H. S. *Offensive Cyber Operations and the Use of Force*

[43] *Id.*

[44] *Id.*

[45] *Id.*

1.3.2.4 Typologies of cybercrime

Cybercrime can take different forms, one of these can be identifies with the term "hacking", which refers to the access and the control of someone's computer network in order to steal information from that individual, organization or agency.[46] A way to hack a computer device is through the use of a malware. As already said, a malware is a malicious software which infiltrates in a computer network and gains the control of it in order to steal information and data.[47] It can take many different forms. For instance, a "worm" is a malware that can replicate itself and spread in the computer network; a "trojan" takes the form of a normal program but it is aimed at stealing and deleting data and can perform as a "Distributed denial of Service" attack (DDoS), which involves the sending of large amount of internet traffic to a computer network in order to stop the users from accessing it.[48] A "ransomware" prevents users from accessing their computers and ask them to pay a ransom in order to have their data back and regain access. Finally, a "spyware" is installed on a computer without the consent of the user in order to monitor his/her activities and transmit the information to a third party.[49]

1.3.2.5 Actors: State and non-States actors

Now the question is to understand who performs cybercrimes.

By definition, a hacktivist is «a private citizen who on his or her own initiative engages in hacking for (…) ideological, political, religious or patriotic reasons».[50] Despite this definition it is important to notice that cybercrimes are performed also by State actors, not only by non-State

---

[46] *Cyber Crime vs Cyber Security: what will you choose? Public awareness and prevention.* Europol. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

[47] Europol, cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[48] *Cyber Crime vs Cyber Security: what will you choose? Public awareness and prevention.* Europol. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

[49] Europol. Cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[50] *Id.*

actors, and sometimes non-State actors act for commission of State entities.[51] An example of a cybercrime implemented by a State is the Russia's attack on Estonia in 2007, when a cyber campaign was launched against websites of Estonia's president, parliament, government ministries and political parties. Moreover, the targets included also banks and media organizations.[52] These attacks originated from the removal of a Soviet-era statue and soviet graves from the main square in Tallinn, which represented a painful period under soviet control for Estonian, but a sacred memorial for ethnic Russian living in the country. As a consequence of these attacks, which consisted in denial of service attacks, Estonian governmental websites went offline, and online banking functions were disrupted for several hours preventing Estonians to use their credit cards abroad.

1.3.2.6 Cybersecurity

Having defined cyber space, cyber power, cyber-attack and other terminology relative to malicious cyber operations, I considered the definition of cybersecurity. However, there is not a broadly accepted definition of this term. One reason of the difficulty to give a definition that is broadly accepted is the interdisciplinary nature of cybersecurity.[53] In fact, the field of cybersecurity gather together scholars from different disciplines, from the IT sector, to law, politics and sociology. Some scholars[54] have tried to give a unifying definition that takes in consideration the definitions previously given by academics coming from different sectors[55] trying to support the interdisciplinarity of this term.

---

[51] Williams P.D, McDonald M (eds.), *Security Studies: an introduction*, 3rd edition, Routledge, 2018
[52] *Id.*
[53] Craigen D., Diakun-Thibault N. ,Purse R. "*Defining Cybersecurity*",. Technology Innovation Management Review. October 2014
[54] *Id.*
[55] Kemmerer. "Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders."
"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." (Lewis, 2006)
"Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." (Amoroso, 2006)
"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's

«Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from the facto property rights».[56] This definition encompasses the multiple dimensions and dynamic nature of cybersecurity which involves interactions between humans, systems and humans and systems together.[57] Moreover, a cybersecurity incident includes any activity that alters actual, so de facto, property rights from perceived, so de jure, property rights.[58]

assets." (ITU, 2009)
"The ability to protect or defend the use of cyber- space from cyber-attacks." (CNSS, 2010)
"The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability." (Pub- lic Safety Canada, 2014)
"The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, as- sets and critical infrastructure." (Canongia & Mandarino, 2014)
"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014)
"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014)
[56] Craigen D., Diakun-Thibault N. ,Purse R. "*Defining Cybersecurity*",. Technology Innovation Management Review. October 2014
[57] *Id.*
[58] *Id.*

Chapter 2 – International Law applicability to the Cyberspace

2.1 Cybercrime's challenges to criminal law

When cybercrime became an issue for national governments, the different types and purposes of cybercrimes made it difficult for criminal law to formulate measures to contrast them. One of the major issues is that the existing criminal law failed to cover the new forms of cybercrime.[59] For example, the provisions applied to credit card fraud couldn't be applied to a case of a computer hacker which had stolen the credit card data of a consumer.[60] The evidence showed that the existing criminal law was outdated and failed to comply with the rising threat of cybercrime, making the existing provisions inapplicable to these new challenges. As a result, new cyber specific legislation had to be enacted.[61]

Cyber threats represent a huge challenge that can't be addressed only by national governments, as a consequence there's the need of cooperation between the international law enforcement agencies, private sector companies and the internet security industry in order to restrict the damage of cyber activities, investigate cybercrime cases[62] and regulate them.

2.2 Defining cybersecurity law

In order to understand how the cyberspace can be regulated, I considered the definition of cybersecurity law given by Jeff Kosseff, assistant professor of cybersecurity law at the United States Naval Academy. He claims that in order to give a proper definition of this term we should answer five questions: (1) what are we securing?; (2) where and whom are we securing?; (3) how are we securing?; (4) when are we securing?; and (5) why are we securing?.[63]

---

[59] Wang Q. *A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe.*
[60] *Id.*
[61] *Id.*
[62] Internet Organized Crime Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation 2018. EUROPOL. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018
[63] Kosseff J. *Defining cybersecurity law.*

To begin with, cybersecurity law aims at safeguarding the confidentiality, integrity and availability of information, systems and networks.[64]
Confidentiality refers to «the prevention of unauthorized disclosure of information»[65] and can be identified with the violation of data through cyber operations that steal personal data without the consent of the user.
Integrity concerns ensuring that «the message that is sent is the same as the message received and that the message is not altered in transit».[66] Finally availability refers to «the guarantee that the information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of the location of the user».[67]
International law should protect both government and private sector network systems since these two are highly interconnected and an attack happening in one sector can easily spread to the other. Concerning the way cybersecurity law is going to achieve this goal, it should adopt both coercive and cooperative laws. Coercive laws should deter wrong cyber practices while cooperative laws should give incentives to the public and private sector to invest in cybersecurity protection.[68]
For cybersecurity law to be effective, there should be a cooperation between these sectors through the sharing of information.
Regarding the timing for securing, cybersecurity law should have a foreword looking approach in order to prevent the happening of cybersecurity incidents.[69]
To answer the last question, so why are we securing, the first answer is that we should implement cybersecurity law to prevent harm to individuals that can occur through the violation of privacy; then cybersecurity law should prevent economic harm to companies; finally, cybersecurity law should prevent threats to national security.

---

[64] Kosseff J. *Defining cybersecurity law*
[65] Agarwal A., Agarwal A. *The Security Risks Associated with Cloud Computing.* International Journal of Computer Applications in Engineering Sciences
[66] *Id.*
[67] *Id.*
[68] *Kosseff, supra note 64*
[69] *Id.*

After all these considerations, Jeff Kosseff gives a definition of cybersecurity law affirming that: «cybersecurity law promotes confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security»[70]

2.3 International law applicable to the cyberspace

Existing principles of international law could be used to regulate also the cyberspace. Now it is to be analysed how these principles apply to cyber operations, analysing the Budapest Convention of Cybercrime of 2001, the reports released by the United Nations Groups of Governmental Experts on cyber issues in the context of international security starting from 2004, and the Tallinn Manual 2.0 on the international law applicable to cyber operations of 2017.

2.3.1 Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was drafted by the Council of Europe and other observer States[71] in 2001, and it's a binding multilateral treaty intended to fight cybercrime. The particular feature of this Convention is that it provides a framework of cooperation among EU member and non-member States. In fact, it is open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.[72] The Convention addresses crimes related to the threat of confidentiality, integrity and availability of computer systems and data like illegal access, data and system interference and misuse of device; computer-related offences, such as computer-related fraud and child pornography; offences related to infringements of copyright and

[70] Kosseff J. *Defining cybersecurity law*
[71] Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY https://www.coe.int/en/web/cybercrime/parties-observers
[72] Convention on Cybercrime. Budapest, 23.XI.2001. Article 36.

related rights. Then the Convention gives some provision to strengthen the cooperation and the dialogue among the States.[73]

In the preamble the States acknowledge the important changes that the digitalisation has brought to our society and the risk that the bad use of computer networks could lead to criminal offences. This is why they strengthen the need to pursue a common criminal policy intended to protect the society against cybercrime through the adoption of a legislation and international cooperation. Moreover, States recognize the need of cooperation between States and private industries, so between public and private sectors.[74]

Chapter I, Article 1 of the Convention gives the definitions of computer system, computer data, service provider and traffic data. Computer system indicates interconnected devices which perform the processing of data. Computer data is represented by information that can be processed in a computer system. A service provider is a public or private entity which allows users to communicate through a computer system. Finally, traffic data can be identified by computer data related to computer system communication.

Chapter II deals with measures to be taken at national level concerning offences against the confidentiality, integrity and availability of computer data systems. To begin with, Article 2 affirms that States have to consider the illegal access to computer systems a criminal offence under their domestic law. Then, article 3 asserts that States should contrast the illegal interception of computer data made by technical means. Articles 4 and 5 deal with the interference of data and systems, claiming that States have to establish as criminal offences under their domestic law the damaging, deletion, deterioration, alteration or suppression of computer data which create damages to computer systems. Moreover article 6 defines as criminal offence the production, sale and distribution of devices and computer programs such as malwares aimed to commit cyber offences. Articles 7 and 8 deal with the falsification of computer data and computer related fraud,

[73] Convention on Cybercrime. Budapest, 23.XI.2001

[74] Convention on Cybercrime. Budapest, 23.XI.2001. Preamble.

which could cause a loss of property for a user, for example through the deletion of the computer data of a company. Article 9 deals with child pornography and declares illegal the production, distribution and possession of thereof. Finally, article 10 deals with offences related to infringements of copyrights and related rights such as rights related to literary, musical, graphic and audio-visual works.

Concerning sanctions and measures to take to contrast these illegal operations in the cyberspace, article 13 states that the punishment should be characterized by «effective, proportionate and dissuasive sanctions, which include depravation of liberty» and that the measures can include monetary sanctions. Moreover, each State should adopt contrasting measure in case the cyber offence is committed: « a. in its territory; b. on board a ship flying the flag of that Party; c. on board an aircraft registered under the laws of that Party; d. by one of the nationals».[75]

In chapter III, articles 23 and 25 deal with the important issue of international cooperation and mutual assistance, essential in the field of cyber security in order to have a consistent response against cyber threats. The articles specify that the Parties should cooperate in relation to investigations or proceedings regarding criminal offences to computer systems and data, or relatively to the collection of evidence showing criminal cyber offences.[76] Moreover, article 34 deals particularly with mutual assistance «in the real-time collection or recording of content data of specified communications transmitted by means of a computer system»[77]such as conversation among terrorists which allow the police to discover their refuge or implement a blitz to prevent a possible terror attack. It is important to notice that assistance among countries relies on pre-existent agreements about cooperation between the States.

In order to give a consistent response to cyber threats, States should also share information regarding investigations over illegal cyber operations. This is why article 26 allows the sharing of information among States when

[75] Convention on Cybercrime. Budapest, 23.XI.2001. Article 22.
[76] Convention on Cybercrime. Budapest, 23.XI.2001. Article 23
[77] Convention on Cybercrime. Budapest, 23.XI.2001. Article 34.

these are considered to be essential for helping a Party in its investigations. To make this possible and provide assistance for investigations each State have to indicate a contact available twenty-four hour, seven-day-a-week basis. [78]

Finally, article 46 of the Budapest Convention deals with consultations between the Parties affirming that the Parties should consult periodically in order to facilitate the use and implementation of the Convention, the exchange of information and possible amendments. Following this, the Cybercrime Convention Committee (T-CY), which represents the States that have taken part to the Budapest Convention, has been created.

2.3.2 United Nations Groups of Governmental Experts on cyber issues in the context of international security (UN GGE)

Starting from 2004 United Nations Groups of Governmental Experts (UN GGE), have started studying how to face the threats posed by the bad use of cyberspace. The focus of their study was on existing emerging threats; how international law applies to the use of ICTs; norms, rules and principles of responsible behaviour of States; confidence-building measures and capacity building.[79] The UN GGE has made two important achievements: an outline of the global security agenda and the introduction of the principle of applicability of international law to the cyberspace.[80] The result has been three reports with conclusions and recommendations. The report of 2015 has been adopted by consensus in the UN resolution 70/237. In particular, this report affirms that States must observe the principles of international law like State sovereignty, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States.[81] Moreover, it establishes that the existing obligations under international law are applicable to the State use of International

[78] Convention on Cybercrime. Budapest, 23.XI.2001. Article 35.
[79] United Nations Office for Disarmament Affairs. Fact Scheet. Developments in the field of information and telecomunications in the context of international security
[80] Geneva Internet Platform. Digital Watch Observatory. https://dig.watch/processes/un-gge
[81] United Nations Office for Disarmament Affairs. Fact Scheet. Developments in the field of information and telecomunications in the context of international security

Communication Technologies. As a consequence, States must comply with these obligations in order to respect and protect human rights and fundamental freedoms. In addition, States are not allowed to use proxies with the aim of committing wrongful acts which can harm the international community. Besides, the States should make sure that their territory is not exploited by non-State actors to achieve these aims.[82] Finally, the UN GGE called for an increase exchange in information and cooperation among the States to face the criminal use of cyberspace. In fact, dialogue through bilateral, regional and multilateral forums is essential to maintain a peaceful ICTs environment. [83]

2.3.3 Tallinn Manual 2.0 on the international law applicable to cyber operations

After acknowledging the applicability of international law to cyberspace by the UN GGE, I considered the "Tallinn Manual 2.0 on the international law applicable to cyber operations" (the Manual), which proposes an application of such norms to cyber activities. The Manual has been written by a group of twenty-one international law experts and fifty-nine reviewers, led by Professor Michael Schmitt from the U.S Naval War Academy and Exter University Law School,[84] at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). The Manual expands the first edition of 2013 analysing international law governing the cyber warfare and addresses topics as sovereignty, State responsibility and human rights. The formulation of the provisions contained in the Manual is the result of consultations between states and legal advisors during a series of meetings held in The Hague and called "The Hague Process". These consultations allowed the States to take an active role in the shaping of the laws. Even if the Manual has been and initiative of the NATO CCD COE,

[82] United Nations Office for Disarmament Affairs. Fact Scheet. Developments in the field of information and telecomunications in the context of international security
[83] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
[84] Schmitt, M. N. U.S. NAVAL WAR COLLEGE, https://usnwc.edu/Faculty-and-Departments/Directory/Michael-N-Schmitt

it is a non-governmental project who has tried to identify the international legal rules that can be applied to cyberspace.

In the foreword the President of the Republic of Estonia Toomas Hendrik Ilves explains that the idea to draft the Manual arose from the cyber-attack that hit the Estonian private and public e-services in 2007. These attacks made the international community aware of the risks that States face every day because of the high reliance on cyberspace. The attacks also fostered the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2008 upon the initiative of Estonia, Germany, Italy, Latvia Lithuania, Slovak Republic and Spain. The North-Atlantic Council subsequently decided to confer full accreditation and International Military Organization status to the Centre. It is upon request of the NATO CCD COE that a study on cyber warfare has started. The experts have analysed how the use of cyber means and cyber operation can be regulated by international law. The result of this analysis is the Tallinn Manual, which is to be considered a guidebook for governments when it comes to the application of international law to cyber operations. It is important to notice that this manual does not represent a binding document for the nations but just a guideline.[85] The Manual analysis several aspects related to the application of international law to the cyber operations presenting 154 rules. It is divided into four parts. Part I deals with international law and cyberspace. Part II focuses on specialised regimes of international law and cyberspace as the law of the sea, air law and space law. Part III is about international peace and security and cyber activities. Finally, part IV applies the law of cyber armed conflict.

In this section I will focus on the principle of sovereignty, prohibition of intervention, use of force, international responsibility, the right to take countermeasures, the duty to make reparation for the injury caused to a state through wrongful cyber activities, precautions against cyber-attacks, international cooperation, collective self-defence and human rights in relation to cyber operations.

[85] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Introduction

2.3.3.1 Tallinn Manual definition of cyber-attack

To begin with, it is important to understand how the Tallinn Manual defines a cyber-attack. «A cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects».[86] This definition shows that in the Manual it is the employment of violence that distinguishes a cyber-attack from other cyber operations. For instance, non-violent operations such as psychological cyber operations don't qualify as attacks. What matters to qualify a cyber-attack are its violent consequences. For example, a cyber operation that manipulates the data relative to medical information of a certain individual it's not to be considered a cyber-attack, whereas a cyber operation against a chemical plant which brings to the explosion of the plant and the release of toxic substances that would kill the population is considered a cyber-attack[87] as it has «caused injury or death to persons or damage or destruction to objects[88]».

2.3.3.2 Tallinn Manual principles

a. Principle of State sovereignty

The first principle to consider is the principle of State sovereignty which can be found in Rule I of the Tallinn Manual, stating that «the principle of State sovereignty applies in cyberspace».[89] The commentary explains how «states enjoy sovereignty over any cyber infrastructure located in their territory and activities associated with that cyber infrastructure».[90] The

---

[86] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 17. Section 2, Rule 92

[87] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 17. Section 3, Rule 94.

[88] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 17. Section 2, Rule 92.

[89] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 1

[90] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 1, commentary 1.

problem with this principle is that the object over which a State has to claim its sovereignty, the cyberspace, lacks physicality. In order to overcome this issue, the Manual divides the cyberspace in three layers: the physical, logical and social layer, asserting that these are all included and regulated by the principle of sovereignty. In particular: «The physical layer comprises the physical network components (i.e., hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consists of the connections that exist between network devices. It includes applications, data and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities».[91] Furthermore, the Group of Experts affirm that a State can claim its sovereignty on all cyber activities taking place on the territory over which a State exercises its power; in addition, in the cases in which cyber activities cross borders, international waters or airspace, they are in any case performed by individuals or entities subjected to the judicial power of one or more States and, as a result, these States can claim sovereignty on them. Moreover, as stated in rule 2 dealing with internal sovereignty, a State can adopt the measures that it considers adequate regarding cyber infrastructures or activities located in its territory. For example, a State can criminalize the posting of inappropriate material such as child pornography and restrict the internet access to a certain online content, such as material related to terrorism.[92]

b. Principle of violation of sovereignty

The cyberspace and the possibility to act in total anonymity presents the opportunity for hackers and state entities to engage in activities which could harm other States. Rule 4 of the manual prohibits the violation of sovereignty caused by cyber operations that could restrain a State from exercising its sovereign power. This rule applies to unlawful actions undertaken by States and does not extend to actions enacted by non-State

[91] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 1, commentary 4.
[92] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 2.

actors.[93] Examples of violation of sovereignty are represented by a case in which «a State conducts cyber operations that could cause damage to the cyber infrastructure of a private company located in another State»;[94] or when «organs of one State are present in another State's territory and conduct cyber espionage against it without its consent or other legal justification».[95]

c. Principle of prohibition of intervention

In relation to the principle of violation of sovereignty, the Manual deals with the principle of prohibition of intervention. Rule 66 of the Manual prohibits intervention in the internal or external affairs of another State. This happens for example when a State intervenes with cyber means in order to alter or influence the political elections, as it happened with Russia's interference in the U.S 2016's elections. In fact, in 2016 11 Russian people have been charged for having gained unauthorized access, having stolen documents and have hacked computers of U.S persons and entities involved in the administration of U.S elections. [96]

d. Principle of prohibition of the use of force

Another important principle analysed by the Manual is the principle on the prohibition of the use of force. In the cyber domain the expression 'use of force' does not imply the employment of a State's armed forces but deals with the operations carried on by a State's intelligence agencies or private companies which act on behalf of the State[97] in order to dismiss the performance of computer systems and delate data. These actions are declared unlawful by rule 68 on the prohibition of threat or use of force

[93] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 4, commentary 1.
[94] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 4, commentary 5.
[95] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 4, commentary 7.
[96] Russian interference in 2016 U.S elections. FBI. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
[97] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 68, commentary 4

which affirms that «cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State are unlawful».[98] One example of this can be the Shamoon virus that hit a petrochemical company in Saudi Arabia in 2012 and caused the reparation and replacement of thousands of hard drives, or, always in Saudi Arabia, the attack at the National Industrialization Company in 2017 in which the hard drives inside the company's computer were destroyed and replaced with an image of Alan Kurdi, the Syrian child found dead along the Turkish coast while escaping the civil war. Here the aim of the attacks was both to damage the company and send a political message to the State.[99]

e. Principle of international responsibility

When a State engage in internationally wrongful cyber acts, it has to bear international responsibility for it. Chapter 4 section 1 of the Manual deals with the principle of international responsibility related to cyber activities. A State is deemed responsible in front of the international community in the case the wrongful action is «conducted by organs of the State, or by persons or entities empowered by domestic law to exercise elements of governmental authority».[100] As a result, actions of state organs such the Unites States' CIA or NSA are attributable to the USA. When it comes to non-State actors, as stated in the Articles on State Responsibility, cyber activities conducted by individual actors are not attributable to States. Despite that, the action is attributable to a State if the State has given instructions to these actors.[101] Examples of non-State actors are hackers, criminal organizations and cyber terrorists.

---

[98] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 14. Rule 68.

[99] Perlroth N., Krauss C. *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.* The New York Times. March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[100] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 1, Rule 15.

[101] Second hand quote about Articles on State Responsibility, Art 17, para. 9 of commentary in the Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I, Chapter 4, Section 1, Rule 17.

f. Right to take countermeasures

A State has the right to take countermeasures in response to a violation of an international legal obligation owed by another State.[102] Countermeasures can be carried out by an injured State in order to lead a responsible State «to comply with the legal obligations it owes an injured State».[103] These can imply the imposition of economic sanctions or the seizure of technological equipment. A State can take countermeasures also against non-State actors that have engaged in cyber operations.[104]

g. Make reparation for the injury

Since a State is responsible in front of the international community for the wrongful cyber acts committed, it also has to make reparation for the injury caused to a second State through for example the payment of economic sanctions. Rule 28 of the Manual defines the term 'injury' and states that it comprehends both material and moral damage. 'Material damage' can be identified with «the loss of data that results in financial loss»[105], while 'moral damage' is represented by violation of dignity and prestige of a State or violation of privacy. An example of moral damage can be represented by the posting of fake news in the government's website or in newspapers which can result in loss of credibility for the government.[106]

h. Precautions against cyber attacks

In order to protect the civilian population against the danger resulting from cyber-attacks, there are some precautions that the State can take. These are described in rule 121 of the Manual and deal with «segregating of computer systems on which critical civilian infrastructure depends from the Internet;

---

[102] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 2, Rule 20

[103] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 2, Rule 21

[104] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 2, Rule 20, commentary 8.

[105] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 3, Rule 28, commentary 2.

[106] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 3, Rule 28.

backing up important civilian data (…); using anti-virus measures to protect civilians' systems that might suffer damage or destruction during an attack on military infrastructure».[107]

i. Importance of international cooperation to face cyber threats

Another way to face cyber-attacks is international cooperation. Rule 13 of the Manual analyses the need of international cooperation in law enforcement. As already discussed, cyber-crime, as terrorism, is not a national issue but an international one, because of this there's the need of cooperation and mutual assistance of the international community in order to investigate criminal actions concerning the sabotage of computer systems and data of states with the aim to face it and deal with it. Examples of international cooperation in relation to cyber-crime are the Council of Europe's Convention on Cybercrime and the League of Arab States' Arab Convention on Combating Information Technology Offences. The first aims to pursue a common policy in order to protect the European society against cybercrime through the adoption of ad hoc legislation and international cooperation. It deals with infringements of copyright, computer-related fraud, child pornography and violations of network security.[108] Similarly, the second seeks to adopt a common criminal policy aimed at protecting the Arab society against information technology offences.[109]

l. principle of collective self-defence

Moreover, the Manual also takes in consideration the principle of collective self-defence analysed in rule 74 which affirms that States are allowed to exercise the right of self-defence collectively and conduct a joint defence

[107] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 17. Section 7, Rule 12, paragraph 3.
[108] Details of Treaty No.185. Convention on Cybercrime. Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[109] League of Arab States General Secretariat. Arab Convention on Combating Information Technology Offences. Preamble.

against a cyberattack.[110] Here an important role is played by the United Nations Security Council which may determine a cyber action to be a threat to peace or an act of aggression and decide to call upon the Member States in order to apply measures such as complete or partial interruption of economic relations, communication and break of diplomatic relations.[111]

m. International human rights in cyberspace

When it comes to the issue of international human rights, it is important to notice that the Manual affirms that «rights that individuals enjoy 'offline' are also protected 'online'».[112] In particular, one important human right underlined by the Manual is the freedom of expression, which in the cyber context is represented by the freedom of receiving information, sharing ideas and writing on the internet. When States block the internet access to some web pages or close some websites which contains for example online forums discussing about the government in a way contrary to its politics, these operations are to be considered against the freedom of expression. Concerning this point, the Chinese government has a real sophisticated internet censorship apparatus, called informally the Great Firewall.[113] It consists of a Central Propaganda Department aimed to monitor, censor and manipulate online content regarding inconvenient news about China, foreign affairs and social activism. Moreover, the Chinese cybersecurity law enacted in 2017 has increased the censorship in the country strengthening restrictions on online activities and placing financial pressure on IT companies and web pages. In practice this new rule implied the shutdown of several accounts and web pages and the censorship of some contents defined inappropriate. Not only domestic IT companies have to deal with these rules but also foreign ones. For example, Apple had to transfer the

[110] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part III. Chapter 14, Section 2, Rule 74.
[111] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part III. Chapter 15, Rule 75, paragraph 3.
[112] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part II. Chapter 6, Rule 34.
[113] Freedom on the Net 2018. China. https://freedomhouse.org/report/freedom-net/2018/china

data of Chinese users to a state-owned cloud, that implies the total control of the data of Chinese people by the Chinese government.
Technology is considered «an enabler of rights», in fact, the internet makes it possible for many people to make their voice herd, share their opinion and make a change. Take for example the social movements that have arisen from internet blogs and have allowed people to get in contact with each other and organize parades for social issues as climate change. This wouldn't have been possible with a high censorship.
Finally, in order to make the internet available for citizens, the State has to establish infrastructures that allows international communications, safeguard and maintain them[114] as stated in rule 61 of the Manual.

n. cyber operations not regulated by international law
Finally, there are some cyber operations which are not regulated by international law. These are described in rule 32 of the manual which deals with cyber espionage. The term «refers to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information».[115] Thanks to remote access, cyber espionage doesn't require to be physically present in a State. The International Group of Experts concurred that «customary international law does not prohibit espionage *per se*».[116]

2.3.3.3 Tallinn Manual and its applicability
It is now to understand whether States put in practice Tallinn Manual's rules or not. Overall, States seem to adopt a 'wait and see' approach regarding to the regulation of cyberspace.[117] This means that they don't

[114] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part II. Chapter 11, Rule 61
[115] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 5, Rule 32, commentary 2.
[116] *Id.*
[117] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

come clear with the rules they want to implement, remaining silent and ambiguous on the actions they take to respond to a cyber-attack.
In order to analyse whether States accept the application of international law rules in cyberspace I considered State practice in relation to malicious cyber operations. To do that I will take in consideration some case studies which involve cyberoperations directed against state entities like database and government infrastructure originated from States or individuals sponsored by States. The cyber operations that I will analyse have some aspects in common: they were politically motivated, they were supported by a foreign State and, in the most extreme cases, they caused significant physical damages to cyber infrastructures.[118]

2.3.3.3.1 Case studies

a. Cyberoperations against Saudi Arabia and Qatar
Between 2012 and 2017 there have been two cyber-attacks addressed to the computer hardware infrastructure of Saudi-Aramco, the world's biggest oil company located in Saudi Arabia and RasGas, a Qatari oil company. Both companies were joint ventures of the United States. Moreover, other two attacks were directed to Saudi government agencies and to both governmental and private institutions in the Saudi Kingdom. All these attacks have been performed through a malware called 'Shamoon' which was used with different aims.[119] First, the malware was used to replace the data of the Saudi-Armco company with the picture of a burning American flag. Subsequently the memory of the computer was erased, and it took months to replace the damaged computers. Second, the data of the RasGas company were destructed. Third, hard drives of Saudi government agencies including the data of the computers of the Civil Aviation were erased.

[118] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*
[119] *Id.*

Fourth, the malware was implemented to activate a bomb which hit governmental and private institution in Saudi Arabia.[120]
The guilty part was identified in the Iran government. Iran may have had interest in harming joint ventures of the U.S, moreover it was involved in religious and geopolitical conflicts between Shiite Muslims led by Iran and Sunni Muslims led by Saudi Arabia over the supremacy of the Arabian/Persian Gulf.[121] In addition, in the same year, Iranian gas facilities had been victims of an explosion which had caused the death of some workers and the responsible had not been found yet. As a matter of fact, it is likely that the cyberattacks of Iran could have been a retaliation against a possible previous attack of Saudi Arabia against its gas facilities.
Iran was not officially blamed either by the Saudi nor by the Qatar government. Despite that, the attacks described seem to have been a way for the States involved to take justice into their own hands, resorting to acts of retaliation through cyber means without resorting to the rules of international law.

b. The U.S presidential campaign hack

In 2016, during the election campaign that led the republican party to win, the network of the Democratic National Committee fell victim of two cyberoperations which brought to the publishing of emails related to the party.[122] These operations were intended to condition the political choice of the electors just a few months before the election day. In the same year, cyberoperations were executed against some U.S voting software supplier. Consequently, a classified intelligence report attributed responsibility for these attacks to the Russian Military Intelligence. Following this, the U.S Intelligence Community Assessment Report concluded that the cyberoperations sponsored by the Russian Government were aimed to harm the democratic candidate during the election campaign.[123] President

---

[120] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*
[121] *Id.*
[122] *Id.*
[123] Efrony, Shany, *supra note 120*.

Obama tried to deal with the situation in different ways, first choosing the diplomatic means, trying to talk with Putin during the G20 summit in China and warning him that other actions of that type would have had serious consequences. Then, he used the 'red phone', a way of communicating confidentially about urgent and sensitive situations. Finally, he issued an Executive Order, shutting downs and imposing economic sanctions to nine Russians entities and two Russian compounds located in the U.S, which were used during the cyber operations.[124]

This case study shows a violation of the principle of non-intervention. In fact, the principle affirms that a State can't intervene in the internal or external affairs of another State. As a matter of fact, data revealed by the U.S Intelligence Community Assessment have shown that the attempts to interfere with the elections could qualify as violation of the principle of non-intervention.[125]

c. Cyberoperations with global effects

In 2017 a malware called WannaCry implemented by a hacker group linked to North Korea infected computers of companies, government agencies and individuals of more than 150 countries.[126] A ransom of $300 in Bitcoins was demanded in order to restore the computers but, despite the payment, they remained blocked. Cyber experts discovered that North Korea had stolen cyber tools from the U.S National Security Agency in order to display the attack. As a consequence, States including the U.S, UK, Canada, New Zealand and Japan attributed the attack to North Korea. Despite that, no countermeasures were taken from the States involved against the attacker. However, important tech companies like Facebook and Microsoft did take countermeasure against North Korea shutting down some accounts used to launch the attacks. [127]

---

[124] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

[125] *Id.*

[126] *Id.*

[127] *Id.*

2.4 Empirical findings

It is now to understand whether the States have applied international law to cyber operations as proposed by the Tallinn manual 2.0.

To begin with, the principle of state responsibility, so the attribution of the responsibility of a cyber-attack to another State, has been put in place consequently to the WannaCry cyber-attacks and in the cyber operations against the U.S political campaign. Here States have attributed responsibility for the cyber-attacks respectively to North Korea and Russia. Conversely, an empirical example of non-attribution of state responsibility is represented by the cyber-attacks between Saudi Arabia and Iraq.

Concerning countermeasures, the cyberoperations between Iran and Saudi Arabia haven't followed the rules of countermeasures deciding to engage in what can be defined a covert cyberconflict with one another.[128] In relation to the WannaCry attack, even if States have attributed responsibility to North Korea, they have refrained to take countermeasures. On the contrary, private companies have reacted to the damages they incurred. In the three cases analysed, the only State which has taken countermeasures against its attacker have been the U.S. In fact, the application of criminal indictments against Russian, the decision to impose economic sanctions against some Russian entities and the closure of two Russian compounds, moves away from the politics of silence and gets closer to the approach of the Tallinn Manual 2.0 in relation to unlawful cyber activities.[129]

To conclude, States are not fully ready to apply the rules and principles of Tallinn Manual. In fact, case studies have shown that not always State attribute the responsibility to other States for the offenses received, and when they do, they're not always ready to take countermeasures. First, this might be explained by the fact that they could be exposed to vulnerabilities which could weaken their freedom to operate in the cyberspace.[130] As a matter of fact, as in the case of Saudi Arabia and Iran, States might prefer to

---

[128] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

[129] *Id.*

[130] *Id.*

act in total ambiguity in cyberspace and don't blame other countries for possible cyber-attacks so that they can, in their turn, act in the same way and protect their national security interests. Moreover, the decision to wait before taking action against a cyber-attack or not doing it at all is also a political and strategic choice since many interests might be involved in the relationship between two States. Second, States might be uncertain whether the provisions of Tallinn Manual really are an accurate application of the international law to cyberspace. Third, States may have doubts whether their actions in cyberspace should be regulated by international rules shared by all the States as it happens with traditional acts of war, or not. In fact, certain cyber operations, especially the ones in which imply the use of force, with the consequent destruction of physical infrastructure, have some characteristics in common with kinetic attacks.[131]

Overall, the behaviour of States concerning the applicability of international law to the cyberspace is not clear yet. As a consequence, this could lead to unpredictability in the actions taken in the cyberspace. To avoid possible conflicts, States should express their views on how international law applies to cyberspace.[132] This will contribute to shed some light on this matter and create stability in cyberspace.

2.4.1 The Budapest Convention and the Tallinn Manual 2.0

Concerning the relationship between the Budapest Convention and the Tallinn Manual 2.0, the first has to be considered a binding multilateral treaty intended to fight cybercrime, the second is an attempt to apply the existent provisions of international law to the cyberspace in order to give an exhaustive response to cybercrimes. The evidence has shown that Tallinn Manual's provisions, which are to be considered just a guideline for governments, are not entirely applied by States, which have to take position regarding the applicability of international law to cyber operations. On the other hand, in July 2019 the Budapest Convention adopted a Guidance

[131] Efrony D., Shany Y. A *Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

[132] Egan B. J. *International Law and Stability in Cyberspace.* Berkeley Journal of International Law

Note facilitating criminal justice action against election interference through cyber operations.[133] In the Guidance Note, the Parties acknowledged that cyber interference during the election process experienced in 2016 in the U.S elections and Brexit referendum with Russian, represent a threat to democracy. This attention for current threats posed by the bad use of cyberspace shows that the Budapest Convention on Cybercrime represents the most relevant international agreement on cybercrime able to address threats to human rights, democracy and the rule of law in the cyberspace.[134]

[133] Cybercrime Convention Committee (T-CY) . T-CY Guidance Note #9 Aspects of election interference by means of computer systems covered by the Budapest Convention. Adopted by T-CY 21 (8 July 2019)
[134] T-CY News. Prosecuting malicious cyber interference with elections: Guidance Note adopted on the tools of the Budapest Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/-/prosecuting-election-interference-by-malicious-cyber-activities-guidance-note-on-the-tools-of-the-budapest-convention-on-cybercrime-adopted

Chapter 3 – The EU Law of the cyberspace

The understanding of the threats that information technology poses to the European citizens, businesses and governments has led the European Union to make cybersecurity one of its priorities in the security program.[135] At first, the EU's interest in developing effective cybersecurity measures was closely related to the economic interests of the Union as information and communication technologies are essential in the development of the EU economy and the single market.[136] As a result, from the 90s the EU started developing cybersecurity non-legally binding instruments with the aim of fostering Member States' awareness concerning cyber threats.[137] It was only from the mid-2000s that the EU acknowledged that organized crime and terrorism represented a threat for the security and stability of information systems inside the Union and that there was the need of a coordinate response across Member States to address this issue. As a result, cybersecurity became a top EU policy priority.[138] This led to the adoption of legally binding instruments and programs to raise the awareness among MS about the cyber threat.

Three important legal documents have become the backbone of cybersecurity in the EU. The first is the Directive on Security of Network and Information System (NIS Directive) of July 2016. The second is the General Data Protection Regulation (GDPR) and deals with the protection of the data of European citizens. The third, recently entered into force at the beginning of 2019, is the Cybersecurity Act. All the three legal documents emphasise the bad consequences that a cyber-attack could have on the economic relations among the Member States and in the common market, therefore they stress the importance of cooperation to build a consistent response to cyber threats.

---

135 Carrapico H., Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*
136 *Id.*
137 *Id.*
138 *Id.*

3.1 The Directive on Security of Network and Information Systems (NIS Directive)

The Directive on security of network and information systems (NIS Directive) is the first example of an EU legislation on cybersecurity. It has been adopted in July 2016 and has entered into force in August 2016. It provides legal measures to improve the level of cybersecurity in the European Union. The directive stresses the importance of networks and information systems in facilitating European trade and emphasises the consequences on the economy of the European internal market that would derive from cyber operations against European technological systems. Such operations could harm the economy of the Union with consequent financial losses. Moreover, the directive acknowledges that the Member States have different levels of preparation regarding cyber security measures which leads to a fragmented approach to the protection of cyberspace across the EU.[139] This might result in a different protection of citizens and businesses across the Member States. As a consequence, in order to set up an effective mechanism for cooperation, it is essential to exchange information among the Member States and establish cooperation and common security requirements for companies which offer operators of essential services and digital service providers. Operators of essential services are companies operating in the field of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution and digital infrastructure sectors.[140] Digital service providers are businesses working in the IT sector. To this end, the directive lays down obligations for the MS to adopt a national strategy on the security of network and information systems;[141] proposes the establishment of a Cooperation Group composed by representatives of each Member States and the European Union Agency for Network and Information Security (ENISA)[142] in order to support the

[139] NIS Directive (EU) 2016/1148 of the European Parliament and of the Councile of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Preamble.
[140] NIS Directive, Annex II
[141] NIS Directive, Article 1(a)
[142] NIS Directive Preamble.

cooperation and the exchange in information among MS;[143] creates a Computer Security Incident Response Teams network (CSIRTs).[144]

3.1.1 National strategy on the security of networks and information systems

Article 7 of the NIS directive concerns national strategy on the security of the network and information systems and affirms that each Member State should adopt a national strategy and define the objectives, policies and regulatory measures to be implemented with the aim of maintaining a high level of security in the cyberspace and cover the sectors of essential services. Moreover, the directive establishes that each State should designate a national competent authority which should ensure the security of network and information systems relatively to the sectors and services of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution and digital infrastructure sectors. This authority has the task of monitoring the application of the NIS Directive at national level.[145] Moreover, national single point of contact shall be designated with the function of ensuring cross-border cooperation among Member States authorities, the Cooperation Groups and the Computer Security Incident Response Teams (CSIRTs).[146] It is essential that the competent authority, the single point of contact and the CSIRT cooperate at national level.[147] To this end, Member States should ensure that CSIRTs have adequate resources to carry out their tasks and that they have access to «an appropriate, secure, and resilient communication and information infrastructure at national level».[148]

3.1.2 Cooperation Group

Concerning the Cooperation Group, it has to be composed by representatives of the Member States, the Commission and ENISA.[149] It is established with the aim of facilitating strategic cooperation and exchange in information among Member States and achieving a common level of security of informatic systems across the

[143] NIS Dirctive, Article 1(b)
[144] NIS Directive, Article 1(c)
[145] NIS Directive, article 8, paragraph 2.
[146] NIS Directive, article 8, paragraph 4
[147] NIS Directive, article 10
[148] NIS Directive, article 9, paragraph 3
[149] NIS Directive, article 11(2)

European Union.[150] The Cooperation Groups has to provide guidance for the activities of the CSIRTs,[151] exchange best practice concerning the security of networks and information systems with Member States[152] and the Union institutions.[153]

3.1.3 The European Union Agency for Network and Information Security (ENISA)

ENISA was established by regulation 460/2004 of the European Parliament and the Council. After that its mandate was extended several times until regulation 526/2013 which extended its mandate until 2020.

The aim of ENISA is to achieve a common level of cybersecurity across the Union supporting European Member States and institutions in the fight against cyber threats. To this end, ENISA aims to help Member States and institutions to build the expertise and capacity necessary to face network and information security threats which could have a bad impact on the EU, developing national strategies[154] and national CSIRTs.[155] ENISA should also help Member States and institutions in putting the security of information and networks at the top of their agenda and make sure they implement the policies of the NIS Directive. As cooperation is important for an effective response to these threats, ENISA's task is also the one of fostering cooperation among European Member States, Institutions and companies of the private sector.[156]

3.1.4 Computer Security Incident Response Teams (CSIRTs)

CSIRTs aim to fight cybercrime and improve cybersecurity in the Union.

They have been established both in the public and private sectors, so both in the EU Member States' institutions and in European companies which play an important role in the digital sphere, namely the ones dealing with essential and digital services. They are composed by small teams of cyber experts which can

---

[150] NIS Directive, article 11(1)
[151] NIS Directive, article 11 (3a)
[152] NIS Directive, article 11 (3c)
[153] NIS Directive, article 11 (3g)
[154] NIS Directive, article 7 paragraph 2.
[155] NIS directive, article 9 paragraph 5.
[156] European Union Agency for Cybersecurity https://www.enisa.europa.eu

help Member States and companies to give an effective response to cyber threats. To do that they analyse the weaknesses of the technological systems of governmental institutions and private businesses and they provide the expertise and recommendations to mitigate the consequences of possible cyber-attacks. [157] The Directive on security of network and information systems has also decided to create a Computer Emergency Response Team at European level (CERT-EU) with the aim of strengthening the cooperation among Member States and European institutions in the fight against malicious cyber operations. CERT-EU operates as a coordinator and supervisor of the IT security teams of the EU institutions and the CSIRTs of Member States and companies for a better exchange in information and cooperation to deal with cyber threats and provide a consistent cybersecurity response.[158]
Finally, the NIS directive establishes a CSIRT's network composed by representatives of Member States' CSIRTs and CERT-EU aiming developing confidence and trust between the MS and promoting cooperation.[159]

The establishment of a national strategy on the security of networks and information systems, a Cooperation Group and Computer Security Incident Response Teams, represent the willingness of the NIS Directive to build a cooperation among European Member States in order to give an effective response to cyber-attacks and guarantee the security in the Union.

3.1.5 Member States compliance with the NIS Directive

One of the tasks of the European Commission is to pursue legal action against Member States which fail to comply with the EU law. If they fail to do so, the Commission could decide to bring them before the Court of Justice of the European Union. The European Commission has intervened in some cases concerning the transposition of the Directive on Security of Network and Information Systems. On 7th March 2019 the Commission has decided to send a

---

[157] NIS Directive, Article 9.
[158] *Cybersecurity: EU institutions strengthen cooperation to counter cyber-attacks*. European Council. General Secretariat. Press release 20/12/201 https://www.consilium.europa.eu/en/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/
[159] NIS Directive. Article 12, pragraph 1.

reasoned opinion to Belgium and Luxemburg for failing to transpose the NIS Directive in their national legislation by May 2018.[160] Besides, the Commission has just closed other two infringement proceedings concerning the transposition of the same directive against Greece and Poland after its transposition in their national legislation.[161]

3.2 The General Data Protection Regulation (GDPR)

The digitalisation has fostered new challenges for the protection of personal data. Nowadays the collection and sharing of personal data has increased a lot and citizens should be able to have their control over it.[162]

The protection of data is important both for individuals, which are worried that their personal information might be subjected to improper use; and businesses, which are afraid that a misuse of their data could have a bad impact on their reputation, leading to a fall in their consumers' trust and in their revenues.[163] Moreover, differences in the level of protection of personal data might constitute and obstacle to economic activities in the EU internal market.[164] To solve this problem there should be an harmonisation of the level of protection of the processing of personal data in all Member States.[165]

On 25 May 2018 the European Union has introduced a new regulation concerning the protection of personal data: the General Data Protection Regulation (GDPR) which repeals the Data Protection Directive 95/46/EC of 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. The GDPR sees the protection of data as a fundamental right affirming that «the protection of natural persons in relation to the processing of personal data is a fundamental right».[166] Moreover, the regulation complements the principles of freedom, security, justice, economic

---

[160] European Commission. Press Release database. March infringements package: key decisions https://europa.eu/rapid/press-release_MEMO-19-1472_en.htm
[161] *Id.*
[162] GDPR preamble, paragraph 7
[163] *General Data Protection Regulation (GDPR): The paradigm shift in privacy.* August, 2018. EY.
[164] GDPR preamble, paragraph 9.
[165] GDPR preamble, paragraph 10
[166] GDPR preamble, paragraph 1

union, social progress, strengthening of MS economies in the internal market and well-being of European citizens.[167] GDPR seeks to protect EU citizens from privacy and data breaches[168] regulating the collection and the processing of data of individuals and introducing new rules for data controllers and processors in the EU.[169] If these don't comply with the regulation, the violation can be seen as a criminal offence resulting in fines for the companies who didn't comply and claims from citizens which have seen their rights violated.[170] The regulation is characterized by an extraterritorial applicability, meaning that it applies to those companies who process the personal data of individuals residing in the European Union, even if the companies are located outside the EU.[171] This means that many of non-EU companies which have economic relations with EU costumers will have to comply with the GDPR.

3.2.1 Definitions

Article 4 of GDPR gives important definitions that should be taken in consideration while analysing the regulation. « 'Personal data' means «any information relating to an identified or identifiable natural person ('data subject'); […] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person». [172]
« 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage […] erasure or destruction».[173] « 'Controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the

[167] GDPR preamble, paragraph 2
[168] *GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive.* https://eugdpr.org/the-regulation/
[169] Alan Charles Raul. *The privacy, data, protection and cybersecurity law review*. Fifth Edition. The Law reviews. 2018 Law Business Reserach Ltd.
[170] *Id.*
[171] GDPR, Article 3.
[172] GDPR. Article 4, paragraph 1.
[173] GDPR. Article 4, paragraph 2.

purposes and means of the processing of personal data».[174] « 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller».[175]

3.2.2 The processing of data

Article 5 of GDPR deals with principles relating to the processing of personal data. It affirms that personal data should be characterized by the principles of lawfulness, fairness and transparency;[176] purpose of limitation; data minimization; accuracy; storage limitation and the integrity and finally confidentiality. More specifically, personal data shall be: collected for specified, explicit and legitimate purposes;[177] limited to the purpose for which they are collected;[178] accurate and kept up to date;[179] kept no more than the necessary period for which they have been collected and processed;[180] processed in order to ensure their security.[181] Furthermore, the processing has to be lawful. To this end, the processing has to satisfy at least one of the conditions described in Article 6 which entails the fact that the data subject has expressed his/her consent for the processing of data;[182] the processing of the data is necessary for: the approval of a contract with the data subject;[183] a compliance with a legal obligation;[184] protect data subject's vital interests;[185] perform a task for the public interest;[186] the legitimate interests pursued by the controller.[187]

On this point, Article 9 deals particularly to the prohibition of processing data which reveals «racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership».[188] Moreover, also the processing of genetic

[174] GDPR. Article 4, paragraph 7.
[175] GDPR. Article 4, paragraph 8.
[176] GDPR. Article 5, paragraph 1(a)
[177] GDPR. Article 5, paragraph 1(b)
[178] GDPR. Article 5, paragraph 1(c)
[179] GDPR. Article 5, paragraph 1(d)
[180] GDPR. Article 5, paragraph 1(e)
[181] GDPR. Article 5, paragraph 1(f)
[182] GDPR. Article 6, paragraph 1(a)
[183] GDPR. Article 6, paragraph 1(b)
[184] GDPR. Article 6, paragraph 1(c)
[185] GDPR. Article 6, paragraph 1(d)
[186] GDPR. Article 6, paragraph 1(e)
[187] GDPR. Article 6, paragraph 1(f)
[188] GDPR. Article 9, paragraph 1

and biometric data or data concerning a person's sex life or sex orientation are prohibited.[189]

3.2.3 The right of the data subjects

Chapter III of the GDPR deals with the rights of the data subjects, here Article 12 affirms that the controllers have to take measures to provide information «relating to the processing of the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language […] »[190] Consequently, article 13 describes the information that the controller should give to the data subjects. These include for example the identity and contact of the controller[191] and the purposes of the processing.[192] Moreover, Article 15 specifies that data subjects have the right to know whether his or her data are being processed and have access to information like the purposes of the processing and the period for which the data will be stored. An important right of the data subjects is the right to erasure, more specifically the right to be forgotten. Here Article 17 affirms that the data subject has the right to obtain the erasure of his/her personal data and the controller is obliged to erase these data whether, for example, the personal data are no longer needed for the purpose of the processing; or the data subjects withdraws the consent to the processing on his/her data; or he data have been processed in an unlawful way.

3.2.4 Measures to take into consideration by the controllers

Article 25 of the GDPR requires the controllers to implement technical and organizational measures in order to put into effect data-protection principles, like data pseudonymisation or minimisation.[193] Moreover, the controller should ensure that only personal data which are necessary are processed.[194] On this point, article 28 explains how the controller should use processors which provide guarantees concerning the security measures which are applied during the processing of data.

---

[189] GDPR. Article 9, paragraph 1
[190] GDPR. Article 12, paragraph 1.
[191] GDPR. Article 13, paragraph 1(a).
[192] GDPR. Article 13, paragraph 1(c)
[193] GDPR. Article 25, paragraph 1
[194] GDPR. Article 25, paragraph 2

Article 35 takes in consideration the data protection impact assessment which is required in the case the processing is using new technologies which could result in «high risk to the rights and freedoms of natural persons».[195] To avoid that, before the processing the controller should do an assessment of the impact that the processing done with new technologies might have on the protection of personal data.[196]

3.2.5 Transfer of personal data

Personal data can be transferred to third countries or international organizations, the Commission has to consider whether the third party can ensure an adequate level of protection of the personal data transferred. To do that, it has to take into account several aspects, for example related to the rule of law, the respect for human rights and fundamental freedoms, the relevel legislation and the access of public authorities to personal data.[197] In relation to third countries and international organizations, article 50 deals with international cooperation for the protection of personal data. International cooperation is aimed to «facilitate effective enforcement legislation for the protection of personal data»[198] and provide mutual assistance.

3.2.6 Supervisory authority and the European Data Protection Board

In order to ensure the application of the GDPR in all the Member states, each MS should nominate one or more supervisory authority aimed to monitor the application of the regulation, protect fundamental rights and freedoms of European citizens concerning the processing of their data and facilitate the free flow of personal data across the European Union.[199] Cooperation and mutual assistance among the supervisory authorities of each Member State is really important to ensure a consistent application of the regulation.[200] The heads of each Member State's supervisory authority together with the European Protection Supervisor form the European Data Protection Board which is established as a

---

[195] GDPR. Article 35, paragraph 1
[196] *Id.*
[197] GDPR. Article 45.
[198] GDPR. Article 50, paragraph 1(a)
[199] GDPR. Article 51, paragraph 1.
[200] GDPR. Article 61, paragraph 1.

body of the European Union and has a legal personality.[201] The Board has the task to ensure the application of the GDPR monitoring the MS, advise the Commission on the protection of personal data inside the EU proposing amendments to the regulation, issue guidelines, recommendation and best practices on procedures.[202]

3.2.7 Case Law of the Court of Justice of the European Union.

Judgement in Case C-40/17. Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

This case is about Fashion ID, a German online clothing retailer, which had embedded on its website the Facebook 'Like' button implying that when visitors consulted the company's website, their data were transmitted to Facebook Ireland. The issue is that visitors' data are transmitted without their consent and without them being aware of it. Verbraucherzentrale NRW, a German public-service association which safeguards the interests of consumers, has criticized Fashion ID for transmitting personal data of visitors to Facebook without their consent and has demanded the company to stop to do so. The Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) has requested the Court of Justice of the European Union to give its judgement. In July 2019, the EU Regulation 2016/679 (GDPR) had already repealed the Directive 95/46 on Data Protection. However, the Court has decided that the Directive 95/46 had to be applied to this dispute.[203] Article 2(d) of Directive 95/46 defines 'controller' as «the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data».[204] Following this definition and having taken into account the provisions of the Directive, the Court has concluded that Facebook Ireland and Fashion ID determine jointly the condition regarding the collection and disclosure by transmission of personal data of the visitors of Fashion ID's website[205] and as a

[201] GDPR. Article 68.
[202] GDPR. Article 70.
[203] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31995L0046
[204] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. Paragraph 65.
[205] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. Paragraph 79.

result, can be considered 'controllers'.[206] In order to justify the operations undertaken by the two actors, it is necessary that both Fashion ID and Facebook Ireland prove that in processing the data they were pursuing their legitimate interest, in accordance with article 7(f) of Directive 95/46.[207] For example, the interest of Fashion ID was aimed to advertise its website on a social network as Facebook in order to be more visible. Finally, it is essential that the operator of a website, such as Fashion ID, should obtain consent from the user before collecting and transmitting its personal data to another operator as Facebook Ireland.[208]

3.3 EU Cybersecurity Act

In April 2019 the EU Cybersecurity Act has been adopted by the European Parliament and the Council of the European Union. The Act creates a European cybersecurity certification framework for ICT products, services and processes; reinforces ENISA, the EU agency for cybersecurity, and complements the Directive on Security of Network and Information Systems (NIS Directive).
As the NIS Directive, the EU Cybersecurity Act acknowledges the impact that network and information systems have on the society and economy of the EU. Moreover, as years pass, the use of the internet by citizens, organizations and businesses increases. This means that products and services are characterized by a high level of digitalisation. The problem here is that despite this high level of interconnectivity and digitalisation, there are not sufficient tools to guarantee the security of the cyberspace. Moreover, cyber-attacks don't involve only one country, but their effect spread across States' borders. Despite that, policy and cybersecurity law measures dealing with cyber-attacks are characterized by a national approach. As a result, there's a lack of a coordination between European Member States' cybersecurity measures. This is why the Cybersecurity Act acknowledges the need to find coordinated responses and polices shared at the

[206] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. Paragraph 85.
[207] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. Paragraph 97.
[208] Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. Paragraph 106

Union level. To this aim, the capabilities of the Member States have to be strengthened in order to give a consistent and coordinate response to cross-border cyber-attacks.[209]

To improve the cybersecurity inside the Union, the Cybersecurity Act establishes a European cybersecurity certification scheme for ICT processes, products and services which will be valid across the EU. This will enhance trust and cybersecurity in the EU Digital Single Market. In fact, there will be more transparency regarding the security of products and services on the internet and companies will provide more secure digital solutions. As a result, the users' trust in ITC products and services will increase and this would allow a safer trade across EU borders.[210] Moreover, the Cybersecurity Act strengthens the role of the European Union Agency for Network and Information Security (ENISA) granting it a permanent mandate and conferring the role of European Union agency for cybersecurity.[211] ENISA will improve the capabilities and expertise of EU and national public authorities, will increase the cooperation and exchange in information between EU Member States and EU institutions and ensure the implementation of EU policies in the field of cybersecurity. Finally, ENISA will cooperate with the European Cybersecurity Certification Group (ECCG) composed by representatives of national cybersecurity certification authorities with the aim to facilitate cooperation between national cybersecurity certification authorities and supervise the application of European cybersecurity standards.[212]

---

[209] EU Cybersecurity Act. Preamble.

[210] *EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency*. Council of the EU. Press release. 19/12/2018. https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

[211] EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency. Council of the EU. Press release. 19/12/2018. https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

[212] EU Cybersecurity Act. Article 62.

3.3.1 Common cybersecurity certification

Cybersecurity certification is important because it increases trust and security in ICT products, services and processes which are essential for the European economy. Before the Cybersecurity Act, the certification of ICT products, services and processes was valid only at State level. This means that a certification issued by one Member State was not recognised in another Member State. This difference in certification among member States led to fragmentation and barriers inside European economy.[213] A European cybersecurity certification framework, on the contrary, aims to improve the level of cybersecurity of the European internal market adopting a common approach relatively to cybersecurity certification. This creates a digital single market for ICT products, services and processes.[214] The European cybersecurity certification framework develops cybersecurity certification schemes, European cybersecurity certificates and EU statement of conformity for ICT products, services and processes which are shared by EU MS.[215] The idea of having European cybersecurity certification schemes is that of ensuring that ICT products, services and processes that have been certified following common rules, comply with European standards and requirements shared by Member States. These standards and requirements seek to protect the availability, authenticity, integrity and confidentiality of IT data and services.[216] The certification schemes will specify the categories of products which are covered; the cybersecurity requirements taken into account and the type of evaluation, which can be done by self-assessments or by third parties;[217] and the level of assurance, which can be basic, substantial or high.[218] The three levels of assurance represent how secure a specific product, service or process is and the risk that users could incur in the use of thereof.

In order to comply with the aim of the cybersecurity certification schemes to harmonise cybersecurity practices and increase the level of cybersecurity across the European Union,[219] Member States should adopt the European cybersecurity

---

[213] The EU cybersecurity certification framework. Digital Single Market. European Commission. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[214] EU Cybersecurity Act. Article 46.
[215] EU Cybersecurity Act. Preamble paragraph 69.
[216] EU Cybersecurity Act, Article 46, paragraph 2.
[217] EU Cybersecurity Act, Article 53
[218] EU Cybersecurity Act, Article 52
[219] Cybersecurity Act, preamble, paragraph 95

certification scheme in their national legislation.[220] Moreover, each Member States has to appoint a national cybersecurity certification authority which would supervise the actions of that State.[221] Finally, cybersecurity certification authorities are subjected to peer review. This is done in order to achieve equivalent standards across the EU Member states. [222]

3.3.2 Strengthening of ENISA

Since the establishment of ENISA in 2004, the cyberspace and its use have changed a lot becoming less secure. This is why the Cybersecurity Act has reviewed the mandate of ENISA in order to adapt it to the new cybersecurity ecosystem. Based on the new mandate, ENISA should become the reference point of European Member States and institutions regarding every policy or regulation to be implemented. It should provide advices and expertise acting as the centre of information and knowledge in the Union.[223] Moreover, it has to foster the exchange in information about cybersecurity and increase cooperation among Member States, EU institution and private businesses. In order to increase MS and institutions' capabilities, ENISA should develop a cybersecurity training platform which should foster the cybersecurity awareness and improve coordination among States.[224] Furthermore, ENISA should cooperate with Member States in the preparation of an EU Cybersecurity Technical Situation Report on incidents and cyber threats based on the information shared by the CSIRTs of each Member State.[225] ENISA should also adopt a preventive approach analysing current and emerging cybersecurity risks. To this aim it should conduct analysis of the new technological innovations and try to predict which could be the threats posed by these new technologies.[226] ENISA should also care about the impact of cyber threats to the single European citizens, making them aware of the threats which they could incur everyday using the internet. To this end, ENISA should organise awareness and public education campaigns to

[220] EU Cybersecurity Act, preamble, paragraph 98
[221] EU Cybersecurity Act, Article 58
[222] EU Cybersecurity Act, Article 59
[223] EU Cybersecurity Act. Article 4 paragraph 1.
[224] EU Cybersecurity Act. Article 4 paragraph 7.
[225] EU Cybersecurity Act. Article 7 paragraph 6.
[226] EU Cybersecurity Act. Preamble. Paragraph 38.

educate and guide individual citizens but also organisations and businesses in the use of cyberspace. These campaigns would promote a safe behaviour in cyberspace making users aware of some kinds of criminal activities like banking and data frauds and provide them with protection advices.[227]
When it comes to cooperation with other organizations,[228] ENISA should cooperate with all the European institutions which operate in the field of cybersecurity such as the European Defence Agency (EDA), the Body of European Regulators for Electronic Communications (BEREC) and the European Data Protection Board.[229]Concerning non-European organizations, ENISA should cooperate with OSCE, NATO and OECD in order to organise joint cybersecurity exercises and joint incidence response coordination.[230]

3.3.3 The EU Digital Single Market

Nowadays everyone can buy online and have their purchases delivered at home in a few days, it's easy, it's quick and sometimes is also cheaper. In the EU, one out of five businesses sell online through websites and apps. E-shopping is common among all age groups, with the highest percentage of 77% among 25 to 34 years old's users. The most popular online purchases in the EU are clothes and sports goods, followed by household goods (46%), holiday accommodation (43%) and tickets for events (39%).[231] Shopping online also implies that the users provide information about their credit cards and their address, these are very sensitive information and require the internet to be a safe place in order to function in a safe way for everyone. As digital technologies and internet are changing the way we trade, the European Union wants to ensure to offer a common market that fits in the digital age.[232] Until now there have been some barriers among Member States' digital markets leading the consumers to have a restricted access to some goods and services, and the businesses not to gain enough profits. Since cyber-

[227] EU Cybersecurity Act. Article 10.
[228] EU Cybersecurity Act. Article 42
[229] EU Cybersecurity Act. Preamble. Paragraph 44.
[230] EU Cybersecurity Act. Preamble. Paragraph 43
[231] *Online shoppers and e-purchases*. Erostat.
https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-2a.html
[232] *What is the digital single market about?*. Eurostat
https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

attacks represent a possible threat to the economy of the Union, the EU has developed a policy related to those aspects of the economy which take place on the cyberspace: the Digital Single Market. The aim of the Digital Single Market is removing barriers to digital trade among EU Member States seeking to give more opportunities to consumers and businesses. The strategy of the Digital Single Market, adopted in 2015, is made of three policy pillars that deal with improving the access to digital goods and services, creating an environment in which digital networks and services can prosper and making the digital sector become a driver for growth.[233] To this end, first, barriers to the online markets of EU MS will be removed, ensuring better access to online goods and services in the EU. Second, high-speed and secure infrastructures and services will be provided to ensure protection and transparency in online trade. Third, digital skills will be intensified in order to maximise the capability of the European Digital Economy. [234]

3.4 Implementation of EU's cybersecurity policy

Despite the EU's attempts to promote a coordinated response to ensure cybersecurity in the Union, the EU approach to cybersecurity is still not uniform.[235] This is caused by different factors. First, there's a lack of coordination between institutions, whose evolution in cybersecurity matters have evolved in different ways and whose objectives are sometimes not enough clear and distinguished from one another. Second, Member States seems to be reluctant in enhancing EU powers in the field of cybersecurity and this leads to problems of coordination between MS and EU institutions, which fails to convince MS of the importance of a coordinate response to cyber threats.[236] Third, the resources allocated to cybersecurity programmes are very low, especially compared to the U.S. For example, in 2013 the U.S government allocated USD 3.2 billion to cybersecurity, while ENISA got € 11 million and the European Cybercrime

---

[233] *What is the digital single market about?*. Eurostat https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

[234] *Id.*

[235] Carrapico H., Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*

[236] *Id.*

Centre € 7 million.[237] Fourth, at national level, cybersecurity is seen as a new sensitive area and Member States are reluctant in sharing information. In particular, some MS, like France, Germany, The Netherlands and Italy are more inclined to cooperate at the EU level, while others, such as the Visegrad countries and Austria, prefer a sub-regional form of cooperation.[238] Fifth, there's a difference in capabilities and prioritization among MS, which are not ready to deploy equal economic resources for cybersecurity programs. Finally, there's a lack of coordination among private companies in addressing cyber threats in a homogeneous way.[239]

[237] Carrapico H., Barrinha A., *supra note 235*
[238] *Id.*
[239] *Id.*

Chapter 4 – The U.S Law of the cyberspace

The development of information technologies and the number of economic activities performed online have increased the crimes related to cyberspace both in the public and in the private sector. The U.S has been victim of several cyber-attacks which aimed particularly to breach the users' data. Examples of these are the attacks at Sony and at Yahoo in which hackers stole millions of user's data and information. The attacks of 11/9 at the World trade Center and the Pentagon, were the starting point for the U.S to improve their national security addressing both physical and cyber infrastructures.[240] These attacks have also changed the perception of security in the U.S, shifting it from a state-oriented to a people and infrastructure oriented.[241] As a consequence, also U.S cybersecurity has become human-oriented and critical infrastructures, such as telecommunications, electrical power systems, transportation and emergency services,[242] have become the major reference objects in the U.S cybersecurity programs.[243] One explanation of this is that the state-centric concept of security can't be applied to the cyberspace due to its conformation. In fact, the virtual aspect of the cyberspace makes it possible to cyber threats to target not only the state, but also individuals and every aspect of their lives.[244]

I will analyse in which way the security of individuals and in particular the protection of their data information is ensured by U.S law of the cyberspace. Moreover, the U.S approach to cybersecurity highlights the importance of cooperation between private and public sectors. This shifts the responsibility of security from the state to both the state and the private companies which play an important role in the cyberspace, creating a public-private cooperation between these two sectors.[245] I will investigate, through the analysis of some Acts, how the cooperation between these two sectors is put in place in the U.S.

---

[240] Le Cheng J. P., Danesi M. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse.*
[241] *Id.*
[242] Executive Order 13010: Critical Infrastructure Protection. 1996. In Le Cheng, Jiamin Pei & Danesi Marcel. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse*
[243] Le Cheng, Danesi, *supra note 240*
[244] *Id.*
[245] *Id.*

To do that I would consider the most recent acts concerning cybersecurity issues, namely the Federal Information Security Management Act (FISMA) of 2002, the National Cybersecurity Protection Act and the Cybersecurity Enhancement Act of 2014, the Cybersecurity Information Sharing Act of 2015, the Cybersecurity and Infrastructure Security Agency Act of 2018 and the role of CISA, the agency instituted by it. And finally, the California Consumer Act of 2018 dealing specifically with the protection of personal data information.

4.1 Federal Information Security Management Act (FISMA)

One important act to consider is the Federal Information Security Management Act (FISMA) included in the E-Government Act of 2002.

The E-Government Act is focused on the government services that can be enjoyed by American citizens on internet and how to regulate them. Its aim is the establishment of a Federal Chief Information Officer within the Office of Management and Budget in order to enhance the management and promotion of electronic Government services and processes. Moreover, it aims at promoting the use of the internet in order to increase the participation of citizens in the U.S Government, providing them with more information and services.[246]

The Federal Information Security Management Act is important because it strengthens the Federal Government information security developing mandatory information security risk management standards.[247] It applies to every governmental agency and its aim is to ensure the security of data of the federal government.[248] To this aim, U.S federal agencies have to implement an information security and protection program. More specifically, each Federal agency should provide information security protections to avoid the harm which could result from the «unauthorized use, disclosure, disruption, modification or destruction of […] » agencies' information, and information systems used by the agencies. [249]

[246] E-Government Act of 2002. Section 2.
[247] Federal Information Security Management Act of 2002.
[248] Federal Information Security Management Act of 2002. Section 3531.
[249] Federal Information Security Management Act of 2002. Section 3534.

4.2 National Cybersecurity Protection Act

The National Cybersecurity Protection Act of 2014 is to be taken in consideration because it amends subtitle C of title II of the Homeland Security Act of 2002 dealing with information security, by adding the definition of 'cybersecurity risk' and by codifying the National Cybersecurity and Communication Integration Center.[250] By definition, cybersecurity risk can be identified as «threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism».[251]

The National Cybersecurity and Communication Integration Center should be an interface and a coordinator for the sharing of information related to cybersecurity risks and incidents across the Federal Government. It should provide shared situational awareness relatively to incidents to Federal and non-Federal entities and technical assistance. It should be composed by representatives of sector-specific agencies, civilian and law enforcement agencies and elements of the intelligence community. [252]

4.3 Cybersecurity Enhancement Act

The Cybersecurity Enhancement Act of 2014 is aimed at providing an ongoing, voluntary public-private partnership to improve cybersecurity; strengthen cybersecurity research, development, education and public awareness.

It amends the National Institute of Standards and Technology Act in order to «facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedure, and processes to cost-effectively reduce cyber risks to critical infrastructure».[253]

---

[250] National Cybersecurity Protection Act of 2014. Section 226.
[251] National Cybersecurity Protection Act of 2014. Section 226 (a) Definitions.
[252] National Cybersecurity Protection Act of 2014. Section 226 Composition.
[253] Cybersecurity Enhancement Act of 2014. Section 101.

In carrying out these activities, coordination and with the private sector and consultation with public sector's national security agencies and organizations are essential.[254] The final purpose is to identify and mitigate the impacts of the cybersecurity measures on businesses confidentiality [255] and protect individual privacy and civil liberties. Moreover, every four years should be developed a Federal Cybersecurity Research and Development Strategic Plan in order to reach objectives such as secure complex software-intensive systems, privacy of individuals, a robust security for the internet and protect the information processed. [256] Section 301 of the Act highlights the importance of innovation in cybersecurity research, technology development and prototype demonstration. Importance is also given to national cybersecurity awareness and education programs [257] in order to make cybersecurity best practices available for individuals, businesses, educational and governmental institutions; increasing public awareness of cybersecurity; and increasing the understanding of the benefits of having the means to face cyber threats. Finally, section 502 deals with international cybersecurity technical standards related to information system security to be reached through coordination among the Federal agencies.

4.4 Cybersecurity and Infrastructure Security Agency Act

The Cybersecurity and Infrastructure Security Agency Act amends the Homeland Security Act of 2002 to reorganize the Department of Homeland Security's with the Cybersecurity and Infrastructure Security Agency (CISA).[258] The Agency will be composed by: a Cybersecurity Division[259] and an Infrastructure Security Division.[260] The Agency will be headed by the Director of the Cybersecurity and Infrastructure Security whose task is to lead cybersecurity and critical infrastructure security programs; coordinate with Federal and non-Federal entities;

[254] Cybersecurity Enhancement Act of 2014. Section 101.
[255] Id.
[256] Cybersecurity Enhancement Act of 2014. Section 201
[257] Cybersecurity Enhancement Act of 2014. Section 401
[258] Cybersecurity and Infrastructure Security Agency Act of 2018
[259] Cybersecurity and Infrastructure Security Agency Act. Section 2203
[260] Cybersecurity and Infrastructure Security Agency Act. Section 2204

provide analyses, expertise and technical assistance.[261] The aim of the CISA is protecting U.S critical infrastructure from physical and cyber threats.[262] The National Cybersecurity and Communications integration Center (NCCIC) would provide Federal government and private agencies with cyber situational awareness, analysis, incident response and cyber defence capabilities; and the National Risk Management Center would provide risk analysis for critical infrastructure. This center works closely with the private sector in order to identify and analyse risks to the U.S Critical Functions.

The work of CISA is possible thanks to coordinated efforts among the private and public sectors which are provided by the agency with trainings and technical assistance. Moreover, CISA aims at strengthening U.S emergency communication capabilities and build effective emergency responses in the case of emergency situation as cyber or terrorist attacks or natural disasters.

4.5 Cybersecurity Information Sharing Act

The Cybersecurity Information Sharing Act was signed by President Obama in 2015 and is considered the most significant piece of cyber-related legislation enacted to date.[263] It is aimed at improving cybersecurity in the United States through the enhancement of the sharing of information about cybersecurity threats between public and private sectors. To this aim, the act creates a framework for the information sharing between governmental agencies and institutions and private companies.

Section 103 of the Act affirms that the sharing of information has to be done relatively to classified and unclassified cyber threat indicators, defensive measures, cybersecurity threats and cybersecurity best practices. Section 104 deals with authorizations for preventing, detecting, analysing and mitigating cybersecurity threat. Here a cybersecurity threat has to be identified as « a means an action, not protected by the First Amendment of the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an

---

[261] Cybersecurity and Infrastructure Security Agency Act, Section 2202

[262] CISA https://www.dhs.gov/CISA

[263] Sullivan & Cromwell. *Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector.*

information system or information that is stored on, processed by, or transiting an information system». [264]

Moreover, the Act describes the operations that private entities can adopt for cybersecurity purposes. Here 'cybersecurity purpose' indicates «the purpose of protecting an information system […] that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability». [265] A private entity can, for example, monitor information systems or adopt defensive measures for cybersecurity purposes in order to protect the rights or property of a private entity; share and receive cyber threat indicator or defensive measure with other non-Federal entities or with the Federal Government.[266] Here 'cyber threat indicator' refers to an information necessary to describe or identify anomalous patterns of communications, security vulnerabilities and malicious cyber activities.[267] It is important to notice that the private sector cannot undertake offensive security measures but can only adopt defensive measure for cybersecurity purpose to contrast cyber threats.

The aim of the Act is also to confirm the authority and operational framework of the National Cybersecurity and Communications Integration Center.[268] The Center, as codified by the National Cybersecurity Protection Act, is a civilian agency of the Department of Homeland and Security and its aim is to coordinate the sharing of information relatively to cybersecurity operations within the Federal Government and with private entities.

The Cybersecurity Act of 2015 is the result of years of discussions on whether the sharing of information could be beneficial to the fight against cyber threats or could result in a further threat for the parties involved.[269] While some see the adoption of the Cybersecurity Act as a success,[270] other have concerns about some provisions of the act dealing with the lack of protection of privacy that could

---

[264] Cybersecurity Information Sharing Act of 2015. Section 102(5)
[265] Cybersecurity Information Sharing Act of 2015. Section 102(4)
[266] Cybersecurity Information Sharing Act of 2015. Section 102(c)
[267] Cybersecurity Information Sharing Act of 2015. Section 102(6)
[268] Cybersecurity Act of 2015. Title II – National Cybersecurity Advancement.
[269] Sullivan & Cromwell. *Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector*
[270] U.S. Chamber of Commerce, U.S. Chamber President Comments on Omnibus Spending Bill (Dec. 16, 2015) https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill

result from the sharing of information between private entities and the government.[271] This means that the U.S government could use the information shared for purposes which have nothing to do with cybersecurity issues.[272] Other concerns deal with the fact that the share of information would do very little to solve cybersecurity issues putting at risk U.S citizens' privacy.

Jeff Kosseff, whose definition of cybersecurity law has been analysed in Chapter 2 of this thesis, claims that the Cybersecurity Information Sharing Act is the statute that is most close to the concept of cybersecurity law described by him. Especially because of the cooperation between the public and private sector in countering cyber threats. Moreover, the Cybersecurity Information Sharing Act deals with all the threats described by Kosseff, namely threats to the confidentiality, integrity and availability of information, systems and networks. [273]

4.6 Data protection in the U.S

In the U.S there is not a general federal legislation about the protection of data like in the European Union with the GDPR. Despite that, there are several specific laws about data protection which are enacted both at federal and state level. Federal and state laws address specific sectors like financial services and healthcare or focus on particular types of data.[274] Some examples of specific federal data protection laws include the Children's Online Privacy Protection Act, which forbids the collection of information about children under 13 years old and requires consent of parents when information about children are being collected. Or the Video Privacy Protection Act aimed at regulating the wrongful disclosure of audio-visual materials.[275] Concerning state laws, they address the collection, use, disclosure and security of information of citizens collected by businesses relative to different areas like medical records, email addresses or insurance

---

[271] McLaughlin J. *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity*, THE INTERCEPT (Dec. 18, 2015) https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/

[272] *Id.*

[273] Kosseff J. *Defining Cybersecurity Law*

[274] USA: Data Protection 2019 ICLG.com https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

[275] *Id.*

information.[276] The types of data information protected by these laws vary from state to state, moreover, some states are more concerned about the protection of data. I will analyse the case of the State of California as it has always been inclined to adopt laws to protect data information also in relation to the technological development and the presence of a high number of IT companies in this state. Moreover, in 1972 California's constitution has been amended in order to include the right of privacy among the inalienable rights of people and has defined fundamental the individual's ability to control the use of their personal information.[277]

4.6.1 California Consumer Privacy Act

In June 2018 California's governor Brown has signed the Assembly Bill 375, known as the California Consumer Privacy Act of 2018 (CCPA). The act, which will become effective in January 2020, aims at giving citizens new rights regarding the collection of their personal information. Section 1 of the act acknowledges the personal privacy implications that can result from the collection of personal information. The misuse of these information could result in financial fraud, identity theft, reputational damage and even physical harm.[278] The act refers also to the misuse of personal data by the company Cambridge Analytica [279] that has been analysed in this thesis in relation to U.S 2016 elections, to show how personal information could be used for every kind of purpose, even to threat a state's democracy.

Having explained the reasons why the protection of data information is important, the act lists the rights that it will ensure to California's citizens. Californians will have the right to know what personal information is being collected about them,[280] the purposes for which the personal information are

[276] USA: Data Protection 2019 ICLG.com https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
[277] California Consumer Privacy Act of 2018. Section 2(a).
[278] California Consumer Privacy Act of 2018. Section 2(f)
[279] California Consumer Privacy Act of 2018. Section 2(g)
[280] California Consumer Privacy Act of 2018. Section 2(1)

used[281] and whether their personal information is sold or disclosed and to whom.[282] Moreover they will have the right to 'say no' to the sale of personal information;[283] access their personal information[284] and the right to equal service and practice.[285] Important is also the right to request a business to delate any personal information that has been collected from the consumer. [286]
The act also grants some rights to businesses as the right to keep the personal information collected if these are useful for some purpose of the business as complete the transaction for which the information was collected[287] or detect security incidents.[288]

Many of the purposes of the California Consumer's Privacy Act resemble with the European General Data Protection Regulation. However, not all the U.S States grant the same rights and protection to their citizens. This is an important issue that will be discussed in the next chapter.

[281] California Consumer Privacy Act of 2018. (1798.100)
[282] California Consumer Privacy Act of 2018. (1798.100) (2)
[283] California Consumer Privacy Act of 2018. (1798.100) (3)
[284] California Consumer Privacy Act of 2018. (1798.100) (4)
[285] California Consumer Privacy Act of 2018. (1798.100) (5)
[286] California Consumer Privacy Act of 2018. (1798.105)
[287] California Consumer Privacy Act of 2018. (1798.105) (1)
[288] California Consumer Privacy Act of 2018. (1798.105) (2)

Chapter 5 - Protection of personal data in the post-Snowden Era

Nowadays the social media play a huge role of our lives, we share pictures and comments every day, and these represent personal information that other people learn about us, which is also the scope of posting them. Our aim is sharing our experiences with our friends, but the truth is that we end up sharing personal information that could be used against us. Moreover, we share personal information when we pay with our credit card at the supermarket, when we sign up at the gym or when we buy a ticket for a concert online. All these operations and transactions make our life much easier as we can perform them really quickly, but they also make it really easy to collect information about us, what we do, where we do it, what time we do it, and with whom we do it. Everything we do through internet leaves a digital trace and becomes part of a large quantity of data which can be collected.[289] But who should collect personal data information and why?

5.1 Differences in data protection in the U.S and EU

The cybersecurity policy of the U.S and EU are characterized by different elements. The U.S policy is dominated by the logic of military defence and deterrence. The European policy is aimed at strengthening domestic capabilities and resist or recover from cyber-attacks.[290] In the same way, concerning the protection of individuals' privacy, there are differences between the U.S and the EU. For example, privacy is enshrined as fundamental right in the European Convention on Human Rights,[291] but no right to informational privacy is enshrined in the American constitutional law.[292] The U.S Fourth Amendment offers limited privacy protection in the public sector, but no constitutional protection for individuals that exchange data in the private sector.[293] To make

[289] Halbert D., Larsson S. *By Policy or design? Privacy in the US in a Post-Snowden World.* Journal of Law, Technology and Public Policy. Lund University.
[290] Bendiek A. *Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*
[291] Petkova B. *Privacy as Europe's First Amendment*
[292] *Id.*
[293] *Id.*

some practical examples, the U.S law doesn't consider it a problem when the police of the secret services collect personal data information that U.S citizens has published on social networks, or when businesses exchange contact information about their employees, because these operations are not considered dangerous for the privacy of individuals[294] and could be useful to improve the security of the U.S. On the other hand, according to the EU data protection law, companies in the EU can't transfer any personal data to the U.S, not even relatively to the information that people post voluntarily on social networks.[295] These differences show that the U.S haven't enacted laws which prohibits or minimize the automated processing of personal data and could be explained by the fact that limitations in the processing of data would have represented an obstruction to the evolution of information technologies,[296] essential in for the U.S economic development.

5.2 U.S perspective

In 2013 Edward Snowden, a former United States National Intelligence contractor, divulgated information about mass surveillance practices in the U.S, namely how the U.S National Security Agency had been collecting data information about U.S and European citizens and politicians. The NSA had managed to collect data from the severs of some U.S service providers like Microsoft, Google, Facebook, Skype, YouTube and Apple.[297] The information disclosed have highlighted the lack of adequate legal regulation to protect personal data in the U.S and have proved that the U.S intelligence services had been collecting and analysing data about a large number of people against whom there was no suspect of criminal behaviour.[298]

After the attacks of 9/11, the U.S government increased security and mass surveillance to protect the country from every kind of threat, including the cyber

---

[294] Determann L. *Adequacy of data protection in the USA: myths and facts. International Data Privacy Law*, 2016, Vol. 6, No. 3.
[295] *Id.*
[296] *Id.*
[297] Rossi A. *U.S., British intelligence Mining data. Gellman and Poitras. In How the Snoeden Revelations saved the EU General Data Protection Regulation.*
[298] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance.

ones. The U.S Patriot Act has played a huge role increasing American surveillance systems.[299] The Act, aimed at enhancing domestic security against terrorism and surveillance procedures, allows to intercept wire, oral and electronic communications related to terrorism[300] or computer fraud.[301] This has led the NSA to collect information about every single American citizen, not only the ones suspected of terrorism or having contacts with terrorists.

The collection and storage of personal data could be seen as a threat to the privacy rights of Americans as it brings the U.S government to collect sensitive information about citizens and build profiles of people and relations among them.[302] On the other hand, the Intelligence Agency claims that the control over personal data is constitutional and essential to protect the U.S from terrorism.[303] In fact, as former NSA general counsel Stewart Baker claims, it is the lack of collection of data that fails the prevention of terrorist's attacks. [304]

One of the first leaks of Snowden was a document containing proof that NSA was collecting telephone records of millions of US citizens. On this point, U.S senator Ron Wyden defines the fact that the government knows who the citizens call or are in contact with «enormously intrusive».[305] Moreover, as Chris Soghoian, principal technologist of ACLU, claims, each time we connect to the internet, send an email or have a call, we create data, but we don't expect data to be shared with the government or other entities.[306] We should be free to communicate without fearing to be under surveillance. On the other hand, the chair of the Senate intelligence committee Dianne Feinstein claims that the collection of call

---

[299] Halbert D., Larsson S. *By Policy or design? Privacy in the US in a Post-Snowden World.* Journal of Law, Technology and Public Policy. Lund University.

[300] Patriot Act. Section 201.

[301] Patriot Act. Section 202.

[302] Jameel Jaffer, Deputy legal director ACLU
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2

[303] NSA Files: decoded. The Guardian By EWEN MACASKILL and GABRIEL DANCE Produced by FEILDING CAGE and GREG CHEN Published on November 1, 2013
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[304] *Id.*

[305] *Id.*

[306] *Id.*

records is not to be identified as surveillance as it doesn't imply the collection of the content of communication among individuals.[307]

Understandably, there are many different opinions concerning the protection of data in the U.S. Moreover, the regulation of protection of privacy seems to be really controversial. On one side the U.S government seeks methods to enhance its surveillance capabilities, as it did with the Patriot Act, on the other, the House of Representatives fails to pass laws related to the protection of data in the cyberspace, as it did when it filed to pass the Protecting Children from Internet Pornography Act because it would have entailed the collection of IP addresses for more than a year and this was considered to interfere the internet privacy of U.S citizens.[308]

5.3 European perspective

In Europe, Snowden's revelations led to huge debates and loss of trust towards Europe's closest political ally that had used internet platforms such as Google and Yahoo, to collect information about European citizens, violating the European fundamental right on the protection of privacy.[309] Moreover, the revelations produced a shock which led to an increase attention to the issues of privacy, surveillance and as a result, a push for the approval of the General Data Protection Regulation in order to strengthen privacy protection.[310] The Parliamentary Assembly of the Council of Europe has in fact invited the European Union to accelerate its work for the finalisation of the GDPR.[311]

---

[307] NSA Files: decoded. The Guardian By EWEN MACASKILL and GABRIEL DANCE Produced by FEILDING CAGE and GREG CHEN Published on November 1, 2013 https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[308] Halbert D., Larsson S. *By Policy or design? Privacy in the US in a Post-Snowden World.* Journal of Law, Technology and Public Policy. Lund University.

[309] Bendiek A. *Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*

[310] Rossi A. *How the Snoweden Revelations saved the EU General Data Protection Regulation.*

[311] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 18.

5.3.1 Comments of the Council of Europe

Resolution 2045 of the Council of Europe's Parliamentary Assembly express the Assembly's concerns about the information disclosed by Snowden and the threats to internet security that they represent.[312] It affirms that the practices of mass surveillance represent a threat for fundamental human rights as the rights to privacy, freedom of information and expression affirmed in the European Convention of Human Rights. These rights are essential for the existence of democracy and their violation would also put at risk the rule of law.[313]

The Assembly is also worried that the documents collected could be used wrongly by State and non-State actors.[314] Moreover, the spread of mass surveillance tools, such as the ones used by the U.S government, could be detrimental if used by authoritarian regimes which could use them to control freedom of expression and information. [315]

The Assembly notices how targeted surveillance of suspected terrorists and organised criminal groups would be effective for law enforcement and crime prevention. On the other hand, mass surveillance represents a wastefulness of resources and, contrary to what intelligence officials claim,[316] does not prevent terrorist attacks.[317] In order to fight terrorism, also in the form of cybercrime, it is necessary an international cooperation. In order to establish it, mutual trust among nations is essential. It is exactly this trust that has been questioned after the disclosure of information by Snowden.[318] To repair the damage, it is to be established a legal framework at national and international level aimed at ensuring

---

[312] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 5

[313] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 4.

[314] [314] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 6.

[315] [315] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 8.

[316] Stewart Baker, former NSA general counsel. NSA Files: decoded. The Guardian By EWEN MACASKILL and GABRIEL DANCE Produced by FEILDING CAGE and GREG CHEN Published on November 1, 2013 https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[317] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 11.

[318] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 12.

the protection of human rights, in particular the right to privacy. One way to do that is represented by the guarantee of protection of whistle-blowers like Snowden, who expose themselves to danger in name of the truth, namely make the American citizens aware that their rights have been violated. It is to be noticed that at the moment Snowden is living in Russia after being granted a political asylum.

Concerning the role of national parliaments and member states of the Council of Europe, the Assembly requires them to monitor, scrutinize and control national security services and armed forces to guarantee the respect of human rights, rule of law, democratic accountability and international law.[319] Moreover, national intelligence services should be subject to judicial and/or parliamentary control mechanisms.[320] Finally, national laws should adopt effective security measures concerning the collection of personal data and should allow it only after the approval of the person concerned.[321]

5.3.2 Comments of the European Parliament

After the Snowden's revelations, the European Parliament adopted a resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizen's fundamental rights.[322]

5.3.2.1 Mass surveillance as violation of fundamental rights

The European Parliament affirms that the practices of mass surveillance put in place by the U.S, are in contrast with fundamental rights as the freedom of expression, thought and data protection, affirmed in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights.[323] As a consequence, since data protection and privacy are considered

---

[319] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 16.
[320] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 19.2
[321] *Id.*
[322] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)
[323] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph A.

fundamental rights, the measures put in place to ensure people's security and counter terrorism, must be pursued through the rule of law and must be subject to privacy and data protection obligations.[324] It follows that the transfer of personal data among EU institution, agencies or MS to the U.S in the absence of adequate protection of these data in respect of the fundamental rights guaranteed to EU citizens, would represent a violation of fundamental rights enshrined in the EU Charter.[325] Moreover, The European Parliament calls on MS to evaluate and revise their national legislation concerning the activities of intelligence services in order to ensure they're subjected to parliamentary and judicial oversight.[326]

5.3.2.2 Relation between the European Union and the United States

The European Parliament affirms that the trust between the European Union and the U.S, their democratic institutions, the rule of law and the security of IT services has been put at risk. This is why there's the need of a response plan to restore trust.[327] A way to do that is represented by an agreement between the EU and the US concerning data protection. This agreement has to be negotiated by the European Commission and will be called 'Umbrella Agreement'.[328] The Parliament also recognizes that cooperation between the European Union and the U.S in the field of countering terrorism is vital for the security of both actors.[329] In order to continue this partnership, the cooperation between the two actors should be based on the respect of rule of law and the rejection of the practices of mass surveillance.[330]

5.3.2.3 Protection for whistle-blowers

The Parliament calls on the Commission to consider the possibility of a legislative proposal concerning a programme for the protection of whistle-blowers like

[324] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph A.
[325] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph AD.
[326] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 21.
[327] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 4.
[328] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 57.
[329] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph D.
[330] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 115.

Snowden and calls on the MS to examine the possibility of granting to whistle-blowers an international protection from prosecution.[331]

5.2.2.4 Enforcement of IT security capabilities

The European Parliament is also concerned to the development of European IT security capabilities and calls on European agencies and institutions to review technical and budget EU capabilities in order to ensure a high level of IT security systems. [332] Moreover, MS in cooperation with ENISA, Europol's Cybercrime Center, CERTs and national data protection authorities and cybercrime units should develop a culture for security through education campaigns aimed to make European citizens more aware and informed about the protection of their personal data.[333]

5.4 Meeting point between the U.S and EU

In response to the requests of the European Parliament, the European Commission signed the "Umbrella Agreement" with the U.S.

In fact, after the Snowden revelations, the U.S needed to restore trust both nationally and internationally. One step towards this aim has been the "Umbrella Agreement" with the EU, aimed to the protection of personal information in relation to the prevention, investigation detection and prosecution of criminal offences.[334] The EU Umbrella Agreement was signed in June 2016 in order to strengthen the protection of personal data exchanged between EU and U.S law enforcement authorities, namely police and criminal justice authorities. The agreement represents a common data protection framework between the EU and the U.S regarding the exchange of information for law enforcement purposes.[335] The Umbrella Agreement is conditional to the adoption of the Judicial Redress

[331] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 88.
[332] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 101.
[333] Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph 109.
[334] EU-US Umbrella Agreement on data protection. European Parliament. Plenary, 28 November 2016
[335] EU-US agreement on personal data protection. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8

Act by the U.S Congress, which extends to European data subjects the right to enforce their data protection rights in U.S courts.[336]

[336] EU-US Umbrella Agreement on data protection. European Parliament. Plenary, 28 November 2016

Conclusion

The virtual feature of the cyberspace has challenged legal regimes to find the appropriate measures to regulate cyberoperations and deal with cybercrimes.
In this thesis I tried to understand how the cyberspace can be regulated, analysing on which aspects some legislations on cybersecurity matters focus and the gaps they present.
To this end, I introduced some terminology related to the cyberspace and cybercrimes, this helped me to narrow down the threats against which the law of the cyberspace should protect States, citizens and businesses. Namely, threats to the confidentiality, integrity and availability of information, systems and networks.[337] This first part showed that the focus of the law of the cyberspace should be on the protection of users' data, the information shared among them and the guarantee that the cyberspace is always available for everyone.[338]
Then I moved to the analysis of the principles of international law that can be applied to the cyberspace taking in consideration the United Nations Groups of Governmental Experts on cyber issues in the context of international security (UN GGE), which has introduced the principle of applicability of international law to regulate the cyberspace.[339] I also considered the Tallinn Manual 2.0 on the international law applicable to cyber operations, a proposed application of such norms to cyber activities which does not represent a binding document. After having analysed some types of cyberoperations, I considered the application of the Tallinn Manual provisions by the victim States. the evidence has shown that States are not ready to accept all the provision of the Manual and still have some doubts about the applicability of international law to the cyberspace. On this point, I concluded that despite the failure of nation States to apply the principles of international law to the cyberspace, the application of these principles in the resolution of disputes over cyber issues is still valuable and it's just a question of time before states express their views on the applicability of international law principles to the cyberspace.[340]

---

[337] Kosseff J. *Defining cybersecurity Law*
[338] *Id.*
[339] Geneva Internet Platform. Digital Watch Observatory. https://dig.watch/processes/un-gge
[340] Egan B. J. *International Law and Stability in Cyberspace.* Berkeley Journal of International Law.

This outcome moved my research to the analysis of the EU and U.S law of the cyberspace, where I provided for a detailed analysis of legal documents recently enacted. Both actors have in fact created ad hoc legislations and institutions in order to deal with cybercrime. Despite that, these legislations present some gaps that were useful to outline the focus of the law of the cyberspace.
The EU law of the cyberspace provides for a framework of cooperation among Member States, and between Member States and Institutions, but some European MS seem not willing to comply with these legislations. In fact, despite the adoption of the NIS Directive, which tries to solve the issue of different levels of cybersecurity preparation of Member States;[341] the GDPR, which ensures the protection of privacy and data of European citizens; and the most recent Cybersecurity Act, aimed at coordinating the different legislations and protection measures across the Member States; the European approach to cybersecurity is still not uniform.[342] In fact, Member States seem to be reluctant in enhancing EU powers in the field of cybersecurity and sharing information, leading to problems of coordination between MS and EU institutions.[343] Moreover, at national level, cybersecurity is seen as a new sensitive area and Member States are reluctant in sharing information.[344] Additionally, the resources allocated to cybersecurity programmes are still very low.[345] These issues revealed the historical fragmentation among European Member States. Besides, cohesion on cybersecurity matters among European MS is essential in order to give a consistent response against cybercrimes. To have cohesion, it is important that the EU raises the awareness among MS about the threat represented by cybercrime and allocates more founds to improve cyber capabilities. When awareness about cybercrimes is reached not only at European level, but also and especially at State level, and when more founds will be allocated to each MS, these will probably become more willing to adopt the measures enacted by the EU.

---

[341] NIS Directive (EU) 2016/1148 of the European Parliament and of the Councile of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[342] Carrapico H., Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*
[343] *Id.*
[344] *Id.*
[345] *Id.*

After considering the gaps in the EU law of the cyberspace, I moved to the U.S law of the cyberspace in order to see if it presented the same gaps.
Overall, the U.S security policy is dominated by the logic of military defence and deterrence,[346] and this is reflected also in the approach to cybersecurity, where the U.S allocates more financial resources compared to the EU.[347] The U.S law of the cyberspace focuses on the importance of cooperation among public and private sectors and sharing of information with the ultimate aim of guaranteeing security of the U.S, no matter the costs or the rights at stake. While some see the sharing of information beneficial to the cybersecurity of the U.S, other have concerns about the lack of protection of privacy that could result from the sharing of information between private entities and the government.[348] These concerns raised from the experience of NSA collection of data information that Edward Snowden had revealed in 2013. In fact, although the aim of the Cybersecurity Enhancement Act is to provide for the protection of privacy of individuals, in the U.S there is not a general federal legislation about the protection of data like in the European Union with the GDPR.[349] Despite that, there are several specific laws about data protection enacted both at federal and state level.[350]
Understandably, some U.S States are more concerned than others about the protection of privacy and data information and provide for exhaustive legislations on this matter.[351] It has been the lack of a legislation at federal level on the protection of privacy and data information that, following the disclosure of information made by Snowden in 2013 about the practices of mass surveillance carried on by the U.S National Security Agency, has led to many debates inside the U.S. and between the U.S and the EU.

---

[346] Bendiek A. *Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*
[347] Carrapico H., Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*
[348] McLaughlin J., *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity*, THE INTERCEPT (Dec. 18, 2015) https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/
[349] And in any case the Cybersecurity Enhancement Act has entered into force one year after the Snoeden's leak.
[350] USA: Data Protection 2019 ICLG.com https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
[351] The State of California has adopted the 'California Consumer Privacy Act in 2018', in response to the technological development and the presence of a high number of IT companies in this State.

Thus, these findings show that the EU provides for exhaustive legislations at European level, but Member States are not willing to implement them because of fragmentation, reluctance of MS in enhancing EU powers in the field of cybersecurity and sharing information, lack of awareness of the threats represented by cybercrimes and lack of funds. Oppositely, although the presence of stronger cohesion among U.S States and more funds allocated to the fight against cybercrimes, the lack of exhaustive federal legislation on the protection of privacy and data represents the gap in the U.S legislation. The analysis of EU and U.S legislations on cybersecurity matters underlined the importance for the law of the cyberspace to focus on cooperation and sharing of information in order to make the cyberspace a safer domain. Nevertheless, the sharing of information implies the protection of personal data information as fundamental rights.[352]
The research can finally conclude that the law of the cyberspace should focus on the protection of users' data, information shared among them and the guarantee that the cyberspace is always available for everyone.[353] Moreover, it should take in consideration the principles of international law applied to the cyberspace by the Tallinn Manual 2.0, which could represent a value added to the regulation of the cyberspace. In fact, if these principles are respected in the international relations among States, they could be respected also in the cyber relation among States, as the cyberspace is defined as a 'global domain'.[354]
The gaps in the EU and U.S legislations were useful to outline the focus of the law of the cyberspace which should foster cooperation and sharing of information in all the domains addressed by the EU and U.S legislations, namely among States, institutions, international organizations and the private sector. This shifts the responsibility of security from the state to both the state and the private companies, which play an important role in the cyberspace, creating a public-private cooperation between these two sectors.[355] Finally, the law of the

[352] In fact, privacy is enshrined as fundamental right in the European Convention on Human Rights. Moreover, the GDPR regulation sees the protection of data as a fundamental right affirming that «the protection of natural persons in relation to the processing of personal data is a fundamental right» (GDPR preamble, paragraph 2)
[353] Kosseff J., *Defining cybersecurity Law*
[354] Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009). Table 2-1. Definitions of Cyberspace.
[355] Le Cheng J. Pei & Danesi M. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse.*

cyberspace should protect privacy and data information. This last aspect will represent a new challenge for the law of the cyberspace, which will have to ensure that the processing of data and sharing of information among states, institutions and business, essential for preventing cyber threats to result into cyber-attacks, won't harm the privacy and data of individuals. The protection of data information and privacy is strictly related to the principle of protection of human rights in cyberspace foreseen by the Tallinn Manual 2.0, which affirms that «rights that individuals enjoy 'offline' are also protected 'online'».[356]

[356] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part II. Chapter 6, Rule 34.

Bibliography

Agarwal A., Agarwal A. *The Security Risks Associated with Cloud Computing.* International Journal of Computer Applications in Engineering Sciences

Alan C. R. *The privacy, data, protection and cybersecurity law review.* Fifth Edition. The Law reviews. 2018 Law Business Reserach Ltd.

Bendiek A. *Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*

Carrapico H., Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*

Craigen D., Diakun-Thibault N., Purse R. *Defining Cybersecurity.* Technology Innovation Management Review. October 2014

Determann L. *Adequacy of data protection in the USA: myths and facts. International Data Privacy Law*, 2016, Vol. 6, No. 3.

Efrony D., Shany Y. *A Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

Egan, B. J. *International Law and Stability in Cyberspace.* Berkeley Journal of International Law

Fabbrini S., *Compound Democracies: Why the United States and Europe Are Becoming Similar*, Oxford, Oxford University Press, 2010;

Halbert D., Larsson S. *By Policy or design? Privacy in the US in a Post-Snowden World.* Journal of Law, Technology and Public Policy. Lund University.

Hitoshi N. *The expanded conception of security and international law: challenges to the collective security system.* Amsterdam Law Forum, VU University Amsterdam

Iztok P. *Relationship between security and human rights in counter-terrorism: a case of introducing body scanners in civil aviation'.* International studies. Interdisciplinary political and cultural journal, Vol. 17, No. 1/2015

Kemmerer. *Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders.*

Kosseff J. *Defining cybersecurity law.*

Kuehl D. T. "*From Cyberspace to Cyberpower: Defining the Problem*," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009). Table 2-1. Definitions of Cyberspace

Le Cheng J. P. & Danesi M. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse*

Lin, H. S.*Offensive Cyber Operations and the Use of Force*

Nye J. S. Jr. "*Cyber Power*" Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010

Petkova B. *Privacy as Europe's First Amendment*

Ramcharan B. *Security and Human Rights*.

Rossi A. *U.S., British intelligence Mining data. Gellman and Poitras. In How the Snoeden Revelations saved the EU General Data Protection Regulation*.

Sullivan & Cromwell. *Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector*.

Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition.

Wang Q. *A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe*

Watts C. *Messing with the enemy. Surviving in a social media world of hackers, terrorists, Russians, and fake news*

William A. Owens, Kenneth W. Dam & Herbert S. *Lin. National Research Council, Technology, Policy, Law, and Ethics regarding U.S Acquisition and Use of Cyberattack Capabilities* (eds., 2009)

Williams P.D., McDonald M. (eds.), *Security Studies: an introduction*, 3rd edition, Routledge, 2018

Webliography

CCDCOE. https://ccdcoe.org

CISA https://www.dhs.gov/CISA

Cyber Crime vs Cyber Security: what will you choose?. Public awareness and prevention. Europol. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

Cybercrime Convention Committee (T-CY) . T-CY Guidance Note #9 Aspects of election interference by means of computer systems covered by the Budapest Convention. Adopted by T-CY 21 (8 July 2019) https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23

Cybersecurity: EU institutions strengthen cooperation to counter cyber-attacks. European Council. General Secretariat. Press release 20/12/201 https://www.consilium.europa.eu/en/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/

Details of Treaty No.185. Convention on Cybercrime. Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency. Council of the EU. Press release. 19/12/2018. https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

EU-US agreement on personal data protection. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8

EU-US Umbrella Agreement on data protection. European Parliament. Plenary, 28 November 2016 http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-conclusion-of-the-eu-us-data-protection-umbrella-agreement

European Commission. Press Release database. March infringements package: key decisions https://europa.eu/rapid/press-release_MEMO-19-1472_en.htm

European Cybercrime Centre https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

European Union Agency for Cybersecurity https://www.enisa.europa.eu

Europol, cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
file:///Users/sofiabadari/Downloads/area-of-justice-and-fundamental-rights_conclusion-of-the-eu-us-data-protection-umbrella-agreement_2019-09-01.pdf

Freedom on the Net 2018. China. https://freedomhouse.org/report/freedom-net/2018/china

GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive. https://eugdpr.org/the-regulation/

General Data Protection Regulation (GDPR): The paradigm shift in privacy. August, 2018. EY
Geneva Internet Platform. Digital Watch Observatory.
https://dig.watch/processes/un-gge

How Fake News Leads to Cyber Attacks. New England College.
https://www.newenglandcollegeonline.com/resources/communications/how-fake-news-leads-to-cyber-attacks/

Internet Organized Crime Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation 2018. EUROPOL.
https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

NATO, Cyber Defence.
https://www.nato.int/cps/en/natohq/topics_78170.htm

Online shoppers and e-purchases. Erostat.
https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-2a.html

OSCE. Cyber/ICT Security. https://www.osce.org/cyber-ict-security

Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY https://www.coe.int/en/web/cybercrime/parties-observers

Russian interference in 2016 U.S elections. FBI.
https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

T-CY News. Prosecuting malicious cyber interference with elections: Guidance Note adopted on the tools of the Budapest Convention on Cybercrime.
https://www.coe.int/en/web/cybercrime/-/prosecuting-election-interference-

by-malicious-cyber-activities-guidance-note-on-the-tools-of-the-budapest-convention-on-cybercrime-adopted

Technopedia definition. https://www.techopedia.com/definition/31562/dark-web

The EU cybersecurity certification framework. Digital Single Market. European Commission. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

U.S. Chamber of Commerce, U.S. Chamber President Comments on Omnibus Spending Bill (Dec. 16, 2015) https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill

UN, Cybersecurity https://unite.un.org/services/information-security

United Nations Office for Disarmament Affairs. Fact Scheet. Developments in the field of information and telecomunications in the context of international security. https://www.un.org/disarmament/ict-security/

USA: Data Protection 2019 ICLG.com https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

What is the digital single market about? Eurostat https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

Legal Documents

California's Consumer Privacy Act

Convention on Cybercrime. Budapest, 23.XI.2001

Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance.

EU Cybersecurity Act

EU General Data Protection Regulation (GDPR)

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)

League of Arab States General Secretariat. Arab Convention on Combating Information Technology Offences

NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Preamble.

Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019.

U.S Cybersecurity and Infrastructure Security Agency Act

U.S Cybersecurity Enhancement Act

U.S Cybersecurity Information Sharing Act

U.S E-Government Act of 2002

U.S Federal Information Security Management Act (FISMA)

U.S Federal Information Security Management Act of 2002

U.S National Cybersecurity Protection Act

U.S National Cybersecurity Protection Act of 2014

U.S Patriot Act

Universal Declaration on Human Rights and Freedoms.

Newspaper Articles

Matthews K. '*What Does Fake News Have to Do with Cybersecurity*? June 19, 2019. Security Boulevard https://securityboulevard.com/2019/06/what-does-fake-news-have-to-do-with-cybersecurity-a-lot/

McLaughlin J. *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity*, THE INTERCEPT (Dec. 18, 2015) https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/

NSA Files: decoded. The Guardian By EWEN MACASKILL and GABRIEL DANCE Produced by FEILDING CAGE and GREG CHEN Published on November 1, 2013 https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Perlroth N., Krauss C. *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*. The New York Times. March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Reports of Cases JUDGMENT OF THE COURT (Second Chamber) 29 July 2019. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31995L0046

Summary

As information technology plays more and more an important role in our society, the world it's changing and with it also the threats to which we are exposed. Traditionally the States and the international community had to deal with threats of kinetic nature such as armed conflicts and terrorism. Nowadays, as we use computer devices and internet every day to performs different kind of operations such as transactions, purchases, sharing of contents and data, this has led some actors with great computer science experience, to exploit the cyberspace in order to make profit. This had led to a new form of crime: the cybercrime. It can take many different forms, ranging from the simple payment fraud, stealing the credit card data of a consumer, or stealing the data of a company through the spreading of a malware, to child sexual exploitation and cyber-attacks to governmental institutions. Understandably, cybercrimes do not only affect individuals, but also private companies, governments and institutions. This is why cybersecurity has become one of the top priorities for international organizations such as the NATO with the Cooperative Cyber Defence Centre of Excellence, the UN, the OSCE and the European Cybercrime Center, which are developing programs to ensure it.

The purpose of my thesis is to understand how the cyberspace can be regulated. The idea behind my research is to find out which are the aspects on which the law of the cyberspace should focus in order to make the cyberspace a safer domain. To this end, I will first analyse whether existing law principles can be applied to the cyberspace. Second, I will examine ad hoc legislations on cybersecurity matters to recognize whether they are exhaustive or present soma gaps.

I tried to answer these questions, first analysing how existing principles of international law can be applied to the cyberspace. Second, I considered how a supranational organization like the European Union and a federal State as the United States are developing their legislations in order to regulate the cyberspace. The choice to consider the EU and the U.S law of the cyberspace is justified by the presence of both similarities and differences concerning their conformation, legal systems and approach to cybersecurity.

Definitions

In order to understand cybercrimes and how to deal with them, it is important to understand what cyberspace is. The cyberspace is defined as a 'global domain' in the field of information technologies which allows people to create, store modify and exchange information.[357] This means that cyberspace can be used by everyone in order to perform daily tasks, easier and quicker, such as doing purchases online or communicate easily with people around the world. It is exactly the easy accessibility to the cyberspace that gives the possibility to some malicious actors to exploit it. In particular, cyberspace can be exploited with the use of soft and hard power.[358] Cyber soft power is the use of the cyberspace to make propaganda, cyber hard power is implied when the aim of the malicious cyber operation is the damaging of computer devices.[359] It follows that cybercrimes divides in the form of cyber-attacks and cyber exploitation.[360] The first leads to the disruption and unavailability of computer networks and systems. The second implies the steal of data and confidential information.[361] Moreover cybercrimes can take many different forms, one of these can be identified with the term "hacking", which refers to the access and the control of someone's computer network in order to steal information,[362] and can be implemented through the use of worms, trojans, DDoS, ransomwares and spywares.[363] Cybercrimes are performed both by state and non-state actors.[364] This means that the law should address both in order to be effective.

---

[357] Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009). Table 2-1. Definitions of Cyberspace

[358] *Id.*

[359] Nye Joseph S. "Cyber Power", Jr. Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010

[360] William A. Owens, Kenneth W. Dam & Herbert S. Lin. 'National Research Council, Technology, Policy, Law, and Ethics regarding U.S Acquisition and Use of Cyberattack Capabilities' (eds., 2009)

[361] *Id.*

[362] "Cyber Crime vs Cyber Security: what will you choose?". Public awareness and prevention. Europol. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

[363] Europol. Cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[364] P.D. Williams, M. McDonald, 'Security Studies: an introduction', 3rd edition, Routledge, 2018

The regulation of the cyberspace

Cybercrime represented a challenge from criminal law, which became outdated and failed to comply with this new threat.[365] As a result, new laws had to be promulgated in order to ensure the security of the cyberspace and the operations performed through it. The laws dealing with cyber matters should in fact ensure the confidentiality, integrity and availability of information, systems and networks.[366] This means that they should prevent the disclosure of personal information such as data, in order to protect the privacy of individuals; ensure that the operations enacted by a user are not altered; and guarantee that everyone can benefit from the use of information technologies.[367] Finally, this new type of law should prevent economic harm to companies and threats to national security.[368]

One of the first attempts to create a framework of cooperation in the cyberspace has been the Budapest Convention on Cybercrime of 2001. Which is a binding multilateral treaty among EU member and non-member States drafted by the Council of Europe and aimed at fighting cybercrime.[369] The Convention calls for cooperation among the States who took part to the treaty and addresses cybercrimes which aim to disrupt the confidentiality, integrity and availability of computer systems and networks, giving provisions against crimes such as payments fraud, infringements of copyrights and child pornography.[370]

I then analysed of how existing principles of international law could be applied to the cyberspace. In particular, the United Nations Groups of Governmental Experts on cyber issues in the context of international security (UN GGE), has introduced the principle of applicability of international law to regulate the cyberspace and operations performed through it.[371] It has affirmed that principles such as the protection of human rights, fundamental freedoms, state sovereignty

---

365 Wang, Qianyun. 'A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe'.
366 Kosseff, Jeff. 'Defining Cybersecurity Law'
367 *Id.*
368 *Id.*
369 Convention on Cybercrime. Budapest, 23.XI.2001. Preamble.
370 Convention on Cybercrime. Budapest, 23.XI.2001. Article 23
371 Geneva Internet Platform. Digital Watch Observatory. https://dig.watch/processes/un-gge

and the settlement of disputed by peaceful means apply to the cyberspace.[372] Besides, also the he UN GGE calls for an increase exchange in information and cooperation among the States to face the criminal use of cyberspace.[373]
The Tallinn Manual 2.0 on the international law applicable to cyber operations, is a proposed an application of such norms to cyber activities. The Manual does not represent a binding document but is to be considered a guidebook for governments when it comes to the application of international law to cyber operations.[374] To begin with, I considered the definition of cyber-attack given by the Manual, which distinguishes from cyberoperations because it implies the use of violence to «cause injury or death to persons or damage or destruction to objects».[375] In my analysis I focused on the application of the principle of sovereignty, prohibition of intervention, use of force, international responsibility, right to take countermeasures, international cooperation and human rights in cyberspace. The principle of sovereignty applies to the cyberspace and implies that a State enjoys sovereignty over cyber infrastructures and operations which take place in their territory.[376] The principle of prohibition of intervention, deals with the illegality of the intervention of a State in the internal affairs of another State with cyber means, in order to alter or influence the political elections.[377] The prohibition of use of force, implies the illegality to implement operations aimed at dismissing the performance of computer systems and delate data through a virus.[378] The principle of international responsibility, implies that when a States or its organs engage in wrongful cyber operations, they have to bear international responsibility for it.[379] The right for a State to take countermeasures gives the right

[372] United Nations Office for Disarmament Affairs. Fact Sheet. Developments in the field of information and telecommunications in the context of international security
[373] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
[374] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Introduction
[375] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. chapter 17. Section 2, Rule 92
[376] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 1
[377] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Rule 66. An example of violation of the principle of intervention is represented by the Russia's interference in the U.S 2016's elections.
[378] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Rule 68
[379] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 1, Rule 15

to a State to impose economic sanctions in response to cyber-attacks.[380] In the same way, it is obligation of the State which caused injury, moral or material, to a second State, to make reparations for it.[381] The Manual also stresses the importance of international cooperation among States to fight cybercrime taking as an example the Budapest Convention.[382] Cooperation among States can be enacted also adopting the principle of collective self-defence according to which the States can collectively conduct a joint defence against a cyber-attack.[383] The Manual tackles also the question of human rights in cyberspace, affirming that the rights «enjoyed offline are also protected online».[384] One important human right underlined by the Manual is the freedom of expression, which in the cyber context is represented by the freedom of receiving information, sharing ideas and writing on the internet, which can be threatened when the government exercises control over web pages and limits the availability of the web pages and social platforms.[385] I then moved to the analysis of different types of cybercrimes against States or private businesses to see if the principles of the Tallinn Manual 2.0 had been applied. The first case study concerns cyberoperations against the computer hardware infrastructure of Saudi-Aramco and RasGad, oil companies located in Saudi Arabia and Qatar; and to governmental agencies. In all these cyberoperations was used a malware called 'Shamoon' with the aim of erasing the computer memory and disrupt the data of the companies and governmental agencies. Moreover, the malware was also used to make a bomb explode inside governmental and private institution in Saudi Arabia.[386] The Iranian government was identified as responsible of the attacks because of its involvement in religious

---

[380] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 2, Rule 20

[381] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 4, Section 3, Rule 28

[382] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part I. Chapter 17. Section 7, Rule 13

[383] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part III. Chapter 14, Section 2, Rule 74

[384] Tallinn Manual 2.0 on the international law applicable to cyber operations. Second edition. Part II. Chapter 6, Rule 34

[385] Reference is made to the Chinese internet chensorship apparatus called 'Great Firewell' Freedom on the Net 2018. China. https://freedomhouse.org/report/freedom-net/2018/china

[386] Efrony D., Shany Y. *A Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*

This cyberoperation could qualify as cyber-attack as it implied the explosion of a bomb with the aim of disrupting physical infrastructures.

and geopolitical conflicts with Sunni Muslims led by Saudi Arabia[387] and because its gas facilities had just been victims of an explosion whose responsible hadn't been found yet. Despite that, Iran was not officially blamed either by the Saudi nor by the Qatar government. As a result, evidence has shown that States have chosen not to resort to the principles of international law but have decided to adopt the strategy of retaliation to solve disputes among them.

The second cyberoperation I've analysed concerns the attacks against the U.S Democratic National Committee which caused the publishing of emails related to the party[388] with the aim of conditioning the election results during the U.S presidential campaign of 2016. The U.S Intelligence Community Assessment Report concluded that the cyberoperations were to be attributed to the Russian Government.[389] In response to this, President Obama issued an Executive Order, shutting downs and imposing economic sanctions to nine Russians entities and two Russian compounds located in the U.S, which were used during the cyberoperations.[390] This case study is an example of violation of the principle of non-intervention, in fact the attempts to interfere with the elections can qualify as violation of such principle.[391]

The last case study I've analysed deals with the WannaCry malware which infected computers of companies, government agencies and individuals of more than 150 countries.[392] The responsibility of the attack was attributed to a hacker group linked to North Korea, but no countermeasures were taken by governments against it. Despite that, important tech companies like Facebook and Microsoft did take countermeasure against North Korea shutting down some accounts used to launch the attacks. [393]

Concerning the application of the Tallinn Manual principles, the principle of state responsibility has been put in place consequently to the WannaCry cyber-attacks and in the cyber operations against the U.S political campaign, but not after the cyber-attacks between Saudi Arabia and Iraq. The right to take countermeasures

---

[387] Efrony D., Shany Y. *A Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*
[388] *Id.*
[389] *Id.*
[390] *Id.*
[391] *Id.*
[392] *Id.*
[393] *Id.*

has been implemented by the U.S against Russian compounds and entities but not by Saudi Arabia and Qatar, nor by States victims of the WannaCry malware.
The evidence has shown that States are not ready to fully apply the principles of international law to solve cyber disputes. This is explained by political and strategic choices concerning the vulnerabilities to which a State is exposed when it responds to a cyber-attack; or by State's doubts about the applicability of international law principle to the cyberspace.[394] Nonetheless, the principles described by the Tallinn Manual represent a valuable way to resolve disputes on cyber issues among states. Understandably, the resolution of disputes over cyber matters is still new for the majority of States, which have to express their views on how international law applies to cyberspace.[395]

The EU Law of the Cyberspace

My research then moved to the European Union law of the cyberspace. At first, the EU's interest in developing effective cybersecurity measures was closely related to the economic interests of the Union as information and communication technologies are essential in the development of the EU economy and the single market.[396] From the mid-2000s the EU acknowledged that organized crime and terrorism represented a threat for the security and stability of information systems inside the Union and that there was the need of a coordinated response across Member States to address this issue.[397] In my research I've analysed three important legal documents, namely the 'Directive on security of network and information systems' (NIS Directive), the 'General Data Protection Regulation' (GDPR) and the 'Cybersecurity Act'. One aspect in common of these documents is the acknowledgement that cybercrimes represent a threat for the economic relations among the Member States and in the common market.
The 'NIS Directive' recognizes that Member States have different levels of preparation regarding cyber security measures which lead to a fragmented

394 Efrony D., Yuval S. *A Rule Book on the Schelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*
395 Egan B. J. *International Law and Stability in Cyberspace*. Berkeley Journal of International Law
396 Carrapico, H. Barrinha, A. *The EU as a Coherent (Cyber)Security Actor*?
397 *Id.*

approach to the protection of cyberspace across the EU.[398] to face these issues it is essential to exchange information among Member States and establish cooperation and common security requirements for companies which offer operators of essential services and digital service providers.[399] To this end, the directive lays down obligations for MS to adopt a national strategy on the security of network and information systems;[400] proposes the establishment of a Cooperation Group composed by representatives of each Member States; establishes the European Union Agency for Network and Information Security (ENISA)[401] aimed to support the cooperation and the exchange in information among MS[402] and creates a Computer Security Incident Response Teams network (CSIRTs).[403]

The 'GDPR' aims at solving the differences in the level of protection of personal data among European Member States through the harmonisation of the level of protection of the processing of personal data.[404] In fact, the regulation sees the protection of data as a fundamental right.[405] In particular, GDPR seeks to protect EU citizens from privacy and data breaches[406] regulating the collection and the processing of data of individuals and introducing new rules for data controllers and processors in the EU.[407]

The 'Cybersecurity Act' acknowledges that the lack of coordination between European Member States' cybersecurity measures derives from the fact that the law of the cyberspace is characterized by a national approach. As a result, there's the necessity to overcome the national approach of the law of the cyberspace and find coordinated responses and polices shared at the Union level. To this aim, the

---

398 NIS Directive (EU) 2016/1148 of the European Parliament and of the Councile of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Preamble.

399 NIS Directive (EU) 2016/1148 of the European Parliament and of the Councile of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Preamble.

400 NIS Directive, Article 1(a)

401 NIS Directive Preamble.

402 NIS Dirctive, Article 1(b)

403 NIS Directive, Article 1(c)

404 GDPR preamble, paragraph 10

405 GDPR preamble, paragraph 1

406 GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive. https://eugdpr.org/the-regulation/

407 Raul A. C. *The privacy, data, protection and cybersecurity law review*. Fifth Edition. The Law reviews. 2018 Law Business Reserach Ltd.

Cybersecurity Act establishes a European cybersecurity certification scheme for ICT processes, products and services which will be valid across the EU.[408] It strengthens the role of the European Union Agency for Network and Information Security (ENISA) granting it a permanent mandate and conferring the role of European Union agency for cybersecurity.[409] ENISA will improve the capabilities and expertise of EU and national public authorities, will increase the cooperation and exchange in information between EU Member States and EU institutions and ensure the implementation of EU policies in the field of cybersecurity. Finally, ENISA will cooperate with the European Cybersecurity Certification Group (ECCG) composed by representatives of national cybersecurity certification authorities with the aim to facilitate cooperation between national cybersecurity certification authorities and supervise the application of European cybersecurity standards.[410]

Despite the EU's attempts to promote a coordinated response to ensure cybersecurity in the Union, the EU approach to cybersecurity is still not uniform[411] because of lack of coordination between institutions; reluctance of MS in enhancing EU powers in the field of cybersecurity and sharing information; low level of financial resources allocated to cybersecurity programs and lack of coordination among private companies.[412]

The USA Law of the Cyberspace

After the analysis of the EU law of the cyberspace, I moved to the analysis of the United States law of the cyberspace. Here the attacks of 11/9 at the World trade Center and the Pentagon were the starting point for the U.S to improve their national security strategy.[413] Overall, the U.S policy is dominated by the logic of

---

[408] EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency. Council of the EU. Press release. 19/12/2018. https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

[409] *Id.*

[410] Cybersecurity Act. Article 62.

[411] Carrapico H. Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*

[412] *Id.*

[413] Le Cheng J. P., Danesi M. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse.*

military defence and deterrence,[414] and this is reflected also in the approach to cybersecurity, where the U.S allocates a huge amount of financial resources.[415] Moreover, the U.S approach to cybersecurity highlights the importance of cooperation between private and public sectors. I have investigated, through the analysis of some Acts, how the cooperation between these two sectors is put in place in the U.S.

The two first acts I've analysed aim at strengthening the cybersecurity capabilities of the federal government. I first considered the 'Federal Information Security Management Act' (FISMA), which is important for the establishment of information security risk management standards[416] that each governmental agency should apply in order to ensure the security of data of the federal government.[417] Then, the 'National Cybersecurity Protection Act' of 2014 codifies the National Cybersecurity and Communication Integration Center,[418] an interface and a coordinator for the sharing of information related to cybersecurity risks and incidents across the Federal Government.[419]

As the European NIS Directive which establishes the European Union Agency for Network and Information Security (ENISA), the Cybersecurity and Infrastructure Security Agency Act establishes the Cybersecurity and Infrastructure Security Agency (CISA),[420] whose aim is to protect U.S critical infrastructure from physical and cyber threats.[421]

The 'Cybersecurity Enhancement Act' of 2014 is aimed at providing an ongoing, voluntary public-private partnership to improve cybersecurity; strengthen cybersecurity research, development, education and public awareness. Moreover, the act underlines the importance of coordination and consultation between the private sector and public sector's national security agencies and organizations.[422] The final aim is to provide protection of privacy of individuals, security of the

---

414 Bendiek, A. T*ests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*

415 Carrapico H. Barrinha A. *The EU as a Coherent (Cyber)Security Actor?*

416 Federal Information Security Management Act of 2002.

417 Federal Information Security Management Act of 2002. Section 3531.

418 National Cybersecurity Protection Act of 2014. Section 226.

419 *Id.*

420 Cybersecurity and Infrastructure Security Agency Act of 2018

421 CISA https://www.dhs.gov/CISA

422 *Id.*

internet and protect the information processed.[423]

The 'Cybersecurity Information Sharing Act' of 2015 is aimed at improving cybersecurity in the United States through the enhancement of the sharing of information about cybersecurity threats between public and private sectors. To this aim, the act creates a framework for the information sharing between governmental agencies and institutions and private companies. This act is the result of years of discussions on whether the sharing of information could be beneficial to the fight against cyber threats or could result in a further threat for the parties involved.[424] While some see the adoption of the Cybersecurity Act as a success,[425] other have concerns about some provisions of the act dealing with the lack of protection of privacy that could result from the sharing of information between private entities and the government.[426] These concerns raised from the experience of NSA collection of data information that Edward Snowden had revealed in 2013. In fact, although the aim of the Cybersecurity Enhancement Act is to provide for the protection of privacy of individuals, in the U.S there is not a general federal legislation about the protection of data like in the European Union with the GDPR.[427] Despite that, there are several specific laws about data protection enacted both at federal and state level.[428] Understandably, some U.S States are more concerned than others about the protection of privacy and data information and provides for exhaustive legislations on this matter. One example is represented by the State of California, which has always been inclined to adopt laws to protect data information also in relation to the technological development and the presence of a high number of IT companies in this state. In fact, after the European GDPR, the State of California passed the California Consumer Privacy

---

[423] Cybersecurity Enhancement Act of 2014. Section 201

[424] Sullivan & Cromwell. '*Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector*'.

[425] U.S. Chamber of Commerce, U.S. Chamber President Comments on Omnibus Spending Bill (Dec. 16, 2015) https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill

[426] McLaughlin J., '*Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity*', THE INTERCEPT (Dec. 18, 2015) https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/

[427] In any case the Cybersecurity Enhancement Act has entered into force one year after the Snowden's leak.

[428] USA: Data Protection 2019 ICLG.com https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Act, which aims at giving citizens new rights regarding the collection of their personal information.

Data protection in the post-Snowden Era

It has been the lack of a legislation at federal level on the protection of privacy and data information that, following the disclosure of information made by Snowden in 2013 concerning the practices of mass surveillance carried on by the U.S National Security Agency, has led to many debates. The information disclosed have highlighted the lack of adequate legal regulation to protect personal data in the U.S and have proved that the U.S intelligence services had been collecting and analysing data about a large number of people against whom there was no suspect of criminal behaviour.[429] One of the explanation of these practices is represented by the increase in security and mass surveillance programs following the attacks of 9/11 established by U.S 'Patriot Act', aimed at enhancing domestic security against terrorism and surveillance procedures, allowing to intercept wire, oral and electronic communications related to terrorism[430] or computer fraud.[431] This has led the NSA to collect information about every single American citizen, not only the ones suspected of terrorism or having contacts with terrorists.

In Europe, Snowden's revelations led to huge debates and loss of trust towards Europe's closest political ally that had used internet platforms such as Google and Yahoo, to collect information about European citizens, violating the European fundamental right on the protection of privacy.[432] Resolution 2045 of the Council of Europe's Parliamentary Assembly, has affirmed that the practices of mass surveillance represent a threat for fundamental human rights, as the rights to privacy, freedom of information and expression affirmed in the European Convention of Human Rights.[433] Moreover, trust that has been questioned after the disclosure of information by Snowden.[434] To repair the damage, it is to be

---

[429] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance.
[430] Patriot Act. Section 201.
[431] Patriot Act. Section 202.
[432] Bendiek A. *Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.*
[433] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 4
[434] Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 12.

established a legal framework at national and international level aimed at ensuring the protection of human rights, in particular the right to privacy. Furthermore, the Council of Europe has called for national laws to adopt effective security measures concerning the collection of personal data.[435] Also, the European Parliament has adopted a resolution on the U.S NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizen's fundamental rights.[436] It has affirmed that the practices of mass surveillance put in place by the U.S, are in contrast with fundamental rights as the freedom of expression, thought and data protection, affirmed in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights.[437] It follows that the transfer of personal data among EU institution, agencies or MS to the U.S in the absence of adequate protection of these data in respect of the fundamental rights guaranteed to EU citizens, would represent a violation of fundamental rights enshrined in the EU Charter.[438]

In response to the requests of the European Parliament, the European Commission signed the 'Umbrella Agreement' with the U.S. This agreement is aimed to the protection of personal information in relation to the prevention, investigation detection and prosecution of criminal offences.[439] It represents a common data protection framework between the EU and the U.S regarding the exchange of information for law enforcement purposes.[440]

Conclusion

The research has concluded that the law of the cyberspace should focus on the protection of users' data, information shared among them and the guarantee that the cyberspace is always available for everyone.[441] Moreover, it should take in

---

435 Council of Europe Parliamentary Assembly. Resolution 2045 (2015). Mass Surveillance. Paragraph 19.2

436 European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)

437 Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph A.

438 Resolution of 12 march 2014 on electronic mass sureillance of citizens. Paragraph AD.

439 EU-US Umbrella Agreement on data protection. European Parliament. Plenary, 28 November 2016

440 EU-US agreement on personal data protection. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8

441 Kosseff, J. *Defining cybersecurity Law*

consideration the principles of international law applied to the cyberspace by the Tallinn Manual 2.0, which could represent a value added to the regulation of the cyberspace. The gaps in the EU and U.S legislations were useful to outline the focus of the law of the cyberspace which should foster cooperation and sharing of information in all the domains addressed by the EU and U.S legislations, namely among States, institutions, international organizations and the private sector. This shifts the responsibility of security from the state to both the state and the private companies which play an important role in the cyberspace, creating a public-private cooperation between these two sectors.[442] Finally, the law of the cyberspace should protect privacy and data information. This last aspect will represent a new challenge for the law of the cyberspace, which will have to ensure that the processing of data and sharing of information among states, institutions and business, essential for preventing cyber threats to result into cyber-attacks, won't harm the privacy and data of individuals.

[442] Le Cheng J.P & Danesi M. *A sociosemiotic interpretation of cybersecurity in U.S legislative discourse.*