HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

LAW SCHOOL

LL.M. in International and European Law
Specialization: European Law
Academic Year: 2021-2022

MASTER'S OF LAWS DISSERTATION
of
Lampridis Konstantinos

(R. N.: **7340202102009**)

"Legal aspects of cybersecurity in the context of EU"

Supervisor: Kyriakopoulos George, Assistant Professor, NKUA

Examination Board:

a. Kyriakopoulos George, Assistant Professor, NKUA
b. Photini Pazartzis, Professor, NKUA
c. Anastasios Gourgourinis, Assistant Professor, NKUA

Brussels, 28/09/2022

Table of Contents

Table of Abbreviations

CCOCOE	Cooperative Cyber Defence Centre of Excellence
CCPCJ	Commission on Crime Prevention and Criminal Justice
CDMB	Cyber Defense Management Board
CERT	Criminal emergency response teams
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSDP	Common Security and Defence policy
DG	Directorate-General
DSP	Digital Service Providers
EC3	European Cybercrime Center
ECOSOC	European Economic and Social Committee
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
EP	European Parliament
EUCSS	European Union Cyber Security Strategy
EUMS	EU Military Staff
GGE	Group of Governmental Experts
HR	Human rights
ICT	Information Communication Technology
LEA	Law Enforcement Authorities
MS	Member States
NCIA	NATO Communication and Information Agency
NICP	NATO Industry Cyber Partnership
NIS	Network and Information Security
OES	Operators of Essential Services
OEWG	Open-end Ended Working Group
SCO	Shanghai Cooperation Organization
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
NIS	Network and Information Security
UNGA	United Nation General Assembly
UNSC	United Nations Security Council
WTDC	World Telecom Development Conference

Abstract

The research regarding the Legal Concepts of Cybersecurity required first and foremost the complete understanding of the notion of Security from the legal perspective along with Peace and its subsets State Security, Collective Security and Human Security before engaging the main term of Cybersecurity. Peace and Security are analyzed as combination with consideration of Copenhagen School theories and of UN perspective. State security covers the term of state, the significance security holds for it and the right of State sovereignty. Collective security extends to the international sphere and includes the international attempts at resolving conflicts. Human Security refocuses from the safety of the State to the safety of the individual. Continuing to the main term the objects of Cyberattacks such as the function of an information system, or the productivity of the host, or its reputation are discussed. Following that, Cybersecurity is defined from the US, EU and online community perspective . Also, the international response it has collected from international actors and the challenges it faces in adopting a common terminology are specified. Subsequently, the main issue of the dissertation, the legal concepts of Cybersecurity from an EU aspect are entailed. Firstly an introduction and a brief history of EU cybersecurity policies are provided. Following that, EU competence to Cybersecurity legal acts and the activities of EU institutions and more specifically the European Commission, ENISA, European Cybercrime Centre and the Computer Emergency Response Teams (CERTs) are illuminated. Then the Cybersecurity Legal Framework is provided, divided in 3 areas that constitute dimensions of Cybersecurity. First, the Network and Information Security is detailed, including the respective NIS directive. Second, the aspect of Cybercrime ,the Directive on attacks against Information Systems and other relevant EU policies in the same context are provided. Third the area of EU Cyberdefense is depicted and the works of EDA, EUMS and EEAS and EU policies such as EUCSS for Cyberdefense are examined. After the European Chapter, it is the turn of the International Legal Framework on Cybersecurity to be placed under the microscope in comparison with the European one. The UN framework and acts on Cybersecurity are provided. The contribution of UNSC, UNGA, ECOSOC, GGEs and ITU on Cybersecurity aspects are assessed in the light of EU framework. Following that, Budapest Convention under CoE as the international legal framework for Cybercrime is referred and is compared to EU activity in the area. Moreover, NATO stance on cybersecurity and its cooperation with EU is scrutinized. Then the Customary International Law on Cybersecurity, especially in respect of the principle of Due diligence is stipulated and an insight on ICJ jurisprudence regarding the duty to warn, the “no-harm” principle and the non-intervention principle and how the apply to Cyberspace is given.

Methodology

The purpose of this essay is to provide a comparative review of European and International legal frameworks for several concepts of Cybersecurity. The research problem is the establishment of EU Cybersecurity Law and its efficacy and the common ground with International Legal Framework on Cybersecurity .The common denominators in both frameworks , are Network and Information Security, Cybercrime and Cyberdefense in terms of substantive acts and policies and the Institutions of each Framework in the institutionalism perspective. These aforementioned factors are the key elements for the comparison of the two legal systems. The sources used were online resources provided by online databases such as Peace Palace library, Jstor, Hein online and Science direct. The method selected was content analysis, with definitions of terminology used and categorization based on the comparing factors. For the purposes of this essay and for reasons of delimitation three issues were not included as main topics. These are GDPR and Cyberterrorism and Cyberdiplomacy. The former is a subset in the dimension of NIS and the latter are dimensions of Cybersecurity. Regarding citations , I used the OSCOLA citation style as it widely used by law academia.

Introduction

In the international legal spectrum, Security is not a predetermined and preconceived notion. For international law, it holds a controversial and principal position. Despite being derived after an extended process of normalization, and supported after experiments, Security as a concept, does not clearly fall within the typical classification of law. It acts in the boundaries between the purpose of the rule, the value of the legal field or as the legal principle and its vague nature often is attached to the notion of peace.[1]
The legal discourse in respect of security initiated its typological journey from State security and has developed through time to Collective and Human security, embarking into a deepening path. The object of National security is the protection of nation-State, and its interests, downgrading the collective and human angle.[2]In the same sequence, Collective security signifies a shift during which national interests are gradually weakening and, in their place, a collective, universal reaction becomes central.[3]

The question regarding the nature of security and its companion "peace" in respect of their normative function for international law can illuminate a number of obscurities and resolve hierarchical dilemmas in clashes security obligations arising from the UN Charter. Simultaneously the vagueness in definition for the term, leading to an incapability of adopting a universally acclaimed interpretation, surfaces subjective opinions. On their part, these differentiated voices resulted in dividing the State-human security and signified the recourse of security from the primary purpose of international law and actors to a primary norm.[4]

1. Peace and Security

For the purpose of clarifying security, its parallel "Peace" requires to be broken down and both terms should be analyzed comparatively. Often the pair is framed together as maintaining or restoring international peace and security.[5] Peace is traditional recognized as the absence of war and is defined more positively by the UN General Assembly as the state that 'inter-dependence and co-operation to foster human rights, social and economic development, disarmament, protection of the environment and ecosystems and the improvement of the quality of life for all are indispensable elements for the establishment of peaceful societies'.[6] Albeit the general and fluid-like interpretation of peace, the accompanying security is more challenging as the UN has not succeeded in defining it. Security as a concept is infused politically, merely theorized and strongly disputed and argued.[7] At large, security is conceived at the absence of threats both to

---

[1] Robin Geiss and others (eds), *The Oxford Handbook of the International Law of Global Security* (First edition, Oxford University Press 2021). *Chapter: The Concept of Security in International Law*
By Nigel D White, Auden Davies-Bright. Page 19

[2] Hitoshi Nasu, '*Law and Policy for Antarctic Security'* in Allan D Hemmings et al (eds), *Antarctic Security in the Twenty-First Century: Legal and Policy Perspectives* by Routledge 2012 considers that national security from external military attacks and threats was recognized as the ultimate existential purpose "*raison d'être*" of sovereign states.

[3] Donald Rothwell, Karen Scott and Alan Hemmings, 'The Search for "Antarctic Security".' (2012). In Rothwell *Antarctic Security in the Twenty-First Century Legal and Policy Perspectives* by Routledge 2012, states 'traditional view of security defines it in military terms with the primary focus on state protection from threats to national interests', but with the end of the Cold War 'security discourse has expanded beyond the traditional military domain with the proliferation of security agendas, including economic security, environmental security, food security, bio-security, health security and human security.

[4] Geiss and others (n 1). Page 19

[5] Among the activities of UN, see https://www.un.org/en/our-work/maintain-international-peace-and-security.

[6] UNGA Res 46/14 (31 October 1991).

[7] Ramesh Thakur, *The United Nations, Peace and Security: From Collective Security to the Responsibility to Protect* (2nd edn, Cambridge University Press 2016). See Page 77

states, entities and individuals and designates the tools and practices to construct a circumstance of safety, harnessing preventive measures that negates the threats or their manifestation. Internationally, among these are dispute settlement methods neutralizing incidents and strong-arm practices such as sanctions or even military action, with the intention of stabilizing peace.

The empowerment of national security as a priority in State policies, has expanded the general notion of security to encompass and non-military threats, deriving from hazardous sources, such as such as the environmental decay or the upcoming food shortage.[8] The expanded view on security was affirmed by the Summit of UN security Council summit of 1992. Before the 1992, in the previous Summits, the notion of security was delimited in its traditional state-wise sense. At the summit, it was highlighted that the peace period and ceasefire of major military hostilities did not guarantee security and underlined the threat produced by non-military actors in other fields such as the economy or environments, that eventually would expand to peace and security.[9]

According to the referent object theory, developed by *the Copenhagen School*,[10] the object of security has been the state, and further, the nation. For the former the desired result is the maintenance of sovereignty and for the latter, of identity.[11]On a constructivist view, securitizing actors will attempt to construct anything as referent object.[12]. Thus the State would assimilate the role of the referent object of security, but it would encompass though time, self-expanding new security agendas, including the environment. This is a reflection of the aforementioned UNSC opinion regarding the new threats to peace.[13] Despite the expanded concept of the 'threat to the peace' under the UNSC resolution of 1994, the implementation of Article 39 of UN chapter has designated that UN security council made use of its discretionary powers only in times of armed Conflicts.[14] Only the classical security threats such as the proliferation of weapons of mass destruction, terrorism, internal armed conflicts or piracy justified the use of article 39 of UN Charter for UNSC.[15] The extension to other notions of security, such as the human security, which would be analyzed below, has been observed only in the occasions such as the protection of civilians in armed conflicts, or in violation of human rights or even violation of democratic principles.[16]

Besides the inherent inter-subjectivity of the term at hand and the difficulty in ascertaining a normative or a legal sense, its legal effects are unambiguous.[17] In the process of legislation, Security as the aim holds the prominent position. Additionally, in the international legal order, the duet, peace and security, are deemed as the principal aim of the UN Charter and the UN.[18] This is confirmed by the ICJ, which reaffirmed the principal place of security and peace and

[8] Marketa Public, 'Buzan, Waever and De Wilde 1998 Security - A New Framework for Analysis'. See Page 5

[9] UNSC 'Statement by the President on Behalf of the Members of the Council Concerning the Council's Responsibility in the Maintenance of International Peace and Security' (31 January 1992) UN Doc S/23500.

[10] The Copenhagen School of security studies is an academic institute focusing on international relations and the contemporary aspects of security.

[11] Public (n 8). Page 36

[12] ibid.

[13]Hitoshi Nasu, 'Law and Policy for Antarctic Security' in Alan D Hemmings, Donald R Rothwell and Karen N Scott (eds), *Antarctic Security in the Twenty-First Century: Legal and Policy Perspectives* (Routledge 2012). See page 25-6

[14] Nico Krisch, 'Article 39' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary* (Third edition, Oxford University Press 2012).

[15] UNSC Res 1718 (2006) (North Korea), UNSC Res 1737 (2006) (Iran); UNSC Res 1540 (2004) (non-State actors), UNSC Res 748 (1992) (Libya), UNSC Res 1267 (1999) (Taliban), UNSC Res 1333 (2000) (Al-Qaeda), UNSC Res 1373 (2001) (general legislation), UNSC Res 161 (1961), UNSC Res 1816 (2008).

[16] Nico Krish in Simma and others (n 14). In the case of UNSC RES UNSC Res 1296 (2000), UNSC Res 688 (1991) (Kurdish region of Iraq) and UNSC Res 841 (1993) (overthrow of elected government in Haiti)

[17] I Johnstone, 'Security Council Deliberations: The Power of the Better Argument' (2003) 14 European Journal of International Law 437.

[18] UN Charter 1 UNTS XVI art 1(1)

interconnected them as the condition for the attainment of other purposes.[19] While the legal jurisprudence concentrates its attention to Article 2 of UN chapter, which sets forth the principles of sovereignty, equality and non-intervention and the duties on States, of peaceful dispute resolution and abstention of the use of force, Article 1 is of wider significance for international law since it instills the values of UN system.[20]Under Article 1(1) of UN Chapter, security acquires its position within the international legal sphere, as the purpose to be achieved with peaceful means and in compliance with principles of justice and international law.[21] The scope of the article includes the pursuit of peaceful settlement of disputes by the UN, but not the coercive measures adopted so as to respond to peace and security threats.

UN Security action unrestricted by the international rules, is a prevalent denominator in Un Charter. First and foremost the action adopted under Chapter VII by the UNSC supersedes the principle of non-intervention in domestic affairs.[22] Then, the exceptions of self-defense and military action for the preservation of peace again escape from the peaceful resolution of conflicts, required by the Chapter. Therefore, in the scaling between accomplishment of security and honoring of international law, the former surpasses the latter, and especially in case of collective coercive actions prescribed in Chapter VII.[23] As such, the achievement of peace and security is the primordial objective for the UN, and the enforcement of international law is secondary to that. Nevertheless the rest of paragraphs of article 1 establish an extensive and well-adjusted legal framework, able to sustain the Human Rights Protection and the embrace of self-determination of people, along with peace and security.[24] The protection and respect of Human rights and freedoms, fabricated by the Chapter, has been developed in consideration of security and this has permitted the symbiosis at great part of the two contrasting forces. The initial political shackles of actions regarding security after WW2, exchanged with the legal constraints, placed by international law.[25] In order for the term of security to be conceived adequately, an elaboration on its different variants is imperative, besides the dynamic relation between security and peace. The aforementioned State, Collective and Human security, are scrutinized in the following chapters, contributing to the construction of term at hand.

2. State Security

States as theoretical constructs provided society with a structure that regulated humanity in all its vastness. Human existence would be unrecognizable today if the known notion of State was not in effect. The different philosophical and political perspectives pertaining the State and its

[19] 'Certain Expenses of the United Nations' (1962) 151 ICJ REP. (Article 17, paragraph 2, of the Charter) (Advisory Opinion).

[20] Nigel D White, 'The Ties That Bind: The EU, the UN and International Law' (2006) 37 Netherlands Yearbook of International Law <https://nottingham-repository.worktribe.com/index.php/output/1019752/the-ties-that-bind-the-eu-the-un-and-international-law> accessed 28 August 2022.

[21] *Under Art 1(1) of UN Chapter* 'The Purposes of the United Nations are: To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

[22] United Nations, 'Charter of the United Nations' (United Nations 1945) art 2(7).

[23] ibid 2(4),2(7), 51 and 42.

[24] Etc) UN. General Assembly (3rd sess. : 1948-1949 : Paris, 'Universal Declaration of Human Rights' <https://digitallibrary.un.org/record/666853> accessed 29 September 2022; UN General Assembly, 'International Covenant on Economic, Social and Cultural Rights' (United Nations 1966) 993; UN General Assembly, 'International Covenant on Civil and Political Rights' (United Nations 1966) vol 993 <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> accessed 1 September 2022; United Nations (n 22) art 2(7),2(4), 51 and 42.

[25] Gabriël H Oosthuizen, 'Playing the Devil's Advocate: The United Nations Security Council Is Unbound by Law' (1999) 12 Leiden Journal of International Law 549, 549.

origins, bypass their contrasting views and converge to the necessity of the State for human survival. The concept of the State, as the field where mankind developed socially and politicly, became the establishment upon which national and international, legal political and social systems appeared and thrived. This trait of the state justified the significance that security holds, as the State is the binding agent of society and must be protected at all costs. Its paramount importance can be affirmed by the extend of human sacrifices for its continuation. Nevertheless, the notion of State Security, is rarely touched upon, when a threat to its existence approaches. Only rhetoric with intention to provoke the sacrificial spirit of the public, attempts to conceptualize so as to utilize its collective benefit. The ambiguity of the term, enhanced by the omission in defining it, allows interests and policies that exploit it as a political tool and even the international State actors partake in this game.

The opacity in the legal requirements of statehood exacerbates the notion of State Security. These legal criteria are not required to be validated externally, in order for a human Construct to be considered as a State, and this aspect designates the origins of a state. It is a product of human interaction and not a naturally occurring phenomenon.[26] Under the Montevideo Convention, the requirements of permanent population, defined territory, government and capacity to negotiate with other states indicate the internal aspect, the structure and the efficiency of the state as well as its concrete and abstract forms.[27] The state security is related on its abstract form, which is the degree of State control over its territory, via state authorities ,institutions and mechanisms and as it is facilitated, it is subjected to external threats.[28] Hence, State to State interaction is enabled by this abstract form and accordingly external recognition is de facto required for the State existence and sovereignty to be established. The Sovereignty is the element of the abstract form for which security is vital since it depends on external factors. These factors are not of the physical dimension, but they originate from a reality manufactured by society standards and beliefs. Therefore, the survival of the abstract form is of higher importance than the protection of the concrete form, whose constituents used as a tool to maintain the abstract tool. Sovereignty as the right of a State to demand independence from external forces is in the heart of State Security

3. Collective Security

Collective security is the area of international affairs where collective action is performed with the aim to resolve conflicts that might grow in a threatening way for peace.[29]The collective security mechanisms provided by the UN Chapter promote both the peaceful settlement of Disputes and the coercive measures for safeguarding peace against acts for hostility.[30] The peaceful dispute resolution, as mentioned above, is in the priority of the UN and has produced positive results in mitigating conflicts. However, in regards of the latter, the military action under UN umbrella is still implemented partly and has not seen its full effect. Despite the UN military activities of the blue-helmeted peacekeeping forces unfolding around the globe, a UN army under its command and control, with its purpose to provide security by enforcing peace is not in use yet. The forces at fault, for that deviation from the Charter were the Cold-war superpowers, whose inhibitions halted the realization of the provision of forces to the UN under its direct control.[31] The result of this refusal, is the absence of a dependable and capable for imminent deployment

---

[26] Convention on the Rights and Duties of States 165 LNTS 19 (Montevideo Convention) art 3: 'The political existence of the state is independent of recognition by other states.'

[27] Ibid art 1

[28] Geiss and others (n 1). See page 24: The concrete form, the human population and physical landmass, are matters of fact independent of any sociopolitical constructs.

[29] 'Nigel D. White,Collective Security Law(The Library of Essays in International Law), Ashgate, 2003, 589 Pp. Hardback, ISBN 0754622355' (2006) 10 Journal of International Peacekeeping 203.

[30] UN Charter, under Chapter VI and VII

[31] Leland M Goodrich, Edvard Isak Hambro and Anne Patricia Simons, *Charter of the United Nations: Commentary and Documents* (3d and rev. ed edn, Columbia University Press 1969). See page 323

UN army, that safeguards Peace from threats.

In spite of the effective peacekeeping UN action and the fulfillment of purpose of article 1 of the UN Charter, the collective security framework provided by the said text was intended to resolve by coercive military means the threats against peace and negate hostilities.[32] To realize that goal, military enforcement action is required to take place in violation of the sovereignty of the target state. That contradiction, that a State is invaded, which is an act of aggression, in violation of peace, is justified by that endgame of maintaining peace. However, instead of operating the prescribed in the Charter military enforcement model, the UN and its member states opted for a decentralized model of coercive action. Under the said model, a Member State or a league of State is delegated with the task of engaging in military action, following the orders of UNSC authority against an aggressor or a threat to peace. The drawback of this scheme lies with the diminished control that UN security council holds over the execution of the acts of war. That control is reserved only to the authorizing UNSC resolution for the military action.[33] The delegated actor bears the obligation to report with regards to the progress of the mission, but this does not certainly link to an in-depth supervision of the UNSC. Essentially the military operation plan is devised based on the UNSC resolution, but the executive orders and controls are issued by the Member State and due to that a certain amount of discretion is granted. That discretion exceeds the expective collective will of the UNSC.[34]

4. Human Security

In the period following the Cold War, the conversation about Security departed from the State Security and relocated the focus to Human Security. While the threat for State Sovereignty, was seemingly diffused when posed by another enemy State, now the danger of the Individual human is placed in the center of attention.[35] The unfair growth between the developing and developed countries and the exploitation of the former by the colonizing superpowers lead to several hostilities, armed conflicts and human casualties. However these incidents did not place the related Sovereign States or official governments at a risk but instead the people were endangered.[36] The term of Human security was referred for the first time in the UN context by the UNDP in the report of 1994, so as to foster the concern with human life and dignity.[37] Under the same text, it was delineated in contrast to territorial security and elimination of external threats, as the insecurities the ordinary human deals with.[38] This new approach introduced a new correlation of factors that might turn out endangering for human life, in the event of a State crisis. In light of the Copenhagen School theory, the individual person becomes the referent object and security is conceived from a close-range perspective.[39]

A dual effect is the result of that refocusing. On the one hand, the respect and the protection of Human Rights is synchronized with the assurance of security since the human life and dignity is placed in the spotlight. On the other hand, due to Human being the center of protection, the purpose of human survival works adversely to the existential issue of the State. In terms of Human Security, human livelihood cannot be sacrificed in favor of realization of State interests. Therefore an

[32] UN Charter (n 21) art 39.

[33] UNSC Res 678 (1990), authorizing 'necessary measures' against Iraq in response to its invasion of Kuwait

[34] UNSC Res 1973 (2011) (the authorization to take 'necessary measures' to protect civilians in Libya).

[35] Rick Fawn and J Larkins (eds), *International Society after the Cold War. Anarchy and Order Reconsidered* (Macmillan Publishers (incl Palgrave, Picador) 1996).

[36] For instance, incidents such as Genocide in Ruanda of 1994 or the Burundi Genocide of 1972 and 1993

[37] UNDP (United Nations Development Programme), 'Human Development Report 1994' [1994] UNDP (United Nations Development Programme).

[38] As stated in the UNDP, Human security means that people can exercise these choices safely and freely [….] and that they can be relatively confident that the opportunities they have today are not totally lost tomorrow.

[39] See Footnote Nr 10

inherent opposition between Human and State security emits, as the former is threatened by the latter on account of armed conflicts, social policies, economic crisis and the latter by the former, owing to the State being a social construct and having human interaction as its pillar. Nevertheless, the monopoly on power, the use of force and the ability to control security is still held by the state. The State configures the security policy and regulates the allocation of resources in consideration of its self-preservation. [40] An emanation of such precedence is the limitation of Human Rights in a state of emergency, which indicates that dependance of Human life to State's interest.[41]

The recourse from the Security of the State to the individual bears its own risks and dangers. The individual now represents a threat to the State and its citizens as his existence may prove harmful for the States interest. Because of that, they are subjected to unfair treatments and State Abuses. Hence, the purpose of Human Security to inspire protection of the individual, to promote freedom and reduce the control of the State, through the establishment of fair global development and regulatory frameworks, amounted to insecurity for certain groups of people.[42]An instance of that incident is the current refugee crisis and the way States addressed it[43]. As refugees are perceived as a foreign invading for the receiving State, the priority of State security over Human Security is clear. This State action is verified by UNSC resolutions, which legitimize governmental measures and reaffirms the State as the referent object, in the context of the war against Terrorism.

The UNSC instructed States to employ a system of strict control over the granting of refugee status, in order to avoid the exploitation of it by terrorist groups and its affiliates.[44] Amongst the measures adopted are movement restrictions, border walls, fast-tracking procedures for the return of illegal immigrants or their relocation to countries of entrance or to transit countries, detention, deportation and the aggravation of the asylum procedure. The aim of these tactics is to discourage illegitimate asylum seekers from attempting the entrance to foreign countries, having the fight against Terrorism as a higher cause. However, the refused of asylum or similar protection status, end up being submitted to harsh conditions, similar to the stateless person.[45] The purpose Human security, dispersing the threats to individual human and mitigating human insecurity is dissipated and rendered impossible. The displaced, escaping from conflict and persecution in their Home-countries are considered as threats and are stamped as dangerous for stability and social cohesion for developed countries.

5. Cybersecurity

After dwelling into the traditional Security concepts, the notion of Cybersecurity should be illuminated. As mentioned above, Security is of key importance for all states. The technological achievements, improving everyday life were firstly indented to be used in the area of National defense. Despite the initial intentions for the general good, this rapid development of technology and its expansion in all fields and its availability has grown to become hostile for State concerns.[46] Nowadays, cyber-attacks have become a common reference in the news cycle. Cyber-attacks are taking place worldwide everyday causing harm to infrastructures, personal data and the economy.

---

[40] James S Coleman, Boris Frankel and Derek L Phillips, 'Robert Nozick's Anarchy, State, and Utopia' (1976) 3 Theory and Society 437.

[41] 1966 International Covenants on Civil and Political Rights (999 UNTS 171) (ICCPR), Art 4

[42] Commission on Human Security, 'Human Security Now : Protecting and Empowering People /' vii.

[43] Arne Niemann and Natascha Zaun, 'EU Refugee Policies and Politics in Times of Crisis: Theoretical and Empirical Perspectives: EU Refugee Policies in Times of Crisis' (2018) 56 JCMS: Journal of Common Market Studies 3.

[44] UNSC Res 2178 (2014)

[45] Emma Stewart and Gareth Mulvey, 'Seeking Safety beyond Refuge: The Impact of Immigration and Citizenship Policy upon Refugees in the UK' (2014) 40 Journal of Ethnic and Migration Studies 1023.

[46] Ilona Stadnik, 'What Is an International Cybersecurity Regime and How We Can Achieve It' (2017) 11 Masaryk University Journal of Law and Technology 129.

Ranging from the Estonian Cyberattack of 2007[47], to the Sony incident of 2014[48], or the WannaCry ransomware attack[49], to the alleged Russian digital attacks against the Ukrainian government in the Ukrainian War[50], cybersecurity gains more ground in the fields of geopolitics, international economics, security and law[51]. Albeit the awareness of these incidents, should have motivated the international actors or the State authorities, the area of international cybersecurity law and policy is moderately underdeveloped[52].

A.Objects of Cyberattacks

The cause of the legal and legislative inactivity can be linked to difficulty in achieving consensus regarding Cybersecurity and the contents of its terminology. For the purposes of defining the term and its legal extensions, the key threats and cyber risks that impinge cybersecurity should be addressed. Taking under consideration of these harms is required in order to shed light to the goals, limits and scope of laws ensuring cybersecurity.[53]To begin with, a cyber-attack targeting an entity or organization, would harm its internal productivity. The Sony Attack of 2014 paralyzed the systems and operation of the company and large amount of data were deleted. And beyond that, an enormous damage was done to the reputation of the company. The hackers disclosed confidential internal data, such as financial details, documents pertaining to contracts and communications about people of high profile.[54]

Secondly cyber-attacks are mainly executed for financial gain and cause concrete damage to economy. During the WannaCry Ransomware attack, the total economic value the National Health System of UK incurred, amounted to £35 in lost revenues[55] and the potential costs of WannaCry attack were estimated at $4 billion[56]. Besides the economic impact, a Cyberattack may target the State and its Civilians. At the Tallin attack of 2007, the Estonian State's infrastructure was assaulted by a series of Distributed Denial-Of Service attacks, that crippled the websites of all governmental ministries, two banks and several political parties and the parliamentary email server.[57] In addition, a Cyber-Attack can have an emanation in the physical world. The 2015 Russian Cyber-Attack against the Ukrainian power grid caused a six-hour blackout for 230.000 people in the vicinity of Kiev.[58] In 2014 a cyber-attack brought massive damage to the system of a German Steel mill. The German authorities reported that the perpetrators used "advanced social

[47] In 2007, a series of cyberattacks targeted websites of Estonian private public entities, including Estonian parliament, banks, ministries, newspapers and broadcasters, due the country's dispute with Russia over the move of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn.

[48] Jeff Kosseff, 'Defining Cybersecurity Law' 103 IOWA LAW REVIEW 47. In 2014 Sony faced a multiple Cyber-Attacks, and the breach damaged Sony's Internal productivity, compromised employee privacy, caused a public relations nightmare, had concrete financial costs

[49] Lawrence J Trautman and Peter C Ormerod, 'Wannacry, Ransomware, and the Emerging Threat to Corporations' (2018) 86 Tennessee Law Review 503.

[50] PRZETACZNIK Jakub, 'Russia's War on Ukraine: Timeline of Cyber-Attacks' (European Parliamentary Research Service 2022) <https://policycommons.net/artifacts/2476881/russias-war-on-ukraine/>.

[51] Scott Shackelford, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' [2016] SSRN Electronic Journal.

[52] ibid.

[53] Kosseff (n 48). See page 989

[54] Gabriel Sanchez, 'Case Study: Critical Controls That Sony Should Have Implemented' [2015] SANS INSTITUTE <https://www.sans.org/white-papers/36022/> accessed 4 September 2022.

[55] S Ghafur and others, 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS' (2019) 2 npj Digital Medicine 98.

[56] Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 AJIL Unbound 202. See page 206

[57] Stephen Herzog, 'Revisiting the Estonian Cyber Attacks' (2011) 4 Journal of Strategic Security 49.

[58] Julia E Sullivan and Dmitriy Kamensky, 'How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid' (2017) 30 The Electricity Journal 30.

engineering" causing failure in the shutting down of a blast furnace and damaging severely the plant.[59]Lastly, the repercussions of a cyber-attackers in the international field should be elucidated. The Sony Attack was attributed by US government to North Korea as retaliation for the release of the *Interview,* a fictional film regarding an attempted assassination of Kim Jong Un. After that, the US imposed sanctions against North Korea.[60]

B.Definitions of Cybersecurity

After highlighting the potential harms a Cyber-attack may have to Cybersecurity, the proposed definitions by the legal community can have a greater degree of understanding. The US department of Homeland security considers cybersecurity as 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. Additionally, an extended definition is provided, including the strategy, policy and standards of security and operations in cyberspace and the whole range of threat and vulnerability reduction, cyber-deterrence, the international engagement, the incident response, resilience and recovery policies. The corresponding cyber activities such as cyber military and intelligence missions were also entailed within.[61]

On the other side of the ocean, the European Union has developed its own conception of Cybersecurity. Under the *NIS Directive*, Cybersecurity is defined as the "ability of network and information systems to resist" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.[62] Moreover, the same term is defined from a different perspective under the Digital Market Glossary. The vocal point are the action and the processes that promote cybersecurity. Pursuant to that, Cybersecurity engulfs the precautionary and suppressive acts for the protection of Cyber-Space, against dangers that are connected or threaten networks and infrastructure of information systems and against Cybercrime. Further, Cybersecurity is defined with the angle of protection for cyber environment, organization and users of cyberspace. It consists of the tools, policies, security schemes and defenses, as well as the activities and risk management approaches to ensure the observance of Security in the cyber-Domain.[63]

The online Community has its own premise regarding the notion of Cybersecurity. It employs a common trait with the EU directive as it follows the strand of the process for the protection of assets that hold information against infiltration and loss. In the *Cybrary* glossary, the term emphases the broad knowledge over dangers in cyberspace, such as viruses, malware, trojan horses and other malicious items and the stresses the identity, risk and incident management as the core triangle of Cybersecurity for enterprises and entities.[64] In addition, the Internet Society

[59] L Vissagio, 'Hacking the Infrastructure Cyber-Attack, Physical Damage'.
[60] Kosseff (n 48). See page 992
[61] 'DHS Lexicon | Homeland Security' <https://www.dhs.gov/publication/dhs-lexicon> accessed 4 September 2022.
[62] 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 2016.
[63] TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, 'SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Overview of Cybersecurity'. The ITU defines cybersecurity as "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 assets".
[64] Cybrary is a cybersecurity platform that offers cybersecurity workforce education and training services for IT professionals. The full quote on its glossary for cybersecurity: Cyber Security are the processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires

considers that Cybersecurity is a catchword term encompassing a vast number of security incidents, technical concerns and legal interventions. It is stressed that as the term attracts attention, the adoption of a common understanding for Cybersecurity is necessary in order to progress the discourse on its regulation.[65]

As many other areas of International Law and Technology, Cybersecurity is shrouded with vagueness and lacks consensus in terms of definitions and contents. The term in question and its familiar one's such as 'information security', 'cybersecurity' ,'cyber-warfare' and 'cyber-surveillance' are not set forth in a binding international legal text of world-wide acceptance.

C. International Response and Challenges to Cybersecurity

The divergences regarding the notion of Cybersecurity have not halted the United Nations organization from attempting to regulate the issue and clarify the term. Amongst its institutions, the UNGA has adopted from early on, resolutions prompting the UN member states to recognize the existence of Cyberthreats and provide the Secretary-General with information as regards the expediency in the development of principles capable of improving security of global network and information systems and combating Cyberterrorism and Cybercrime.[66] In consideration of the broad language of Resolution 53/70, the intense disagreement regarding the issue is reflected and especially between the permanent members of UNSC. On the one hand, Russia introduced a proposal on a Cyber-Space Treaty, similar to Chemical Weapons Convention that would exploit the dual use of Information systems.[67] USA on the contrary, after the efficacy of the Stuxnet worm Cyber-attack, opposed and differed its approach.[68]

Cyberspace, owing to its complexity and multifaceted dimension cannot be subjected easily to a treaty or another legal regulatory text. Since the cyber-domain is a modern setting for the Freedom of Information to elaborate and it may pose a threat to security simultaneously, the consensus required for the regulation of it is challenging for the UN. After determination of existing and potential cyberthreats, UNGA, advised Member-States to develop security strategies for the protection of the free flow of information and urged them to pattern after the international security frameworks pursuing the integrity of global ICT systems. The discussion turned to works of the Group of Governmental Experts, who were called upon to develop the aforementioned security schemes and other measures for the security of information.[69] The Report of the GGE, despite the benign intentions, did not transform into a normative framework for the use of cyberspace[70]

In response to the UNGA persistent request for policy making in the field of Cybersecurity, states such as US, UK and Australia, claimed that international law as a body of law, is adequate enough to function as a regulatory framework for the protection of information security against threats arising from state and non-state actors.[71] The same opinion is adopted by the UN Institute for disarmament Research in regard to the legal frameworks for Cyber-War. *Jus ad bellum and Jus in Bello*, areas well-constrained by an internationally acclaimed framework, can be

---

extensive knowledge of the possible threats such as Virus or such other malicious objects. Identity management, risk management and incident management form the crux of cyber security strategies of an organization.

[65] The Internet Society (ISOC) is a nonprofit organization, originating from the US, founded in 1992 with local chapters around the world. Its mission is "to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world via assuming a consultive role.

[66] UNGA, 'Resolution 53/70' (United Nations 1999).

[67] Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 Journal of Conflict and Security Law 187. See in Pages 205-206

[68] James P Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War' (2011) 53 Survival 23. Page 31

[69] UNGA, 'Resolution 65/41' (United Nations 2010).

[70] UNGA GGE, 'Report on UNGA Res 68/243' (United Nations 2013).

[71] UNODA, 'Disarmament Study Series: No. 33 – Developments in the Field of Information and Telecommunication in the Context of International Security' (United Nations 2011).

implemented in Cyberspace regulating Cyberwar. This is an indication, proving that the Cyberwarfare, a subsection of Cybersecurity, does not fall into a legal vacuum but rather is subjected to the already established rules and procedures.[72] However, this approach mistakenly overlooks the non-kinetic cyber-operation and cyber-criminal activities as cyberthreats, which as a notion does not comprise only Cyber-warfare.[73]

The major challenge in the legalization for Cybersecurity is the conversion of contemporary threats in cyber domain into legal notions, principles, values and rules, that would connect and collectively structure a legal framework. Under the said system, public entities, emanations in the private sector and the individual would be able to address the issue of threats raised by new technologies. Already established international norms and their principles such as arms control law or human rights law can find application in the Cyber-threats or incidents. The Tallin manual, drafted by an international group of experts in 2017 elaborates on such use of international law in the cyber-domain.[74] Nevertheless, in event of cyberattacks against States, the legal frameworks regulating such offences are a source for deliberations as to whether international principles such as non-intervention[75] and sovereignty[76] find effect in the cyber-domain due to its multinational dimension. Last but not least, the principle of due diligence in international law should be illuminated, so as to recognize the obligation of a state to prevent cyberattacks from its ground against other states and the margin of responsibility it holds.[77]

Although the international community cannot find common ground in defining the term at hand and unite in agreeing on a global regulatory framework for Cybersecurity in all its aspects, several international actors have taken steps of diverse levels in providing rules or other solutions to the subject at hand. Owing to the fact that the Internet was born in America, USA were the pioneers in adopting cybersecurity measures and rules, that have been imitated by other States and functioned as a blueprint for their own rules and policies.[78] Simultaneously assumed the leading position in the drafting of Tallin 1 and 2 Manual influencing the establishment of the rules governing Cyberspace. Moreover, under the auspices of the African Union, the *Malabo Convention*[79] is the legal framework for Data protection and Cybersecurity, under which the Member States of AU are obliged to adopt legal, policy and regulatory acts in order combat cybercrime and indorse cybersecurity.[80]

Turning to the east, the Shanghai Cooperation Organization, adopted the *Agreement on Cooperation in the Field of International Information Security* of 2010, which, inter alia, elaborated on the main threats of Information security and on the main areas of cooperation in the same sector between the members of the SCO.[81] Not unexpectedly, the one that holds the prime

---

[72] N Melzer and United Nations Institute for Disarmament Research, *Cyberwarfare and International Law* (UNIDIR 2011). Page 36

[73] Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—a Critical First Assessment of the New Tallinn Manual' (2013) 18 Journal of Conflict and Security Law 331.

[74] Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017).

[75] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 211. Page 221-223

[76] Phil Spector, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017) 111 AJIL Unbound 219.

[77] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 Journal of Conflict and Security Law 429. Pages: 431-433

[78] Mary Manjikian, 'The United States: A Declining Hegemon in Cyberspace?', *Routledge Companion to Global Cyber-Security Strategy* (Routledge 2021). Pages:463-467

[79] Convention on Cyber Security and Personal Data Protection 2014.

[80] Uchenna Jerome Orji, 'The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability' (2018) 12 Masaryk University Journal of Law and Technology 91.

[81] Sarah McKune and Shazeda Ahmed, 'Authoritarian Practices in the Digital Age| The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda' (2018) 12 International Journal of Communication 21. Page 3841-3842

position in configurating a Cybersecurity legal framework is the European Union. Since the turn[82] of the 21st century up to 2022[83], EU has exhibited exemplary and increasing legislative and policy action in the area of Cybersecurity.

The following part of the essay will elaborate on the EU Cybersecurity legal scheme. Firstly, the contribution of EU institutions in developing Cybersecurity policy will be examined. Second in discussion is the substantive part of EU cybersecurity law, id est the regulations and directives governing dimensions of cybersecurity. Next in line is the soft law items and policies of EU on the subject, whereas the new Cybersecurity act will be scrutinized. Finally, the issues of securitization of Cyberspace and EU rules on IoT would be illuminated.

Cybersecurity under EU Law

The European Union holds a well-structured arsenal of legal instruments that deals with various facets of cybersecurity, extending from electronic communication laws, data protection regulations, network and information security legislation, cooperation mechanisms against cybercrime to an advisory position on the coordination to the response towards large scale cyber incidents. However, this state cannot be perceived as predictable. EU treaties, the primary EU law, does not set forth cybersecurity as an area for EU to regulate. Despite being security the initial reason behind the construction of European Communities in the 1950s, EU main activity has been largely economic and financial in nature.[84]

Nowadays there has been a recourse on that route. Since 2013, cybersecurity is of prime importance in the EU agenda. The EU first pure legal act in the area of cybersecurity is the NIS Directive, on a common level of security of network and information systems[85]. Recently, another related act was adopted, the EU cybersecurity act in 2019, which intends to restructure various Cybersecurity policies and rebranded the European Union Agency for Network and Information Security (ENISA) to the European Agency for Cybersecurity.[86] Additionally, a proposal on a revised Directive on Security of network and information Systems has been adopted by the EC and has taken the road towards legislation.[87]

At the same time, numerous policies, reports, announcements take place at European level regarding cybersecurity. The 2013 Cybersecurity Strategy(EUCSS), updated in 2017[88], the council decisions of 2015 regarding Cyber-diplomacy[89], the 2020 EU Security Union Strategy which emphasized the critical infrastructure protection and resilience and introduced the establishment

---

[82] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime 2000.

[83] The latest is the new Cybersecurity Act that is still in deliberations, in order to be adopted.

[84] Ramses A Wessel, 'European Law and Cyberspace', *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) <http://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00036.xml> accessed 9 September 2022.

[85] 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 (n 62).

[86] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2019 (OJ L).

[87] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 2020.

[88] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013.

[89] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe 2015.

of a joint Cyber Unit[90], the 2020 New Cybersecurity Strategy[91] and lastly the two new EC proposals[92] on adopting regulations regarding the upgrade of Cybersecurity specifications for EU institutions and EU organizations and the intergovemental declaration for the establishment of a new emergency fund for Cybersecurity[93] clearly indicate an increasing activity in the area, and a turn in the priorities of the Union.

In spite of all the aforementioned activity amongst the Institutions that partake in the policy making and legislative procedures, there is lack of consistent terminology amidst the Union regarding Cybersecurity. In the 2013 EUCSS the notion was defined broadly aiming at preserving the availability, integrity of networks and information systems and the data preserved within.[94] Contrast to that wide approach, the 2019 Cybersecurity act focuses on the resilience of networks to potential attacks and the capacity of defending to such attacks.[95] This deficit in a commonly accepted term, as it has previously discussed in the introduction, causes difficulties and controversies in the adoption of legal acts. Even worse, in the EU framework and due to the principle of conferral of powers, there is no express competence conferred to the EU.

That lack of express competence of EU in the area of cybersecurity, has forced the EU institutions either to legislate cyber-related issues in the name of other areas where the EU can legislate exclusively or adopt soft-law and coordination measures. This fragmentary resort hardens the understanding of Cybersecurity and the allocation of tasks and responsibilities[96]. Additionally, this incoherent conception of the notion and its contents, permits the production of different approaches adjusted to the national capabilities' directories. This creates a structural danger to the EU, that if enhanced by national security narratives and entangled in the sovereignty claims between EU Member States could renter the EU powerless[97]. The multitude of actors participating in the EU system, id est, the various EU institutions, bodies, agencies and the MS, without having a clear notion for the term at hand and on account of their different origins and targets, might adopt measures in terms of cybersecurity that can be even at odds with each other.[98]

The notion of Cybersecurity for EU has been through several phases as to reach its recent and final conception. At the initial stage, in the start of 2000's the economic aspect of cybersecurity was under the microscope. As communication and information became central in the development

[90] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy 2020.

[91] 'New EU Cybersecurity Strategy' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> accessed 9 September 2022.

[92] 'New Rules to Boost Cybersecurity and Information Security' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1866> accessed 9 September 2022.

[93] Luca Bertuzzi, 'EU Countries to Call for the Establishment of a Cybersecurity Emergency Fund' (*www.euractiv.com*, 8 March 2022) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-call-for-the-establishment-of-a-cybersecurity-emergency-fund/> accessed 9 September 2022.

[94] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88).

[95] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[96] Jed Odermatt, 'The European Union as a Cybersecurity Actor' [2018] Research Handbook on the EU's Common Foreign and Security Policy 354. Page 356

[97] Krzysztof Feliks Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35 Contemporary Security Policy 468, 470.

[98] Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity* (Springer International Publishing 2020).

of society, attention to safe use of computer system was emphasized[99]. During these early stages Cybersecurity regulations had two main concerns, firstly the privacy and data protection[100] and secondly the completion of the single market. Though the creation of ENISA brought up a dispute within EU, that reached even Court of Justice of the European Union (CJEU).[101] The court found that the legal act in dispute indented at the completion of the internal market in the area of electronic communications. Essentially, it affirmed that the primary concern was data security and that the rules on network and information security in the legal acts were rather subsidiary, serving the internal market rather than protecting from harm arising from the use of computer systems. These legal acts set out general requirement for information and network security but their scope was the telecommunication sector, personal data protection and e-signatures.

The turning point was the Estonian Attack of 2007 and cybersecurity was framed as a security issue in the report on the implementation of the European Security Strategy of 2008 submitted in Council of European Union.[102]From there and after the adoption of the New Cybersecurity strategy of 2013, cybersecurity has upgraded to an integral part of EU policies.[103] Under the said document, cybersecurity was evaluated in a comprehensive basis and the scope of operations of the relating activities relating would elaborate in 2 levels, national and European and within different legal frameworks comprising network and information security, law enforcement and defense.[104] Further, the strategy promulgated the priorities of cybersecurity within a framework of 6 directions, namely accomplishing cyber-resilience, mitigating cybercrime, promoting cyber-defense and defensive capabilities in cyber-domain under the Common Security and Defence policy(CSDP), cultivate the industrial and technological assets and reserves for improving Cybersecurity and shape the international Cyberspace policy for EU, while respecting and reflecting fundamental EU values and principles.[105] Again, there is an economic background to the conception of cybersecurity in the 2013 Strategy, and the possible harms that derive from cyber-threats were implied, id est financial loses, decrease in productivity, immaterial loses such as a decrease in trust in e-services and physical damage to citizens.[106]

The shift in Cybersecurity is finalized with the new Cybersecurity strategy of 2017[107] which led to the adoption of Regulation (EU) 2019/881 and the following upgrade of ENISA's mandate and the adoption of EU Certification framework. Further, the most recent act, is the New Cybersecurity package, consisting of a new Cybersecurity Strategy and two proposals, the first being the new NIS directive and the second being a directive on the resilience of critical entities[108]. This contemporary conception of cybersecurity departs from the comprehensive framework of the

---

[99] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach 2001.

[100] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector 1997.

[101] *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union* [2006] ECJ Case C-217/04. Par 59-60

[102] Javier Solana, 'Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -' (EEAS 2008).

[103] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88).

[104] ibid 2. Page 17

[105] Odermatt (n 96). Page 361-362

[106] Christopher Whyte, 'European Union: Policy, Cohesion, and Supranational Experiences with Cybersecurity', *Routledge Companion to Global Cyber-Security Strategy* (Routledge 2021). Page 204

[107] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU 2017.

[108] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (n 87); Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities 2020.

previous stage and leans towards a more integrated one, where the economic, political and strategic dangers of cybersecurity interplay, demanding the same levels of concern and threaten all levels of government, economy and society. The five areas, that Cybersecurity expanded under the previous 2013 Cybersecurity Strategy are now contemplated by policies and legal acts in secondary fields, such as consumer protection, product liability, education, trade and investment. This approach, initially reactive to traditional areas that were susceptible to a cyber-attack, now gains a new direction to a more proactive trajectory. The economic concern is still on going along with the impact of the demise in the functioning of computer systems, but the context of Cybersecurity has evolved, entailing concerns to political autonomy, territorial integrity and to the ability of states to maintain rule of law.[109]
To sum up, in order to comprehend the context of Cybersecurity and elaborate on the premise that European Union Institutions and MS share when adopting Cybersecurity laws and the purpose they intend to achieve, it is necessary to identify the competence of EU and the role of its institutions in connection with Cybersecurity. Afterwards, the related legal acts will be broken down, on basis of 3 main features of Cybersecurity: network and information security, Cybercrime and Cyber-defense.

1. European Institutional Approach to Cybersecurity

There is no clear reference to Cybersecurity in the EU treaties. Under articles 3, 4 and 6 of TFEU, which set out the EU exclusive, shared and supporting competences, the issue of Security in Cyber-domain can only be summoned in connection with other related fields.[110]The principle of conferral, which governs the division of competences between EU institutions and MS, forbid EU from exercising its legislative powers in areas that exceed its conferred under EU primary law, competences.[111] As such there an absence of explicit legal basis for EU policy in that area. Despite this profound lack of competence in this area, EU institutions affirm the Union's position to regulate Cybersecurity and justify that to the scope of the policies and the tools, structures and capabilities at its disposal.[112] Whereas MS hold the reins in National security, as it is within the core of State sovereignty, the scale and the cross-border nature of Cyber-attacks show just cause in the provision of incentives and support to MS for the development of Cybersecurity capacity in national and European level.

Notwithstanding of that reasoning, from a purely legal perspective, there is no expressed transfer of competence in Cybersecurity even after the 2009 treaty update. One could estimate that this striking absence is done purposely. On account of the inherent cross-border nature of Cybersecurity, a cooperation between EU and MS or the conferral of powers might not be sufficient in addressing cybersecurity challenges, as the involved actors are multiple and exceed European borders.[113] Additionally, similarly to other international organizations, the EU in order to function, requires to be equipped with the competent powers both internally and externally, id est in its international relations with other States and Organizations of global scale. Given the division of competences and the aforementioned principle the Union is left with two choices as regards to Cybersecurity acts. Either the adopting act should relate with fields where the EU is

[109] Zsolt Bederna and Zoltan Rajnai, 'Analysis of the Cybersecurity Ecosystem in the European Union' (2022) 3 International Cybersecurity Law Review 35, 40.
[110] Consolidated version of the Treaty on the Functioning of the European Union 2012 (OJ C). Articles 3,4 and 6
[111] ibid 5.
[112] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (n 107).
[113] Wessel (n 84) Page 499.

competent or the only recourse is soft law as incentive for action on the part of the MS or other actors.[114]

The first route is mainly selected by the EU. EU policies that are devised with the intention of being turned into legal acts, are linked to existing EU competences. The economic aspect of Cyber-security is mostly exploited as a legal basis and the potential economic harm that Cyberthreats and the related attacks may impose to EU is the entry point for the adoption of legal acts. Precisely, EU policies in the field aim at ensuring the functioning of the Internal Market.[115] Having as a legal basis article 114 of Treaty on the functioning of the European Union (TFEU), the NIS directive[116] was adopted. Since network and information systems contribute significantly to the execution of the cross-border movement of goods, people and services, a disturbance in the functioning of these systems in one MS would have a spill-over effect in other Member states and eventually disrupt the internal market.[117] In a similar manner, the Directive on combating the sexual exploitation of children online and child pornography is based in articles 82(2) and 83(1) of TFEU and the area of judicial cooperation in criminal matters in the Union.[118] Cybercrime and the integrity of critical infrastructure both have a legal basis for the related adopted acts in the area of Freedom of Freedom, Security and Justice. These legal acts being internal must be subjected in a procedure of linkage with their external manifestations in regards of the relevant EU policy.[119]

This connection of EU actions in cybersecurity with EU competences is confirmed by the European parliament in its resolution of 23.11.2016, which emphasized that due to conflicts that take place physically and in cyberspace, cybersecurity and cyber-defense should be prioritized as core elements of CSDP and fully incorporate in all EU policies.[120] Notwithstanding that required link with existing competences, a common approach to cybersecurity concerns has surfaced across those different pillars. The EUCSS and other policy documents serve as binding agent of these interconnections between cybersecurity and the connecting competence and set the main priorities for action. For instance, EU institutions and the MS must abide by the Charter of Fundamental Rights of the European Union, which after the Lisbon Treaty has risen to primary EU law and ensure respect to fundamental rights and values in the Union. Under the EUCSS, EU and MS must sustain and contribute in a global, open and secure internet.[121] As such, a balancing must be made between enhancement of cyber resilience within EU and the protection of fundamental rights such as privacy or freedom of speech. In addition, the EUCSS entail not only the protection of fundamental rights internally but also the external aspect of the engagement of cyber issues by the EU, in which the EU values of freedom, democracy, equality and the rule of law must be protected. Therefore not only the principal values of EU, including the protection of HR is attained within

[114] cf Ramses A Wessel and Jed Odermatt, 'The European Union's Engagement with Other International Institutions' [2019] Research Handbook on the European Union and International Organizations 2, 11–13.
[115] Odermatt (n 96) 361.
[116] 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 (n 62).
[117] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union 2013. Point 3.1
[118] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011.
[119] Ramses A Wessel, 'Towards EU Cybersecurity Law: Regulating a New Policy Field' [2015] Research Handbook on International Law and Cyberspace 403. Page 404
[120] European Parliament resolution of 23 November 2016 on the implementation of the Common Security and Defence Policy (based on the Annual Report from the Council to the European Parliament on the Common Foreign and Security Policy) (2016/2067(INI)) 2016.
[121] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88).

the EU but also externally and simultaneously with the legal counter measures against cyberthreats.[122]

This practice in adopting legal acts in the area of Cybersecurity, outside of EU conferred competence, does not come without risk. Rather the danger of fragmentation and inconsistency is present, owing to the participation of multiple actors and the convergence of their distinct, often adverse preferences and procedures. Specifically, the process of structuring the EU cybersecurity policy is streamlined with the involvement of the EU institutions, the MS and the private actors such as the service providers and advocates of the tech industry. Thus the requirements of consistency and effectiveness, set in articles 13 of Treaty of the European Union, are not attained with certainty.[123] Rather, Cybersecurity as a field of policy shapes an excellent example of amalgamation of different competences, incentives and interests both vertically and horizontally.[124] The vertical axis relates to consistency and cohesion of cybersecurity policies ,agencies and instruments at EU level among EU institutions, Member states and private actors while the vertical axis deals with the coordination and cooperation between the same actors, at the same level.[125]

In terms of EU, the institutional development dealing with cyber issues has focused more on coordination rather the sheer acquisition of new capacities. Beginning with the establishment of ENISA in 2004[126], the cohesion is shaped in the form of an approved collection of mission objectives and institutional enhancements as a necessity towards the wide protection of Europe's digital society. In the horizontal level, EU approach was to construct the necessary institutional system and network including the main Institutions, agencies as well the upgrade of the latter to a main one[127] ,with the purpose of securing European Society online. On behalf of the MS, the obligation to harmonize cyber policy instruments and national laws is assumed, with the reflective example of cybercrime, as well as the task to secure cooperation with the private sector, realizing the coordinative incentive promoted at a central level. An emanation of the aforementioned attempt of the MS, is the creation of multiple specialized agencies, from ENISA to a Europol subset responsible for cyber-criminal investigation and the respective Computer Emergency Response Teams (CERT)[128]. Their intention is to achieve a high level of coordination between the EU central authorities and the ones in the MS.

In the vertical level, EU intends to ensure a coordination in the understanding of the scope and the objectives of the European Cyber mission. This is attained by promoting awareness of cybersecurity issues and in the development of cybersecurity standards, the last improved by the contribution to the horizontal level. The progress in Europeanization of Cyber policies is visible by the perception in Society that cybercrime is on the rise, by the massive usage of internet and digital services and the international response to cyber-attacks such as the 2007 attack on Estonia. In spite the expanding Europeanization, Cybersecurity has not fully externalized and is still

[122] ibid. Page 15

[123] Consolidated version of the Treaty on European Union 2012 (OJ C). Article 13 : The Union shall have an institutional framework which shall aim to promote its values, advance its objectives, serve its interests, those of its citizens and those of the Member States, and ensure the consistency, effectiveness and continuity of its policies and actions……

[124] Wessel (n 84) 494.

[125] Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 JCMS: Journal of Common Market Studies 1254, 1257.

[126] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) 2004 (OJ L).

[127] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[128] Carrapico and Barrinha (n 125) 1261.

deployed mainly at national level[129]. EU officials consistently argue of the complexity and the cross-border nature of Cybersecurity and at the same time slate the low level of Cybersecurity in several MS.
There are coordination issues between MS and EU institutions, common to the horizontal level as well. In the level between National Authorities and the private sector, similar coordination issues are raised. The number of public private partnerships in the Cybersecurity sector is high, contrary to the level of cooperation which fluctuates significantly and the context of cooperation, such as information sharing is unclear. Also the long identified and still unsolved problem of conflict of interest between the private and public sector exacerbates Cybersecurity at the regional level. The impetus of private interest is the profit and efficiency whereas the priority of the public sector is security[130]. This divergence can be seen in the area of Cybersecurity where the public-private cooperation is the majority of cases in the EU.[131]The fragmentation in both levels, leads to question the accomplishment of the ambitious "resilience though regulation", that has been declared as a goal in multiple EU published document.[132]

2. European Union institutions on Cybersecurity

In an institutional sense, the European Union has been establishing a comprehensive institutional framework, in charge of ensuring Cybersecurity and all its aspects, from the eve of the millennium. During the past twenty years, a robust and diverse network of agencies has been developed, other autonomous such as ENISA, other as a subset to EU main institutions, that have undertaken the task to deal with the multiple issues and goals in the Cybersecurity policies.[133] The institutions comprise the European Defence Agency (EDA), which will be analyzed in a later chapter, Directorate-General(DG) of Migration and Home Affairs and the Directorate-General of Communications, Content and Technology, both subdivision of the EC, the European Network and Information Security Agency(ENISA), the EU Cybercrime Center(EC3), the Computer Emergency Response Teams(CERTS).

A. European Commission role on Cybersecurity

In the Cybersecurity field and the IT field in general, the EC has significantly contributed to establishing the environment upon which the related policies are constructed and to rallying support for future activities. [134] As the main administrative body and the executive arm of EU, is composed of 56 Directorates-General and has whole range of policy units and task forces, empowered with the task of policy making. In order for a proposal to reach the legislative phase, the policy negotiation travels through the different divisions of the Directorate, where the proposal is drafted and then to the EC main body. Then the executive body of the EC, produces the official legislative proposal and furnishes the legislative institutions, the European Parliament and the Council of European Union with it.

---

[129] Thomas Renard, 'The Rise of Cyber Diplomacy: The EU, Its Strategic Partners and Cybersecurity' [2014] European Strategic Partnership Observatory Working Paper 7, 13.
[130] Myriam Dunn-Cavelty and Manuel Suter, 'Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection' (2009) 2 International Journal of Critical Infrastructure Protection 179, 3.
[131] Raphael Bossong and Ben Wagner, 'A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU' (2017) 67 Crime, Law and Social Change 265. Page 266
[132] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy (n 90). Being the latest one
[133] Whyte (n 106).Page 206
[134] Laura Cram, 'The European Commission as a Multi-organization: Social Policy and IT Policy in the EU' (1994) 1 Journal of European Public Policy 195. Page 198

Amongst its departments, the DG for Migration and Home Affairs and the DG for Communications, Content and Technology, have assisted severely into Cybersecurity Policy Making. The former, amongst the items listed in its works, is tasked with various cybercrime missions. It shaped the 2020-2025 European Union Security Strategy, whereas the EC defines a new way towards internal security, and promotes the adoption of actions, tools and measures in areas which inter alia include Cybercrime and security in the digital world.[135]
The latter, also known as DG Connect, is in charge of tele-communications regulation, promoting the approval of ICT in society for economic and social benefits and regulatory policy governing the ICT market as well as EU investment in research and development of critical digital technologies, entailing Artificial Intelligence, 5g networks, Blockchain technology and Cryptocurrency.[136] Its subdivision, the directorate of Digital Society, Trust and Cybersecurity, assumes a supportive role in leadership in Cybersecurity, Digital privacy, Digital Trust Policy, Legislation and innovation.[137] Furthermore, it distributes the parent-DG responsibility for ENISA, it represents the DG in the CERT-EU board and provides the DG response to Cyber incidents.
The EC international role has impacted majorly Cybersecurity. As the representative of the Union in international agreements and organizations, except in areas of Common Foreign and Security Policy, has participated in discussions and negotiations regarding Cybersecurity. For instance in the UN-organized World summit on the Information Society in Tunis of 2005, the EU via EC, advocated for the availability, reliability and security of networks and information.[138] This enhanced the debate regarding the fight against cybercrime and spam, when at the same time it ensured privacy and freedom of expression. Hence, assisted by these two departments, the EC has asserted a leadership role in shaping Cyber policy and Cybersecurity legal acts.

B. European Agency on Cybersecurity

Back in 2004, the European Network and Information Security Agency, now called the European Agency on Cybersecurity, was established, in order to improve EU and MS cyber-capabilities and prevent Network and Information Security (NIS) problems. Its original mandate was to ensure a high degree of NIS and assist in the development of a cybersecurity culture within EU. That last task elevated the ENISA to the centre of Cybersecurity expertise for MS where experiences, best practices and guidelines are published, so as to MS can implement them to national Cybersecurity strategies (NCSS).[139] Located in Crete and in Athens, Greece, ENISA served as an intermediary between the EC and the MS and the private sector. Secure and effective network and information systems are recognized to be essential for the functioning of EU's internal market. As such the presence of a Cybersecurity agency was deemed of high importance.

The objectives of ENISA set out in its original mandate were achieved by assuming a set of tasks, mainly by holding an advisory role to the EC and the MS regarding cybersecurity issues. Also, it collected and analyzed the information pertaining to security incidents in Europe and possible dangers. Moreover, among its main task the raising of awareness and the promoting of cooperation between actors of public and private sectors for the conclusion of public-private partnerships (PPP) in cyber related areas.

---

[135] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy (n 90) 605. Page 10
[136] Neil Robinson, 'European Cybersecurity Policy' [2010] Cybersecurity 159. Page 163
[137] 'What We Do - Communications Networks, Content and Technology' (*European Commission - European Commission*) <https://ec.europa.eu/info/departments/communications-networks-content-and-technology/what-we-do-communications-networks-content-and-technology_en> accessed 15 September 2022.
[138] 'Tunis Agenda for the Information Society' <https://digitallibrary.un.org/record/565827> accessed 15 September 2022.
[139] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance).

ENISA's official remit was to expire in March of 2009 but was extended along with its legal mandate and budget until 2012. Then after the public proposals of the EC, on a public discussion of EU approach to Network Security and Cyber-attacks and the role of ENISA in 2008 and on strengthening and modernizing ENISA, the regulation of 526/2013 was adopted.[140] ENISA 's mission remained the same but it had a new improved mandate, encompassing new areas of responsibility, greater flexibility and a rise on its budget.[141] The intention of raising awareness of NIS and the creation of a mentality for a safe and secure Cyberspace for the benefit of citizens, consumers, enterprises and public sector was still its main priority.

An overview of ENISA's involvement to NIS, does entail, *inter alia*, the provision of recommendations, in support of policy making, as well as active participation, whereby the agency is in direct contact with operational teams all over EU. In the work programme of ENISA for the period of 2017-2019, ENISA features the priorities in its mandate.[142]. Under the said document, ENISA is tasked with anticipating and supporting EU in the event of a NIS incident, stimulating NIS as an EU priority policy, maintaining and improving the state of the European network and information systems at optimal condition, supporting the digital community, and bolster its impact. The adoption of the NIS Directive in 2016 greatly improved ENISA contribution for Cybersecurity and upgraded its role to a more centralized one.[143] Under the directive, ENISA becomes the sole, competent authority to provide support by the EU to the member States and monitor compliance with the directive.[144] Further, as the centre of expertise in Cybersecurity issues, must provide solutions and issue guidelines for the Public and Private cooperation, used by the Cooperation Group, the relative EU sub Unit.[145]In addition to the above tasks, the directive imposed to EC the obligation to be advised by ENISA before proposing legal acts, in its area of expertise. ENISA assumed the mandatory consultive role on all cybersecurity matters within the EU executive body. Alongside that task, ENISA assists in the appointment of representatives of MS in various levels of coordination, and essentially became the source of decisions regarding the selection of EU staff in cyber related positions and the allocation of such resources. As a consequence of the "promotion" ENISA was positioned to enunciate more concise and consistent strategies.[146]

The gradual rise of ENISA to becoming the main Cybersecurity actor in terms of EU institutions and policymaking, was further enhanced by the adoption of the EU cybersecurity act of 2019[147]. ENISA was propelled to the forefront of EU cyber policy, after being instructed as the exclusive and permanent authority for a variety of operational-level initiatives for improving the levels of preparedness to cyber-incidents. Additionally, the previous contrast of a time limited mandate, now it has abrogated and the mandate is permanent. Further, in relation to its budget and tasks both have increased, while serving the same mission of ensuring Cybersecurity in the Digital environment of the Union. Despite novelties and advances in the field of the technology and the

[140] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance 2013 (OJ L).
[141] Robinson (n 136) 167.
[142] Management Board, 'ENISA Programming Document 2017-2019' (ENISA 2016).
[143] 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 (n 62).
[144] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 105336. Page 8
[145] 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 (n 62) arts 11 and 12.
[146] Whyte (n 106). Page 205
[147] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

digital world, ENISA will continue its activity as the EU reference point for Cybersecurity issues, addressed to it by other EU institutions, MS and other relevant Stakeholders of the private sector

The proposal for a new Network and Information Directive includes further responsibilities to ENISA, within its existing mission.[148] On the basis of the proposed directive, ENISA would acquire administrative role, as in preparing a report on the condition of Cybersecurity in the EU every 2 years, as well as keeping up a European vulnerability registry, with information regarding ICT products and services and their exposure to levels to cyber-attacks. This data would be disclosed by entities and their ICT suppliers from the private or the public sector. In addition to that registry, ENISA would have to compose and maintain another registry of the registered offices of entities engaging in the provision of digital services, such domain name system service providers, online search engines or social networking platforms. In this manner, the multitude of different legal requirements owing to their cross-border provision of services, are abolished.

Another contribution of ENISA works is in harmonization in terms of national cyber-policies. Prior to the establishment of ENISA, national authorities and private entities executed cybersecurity initiatives separately, isolated and a minor margin of collaboration. On account of deviating, often conflicting practices, diverging national policies have emanated and outcomes of ambiguous efficiency are produced. Hence, ENISA, in its capacity as the secretary of the Computer Emergency Response Team (CERT) community, provides a direct line of communication and assists in trust building among MS and their respective authorities.[149]ENISA, as an EU agency and now the main cybersecurity institution, does not deliver cybersecurity services *per se*, but enables collaboration and acts as a hub for stakeholders.[150] Lastly, besides the aforementioned tasks of ENISA, the agency is in close cooperation with another EU institute dealing with cybersecurity, the European Cybersecurity Centre

C. European Cybercrime Centre

Before the establishment of Europol in 1999, the confrontation of Cybercrime, was handled bilaterally, via international agreements between MS. However, as an aspect of Cybersecurity, cybercrime has the element of cross-border. That means that a cybercrime can be executed from one state and its effects can reach another state or even happen entirely on that state. Even worse, many states could be involved. As such a cybercrime can affect multiple MS and more Law enforcement Agencies would need to engage in collaborative activities. The lack of a bilateral agreement between the respective countries would mean that cooperation and exchange of information would be unachievable, with further consequence, the limited tackling of cybercrime. Targeting the issue of cross-border criminality, EU and MS accordingly established Europol, in order to enhance police cooperation. The mission of Europol as an agency was not to assume operational role within the sovereign MS, but to contribute to the information sharing between the competent national authorities.[151]Therefore, EUROPOL did not assimilate a judicial authority, rather a central node of criminal intelligence. Under the auspices of EUROPOL, the 'High-Tech Crime Centre (HTCC) was founded and undertaken the responsibility for the area of cybercrime.

The HTCC provided another opportunity for information-sharing and collaboration between MS in order to ensure a safe European Cyberspace and combat cybercrime. In 2013 the EC3 was established, the special EU cybercrime Centre, with a mandate to combat cybercrime committed by organized criminal groups, such as online fraud with large criminal profits, or illicit activities with underage victims or illegal behavior targeting European Critical Infrastructure and

[148] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (n 87).
[149] Robert Scott Dewar, 'Cyber Security in the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern' (PhD Thesis, University of Glasgow 2017). Page 66
[150] Annegret Bendiek, Raphael Bossong and Matthias Schulze, 'The EU's Revised Cybersecurity Strategy' (2017) 47 Stiftung Wissenschaft und Politik (SWP) Comments. Page 4
[151] Dewar (n 149) Page 152.

information systems.[152] That signified the importance of a European central intelligence agency against online criminal activity, since the MS were unable to cope with tackling transnational crime on their own. Therefore EC3 intends to arise to the principal combatant in the fight against Cybercrime, by providing support and improving the operational and analytical capacity for LEA of the MS. Among its tasks is the issuance of Internet Organized Crime Threat Assessment (IOCTA), which depicts the key findings and emerging threats in Cybercrime.[153]During the WannaCry Ransomware Attack, EC3 published and distributed manuals and guidelines as well as created an information webpage, improving awareness on Cyber-attacks and on the protection of private data from malware.[154]

There is a strong connection between EC3 and ENISA. Both agencies collaborate and exchange data, to the point that their goals and objectives converge.[155] There is an unofficial arrangement to improve the collaboration in favor of EU. An emanation of that consensus is the cooperation agreement, concluded between them, in relation to the launching of the Joint Cybercrime Action Taskforce (J-CAT).[156] Under legal acts[157], issued by the Council of EU in 2005 and 2013, it was emphasized that the gaps and differences in national legislation set up boundaries in the optimal cooperation between LEA and promoted the use of operation points of contacts, which are offered by the platforms of ENISA and EC3, in order to achieve efficient cooperation. The Council deemed that cooperation at that level could be better achieved.[158] The statement of the Council of EU, hold a symbolic significance and influences as a guideline the function of other institutions. Owing to its trait as the political body of MS governments in the EU, by recognizing the contribution and the works of these two institutions, permits and authorized unofficially the EC to propose policies for empowering these 2 institutions.

D.Computer Emergency Response Teams

On the basis of the Digital Agenda, adopted in May 2010,[159] the EU announced the intention of establishing a Computer Emergency Response team for EU institutions, in relation of the general obligation of EU for a fortified and state of the art, Network and Information Security Policy in Europe. Therefore in 2012 the Union's permanent CERT-EU for EU institutions was set up. [160] The team consisted of IT experts on security, from the five EU institutions and works in collaboration with other National CERTs in the MS and private entities, trading in the area of IT security. The mandate of CERT-EU is of defensive nature, and therefore confines EU's power in cyberspace.[161] The purpose of CERT-EU is to provide support and protection to EU institutions against Cyberattacks that would damage the integrity of their IT assets and hamper European

[152] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre 2012.
[153] Wessel (n 84). Page 500
[154] Agnes Caspar, Alexander Antonov and Center for European Integration Studies, 'ZEI Discussion Paper C 253: Towards Conceptualizing EU Cybersecurity Law' (2019) C 253 / 2019. Page 7
[155] George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Springer 2016). Page 12
[156] Carrapico and Barrinha (n 125) 1264.
[157] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems 2005 (OJ L) 2; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA 2013.
[158] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
[159] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe 2010. Page 18
[160] Sliwinski (n 97) 477.
[161] ibid.

Interests. Further, CERT-EU functions as a nexus for exchange of information on cybersecurity and responds to Cyber-attacks against the EU institutions.[162]

Due to the nature of network infrastructure, a cyberattack can target up to a number of institutions, that they expand to various MS. This complicates the works of National CERTs, causing their actions to be insufficient.[163] Under the NIS directive, the MS are obliged to designate one competent authority and one Computer Security Incident Response Team (CSIRT), tasked with providing digital services.[164] The former would attain a consultive role and the latter will assist in risk management and respond to security incidents. Additionally the NIS directive required the MS to install a single point of contact, in order to facilitate cross-border cooperation between relevant LEA of MS or the CSIRTs network.[165] Amidst the tasks, the CSIRTs also have to contribute to the exchange of data, related to Cyber-attacks and the operational specifics and capabilities of the associated agencies of the MS and partake in the coordinated response to cyber incident, especially in cross-border cyber-incidents. [166] The works of the CSIRTs Network are monitored by the EC and the administrative services are provided by ENISA.[167]

To sum up, since the dawn of the millennium, there has been several in depth improvements in EU institutions and agencies in terms of Cybersecurity. The establishment of ENISA, the creation of Directorates in the EC, the Cybercrime Unit within Europol and the focusing on coordination between national authorities with Union institutions assuming the role of the intermediate, are signs of acknowledgement of primal importance of cybersecurity and the danger that Cyber-related activities pose. Nevertheless, the ambiguity of the efficiency of this fragmented institutional framework is a factor to be considered, in the regulation of Cybersecurity. This issue would be examined in the following chapter in the light of EU cybersecurity policies

3. European Cybersecurity Framework

The European Union has structured the cyber legal framework on 3 dimensions of Cybersecurity. The first of them correlates with the Network and Information security and includes the adopted legal acts related with Digital Single Market and Data protection. The second pillar deals with Cybercrime and illicit affairs online. The third pillar covers EU Cyber-defense and the activities of EDA in that field. The following sections will commence with the Network and Information Security, as it is the area with the longest legislating activity. Next in line is Cybercrime, as a field where EU legal acts correlate with the Budapest Convention on Cybercrime. Last will be the area of Cyberdefense , as it is the least developed and light will be shed to the reasons thereof.

A. Network and Information Security

The wheel of Modern Digital Economy is Information. Data is collected, analyzed and being sold for commercial purposes. As such, the security of that information is essential and efforts for the strengthening of NIS are stirred mainly by the economic factor[168]. Since the internal Market falls within the shared competences of the EU, a number of Cybersecurity measures with an economic background are adopted, within the framework of the Single Digital Market. Adopted by 2015 the Digital Single Market, it entailed 16 initiatives which have been executed by January

[162] Bederna and Rajnai (n 109) 41.
[163] Sliwinski (n 97) 476.
[164] 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 (n 62).
[165] Bederna and Rajnai (n 109) 41.
[166] Markopoulou, Papakonstantinou and de Hert (n 144) 7.
[167] ibid 8.
[168] Odermatt (n 96) 363.

2017 by the EC[169]. EU in the name of the completion of the Single Digital Market, adopted legal acts, protective for the digital infrastructure, so as to instill trust and confidence to EU citizens, encouraging the use of e-commerce and new connected technologies.[170] The coordinated European response to cyber-attacks and the rules on personal data protection are linked to the trust building effort in digital services.

The legal emanation of the extended internal market competence of the Union, that relates to Cybersecurity and serves the principle of Free movement and competition rules is the NIS directive[171]. The EU competence in "internal market harmonization" under article 114 TFEU served as its legal basis. Despite the economic initiative for its adoption NIS directive contains an international security element, which is the predominant one, due to its focus on prevention of attacks against critical infrastructure. Being the first legal instrument to confront cyberthreats, it was adopted on 6 of July of 2016, with the aim to achieve higher levels of NIS in EU, by abolishing differences and promoting convergence between national legislation of the MS in the NIS area.[172]

Under the directive, 3 main objectives are to be attained. To begin with, the increase of digital capabilities of the MS is required and this translates to the obligation of MS to be prepared against Cyberattacks in an efficient manner. Secondly, NIS intends to promote cooperation between MS across the EU. Third, the NIS goals entail risk management and reporting of cyber-incidents, which elaborate to requirements for security and notification, under which certain entities of the private and the public sector must notify of cyber incidents to national authorities. These entities hold an essential position to digital economy, as operators of essential services and digital service providers.[173]

As mentioned above, cyber security issues have been in European agenda and dealt with systematically with the establishment of ENISA. The NIS directive originates from EC initiative for prevention and awareness and defining a plan for ensuring security and trust in the information society in 2009.[174] Followed by a joint communication of EP, Council of European Union , ECOSOC and Committee of Regions on the *an Open, Safe and Secure Cyberspace*[175], the deliberations on the adoption of EC's proposal for NIS directive began and the legal act entered into effect in August 2016, with the intention of being transposed to national legislations by 2018.[176]

---

[169] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe (n 89).

[170] Wessel (n 84) 501.

[171] 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 (n 62).

[172] Markopoulou, Papakonstantinou and de Hert (n 144) 6.

[173] Odermatt (n 96) 363.

[174] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' {SEC(2009) 399} {SEC(2009) 400} 2009.

[175] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88).

[176] NIS directive contains 27 articles. The first 6 set forth the scope and the terms and definitions including the identification of Operators of essential services. Articles 7-10 prescribe the legal requirements of national legislation, for it to be compliant with the directive. Articles 11 to 13 provide the establishment of the Cooperation group, which is the cooperative mechanism for implementing the task of exchange of information and the strategic cooperation between MS. The following articles 14-18 refer to the security requirements and incident notification for Operators of essential services and digital service providers. Next are the adoption of standards and the process of voluntary notification in articles 19 and 20. Last are the articles 21-27 with the Directive's final provisions.

Fallen within the scope of the directive, are entities, incurred with the obligation of holding certain security requirements and notification of cyber incidents. These undertakings are differentiated in 2 categories, the Operators of Essential Services and the Digital Service Providers. Regarding the first, public or private entities that trade in the sectors of energy, transport, banking and health[177]and fulfill certain criteria that the directive sets. Furthermore, the MS bears the task of tracking these entities, id est categorizing and identifying them, for which it must adopt the relevant national laws for the determining these entities[178] and issues a report every 2 years as an update in changes of the entities. The latter category, the digital service providers extend to any legal person that provides a digital service and more specific an online marketplace, an online search engine or a cloud computing service. Owing to the fact that on these providers, other enterprises rely on their own services, the regulation of their cybersecurity conditions is a necessity. Dire economic consequences may happen in case of a disruption to their digital service. However, the MS are abolished of the tracking obligation, in regard to this category of service providers.[179]

Both of the two types are subjected to a set of obligations, but distinct from each other. On the one hand, OES are submitted to extended monitoring by MS, in respect with the appropriate, technical and organizational measures they implement in order to mitigate the risks to the security of the network and information systems they use. Pertaining to that monitoring and with the intentions of aligning the security requirements, the EC advises the MS to rely to the Cooperation Group guidance document, which sets out the principles in adopting security measures. The mandate of the cooperation group is to promote, contribute to the exchange of information among member states and assist in trust building. In addition to the security requirement, the OES must notify the national competent authorities on any major incident, disrupting the continuity of essential service.[180]

On the other hand, DSP are subjected to security requirements based to a number of elements such as security of systems and facilities, monitoring and compliance with international standards.[181] These elements are elaborated further, by virtue of an implementing regulation[182], which affirms the significance of the obligations imposed to DSP. DSP contrary to OES can freely select the technical and organizational measures, as they see fit, in order to deal with security risks of their systems adequately and proportionally. The clarifications of the Implementing Regulation contribute to achieving a common approach of security specifications across the MS. In terms of Notification requirements, the DSP should follow an incident notification procedure. Under such, DSP should be obligated by MS legislation, to notify the CSIRT or the competent authority of any disrupting incident and of its severity, based on a number of factors.

In the context of the directive, a lighter, softer approach towards DSP is noticeable, as far as their security and notification requirements as well as their ex-post supervision by the competent authorities. This distinction can be reasoned as OES and DSP make use of different infrastructures and provide different services in terms of severity. To be exact, OES offer essential services, and

[177] 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 (n 62). See ANNEX 4

[178] ibid. Recital 25 of the directive

[179] Najmudin Saqib and others, 'Mapping of the Security Requirements of GDPR and NISD' (2020) 7 EAI Endorsed Transactions on Security and Safety 4 <https://eudl.eu/doi/10.4108/eai.30-6-2020.166283> accessed 18 September 2022.

[180] 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 (n 62) art 14.

[181] ibid 16.

[182] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact 2018 (OJ L).

as such it is regulated strictly compared to DSP. Further, this laxer configuration of DSP connects to their commercial and profit-making purpose, as it permits a larger margin of freedom to conduct business, enhancing the success in their operation.[183]
There is an interconnection between NIS directive and GDPR[184]. Despite, none of the legal acts acknowledge each other in their respective tests, with a minor reference to data protection under the NIS directive, there are contact points between the 2 legal acts.[185] For instance, the scopes of the 2 acts interact whenever personal data is found in the systems of DSP or OES, and the security of these systems is threatened. The principle of security of personal data is within the core of GDPR. In this scenario, the issue is whether the security requirements imposed by the NIS Directive suffice also for GDPR and vice versa. The solution to that is to implement security requirements and compliance to each set of rules separately and by each competent authority. No legal reason prevents the application of both texts. Another point of coincidence of applications in both texts, is whether an information system's breach could constitute an incident notification under the NIS directive and a data breach notification under the GDPR.[186] In this case, a similar approach should be adopted and the implementation of both legal acts is considered necessary, as the 2 legal acts have a different subject matter and DSP or OES will have to notify separate authorities.[187]

Furthermore, in the event of a conflict between NIS directive and GDPR, any overlap between the scopes of the 2 acts would be resolved by a *lex specialis/lex generalis* relationship as a general principle. However, in *concreto*, GDPR will prevail, owing to right to data protection being declared as a fundamental EU right, courtesy of art 16(2) TFEU[188]. Data protection as having elevated to a human right, is protected as primary EU law, since the EU Charter of Fundamental Rights, under Lisbon Treaty Reform has acquired the same value as the Treaties in EU legal hierarchy.[189] Hence, the right to data protection is a horizontal legal obligation within EU and if the protection of personal data is to be scaled against cybersecurity, the former should predominate.

To sum up, EU has made significant progress in the field of NIS, but there is still work to be done in order to improve Cyber Resilience in Europe. By May 2017, the EC in its mid-term review of Digital Single Market Strategy, outlined three areas for further action, the development of European Data Economy, the upgrade of online platforms as responsible players and surpassing cybersecurity challenges. In the end of 2020 a new NIS directive was proposed by the EC. The NIS directive enforcement proved hard, causing fragmentation at different levels in the internal market[190]. As a response to the sudden increase in cyber-attacks and the growth of threats with digitalization, an improved new NIS directive[191] was devised in order to empower the security requirements, to include the security of supply chains, to modernize the reporting procedures and

[183] 'New EU Cybersecurity Strategy' (n 91) 6.
[184] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) 2016 (OJ L).
[185] Mark D Cole and Sandra Schmitz, 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape' (31 December 2019) 4–18 <https://papers.ssrn.com/abstract=3512093> accessed 18 September 2022.
[186] Sandra Schmitz-Berndt and Stefan Schiffner, 'Don't Tell Them Now (or at All) – Responsible Disclosure of Security Incidents under NIS Directive and GDPR' (2021) 35 International Review of Law, Computers & Technology 101, 105–19.
[187] 'New EU Cybersecurity Strategy' (n 91) 10.
[188] Consolidated version of the Treaty on the Functioning of the European Union.
[189] Lucia Serena Rossi, '"Same Legal Value as the Treaties"? Rank, Primacy, and Direct Effects of the EU Charter of Fundamental Rights' (2017) 18 German Law Journal 771, 772.
[190] Rolf H Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal Aspects' (2016) 32 Computer Law & Security Review 715, 726.
[191] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (n 87).

the monitoring of national authorities, to apply stricter supervisory measures and enforcement requirements.

The proposal recognized the high degree of digitization in the recent years and interconnectedness of similarly high rate of tech innovations, that led to the eventual demise and inadequacy of the NIS directive, as it no longer covers the digitalized sectors, offering services of essential importance to the Union. An important reform is the abandonment of the former OES and DSP structure and the new directive will include under the same requirements public and private "essential" and "important" entities.[192] Also, an increase in the regulated sectors from seven to ten for the "essential" entities and an introduction of new sectors for important entities.[193] Additional focus was given to security requirements for businesses and a turn to security of supply chains and supplier relationships was made. Moreover, the obligation of incident reporting will be simplified while stricter monitoring measures and procedures will be introduced for MS and its authorities. Further the law enforcement requirements are to be exacerbated, with the simultaneous intention of harmonizing sanctions frameworks across the MS. The exchange of information and the cooperation on cyber incidents at both EU and MS level is placed in priority. Lastly, within the scope of NIS 2 directive, entities in public administration will be entailed, as an advance towards ensuring Cybersecurity in the state authorities.

Finally, it is clear that in the field of NIS, the economic rational holds the predominant position, compared to Cybersecurity, given the importance of the latter to modern digital economy, and of the former as the legal basis for EU initiatives and progress in the area. Albeit it steadily becomes apparent that cyber resilience comes alongside with a security element, and that any attempt to an approach should converge or at least coordinate with the other 2 pillars of cybersecurity, cybercrime and cyber-defense.[194]

B. Cybercrime

Another area where EU has been relatively active and has adopted significant rules is Cybercrime. As an area of purely legal origins, the European approach has mainly legal characteristics and EU Directives and Regulations have been employed as a form of governance.[195] Until 2009, EU had only limited powers regarding legislation in the field of criminal law. The harmonization could be achieved only in specific areas, mainly ones related to the protection of financial interests of the EU.[196] In spite of criminal law belonging to the core of MS sovereign powers, that linkage permitted the EU to adopt and define legal standards.[197] EU at the eve of the millennium attempted to combat cybercrime mainly indirective, by either adopting policy measures such as the initiative 'eEurope'[198] and the EC communication of 2001, referring to

[192] Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) 36 International Review of Law, Computers & Technology 118, 12.
[193] Adrian-Viorel Dragomir, 'WHAT'S NEW IN THE NIS 2 DIRECTIVE PROPOSAL COMPARED TO THE OLD NIS DIRECTIVE.' (2021) 9 SEA: Practical Application of Science.
[194] Odermatt (n 96) 365.
[195] ibid 362.
[196] H Wilt and A Klip, 'Harmonisation and Harmonising Measures in Criminal Law' [2003] Nederlands Tijdschrift Voor Traumatologie.
[197] Marco Gercke, 'Europe's Legal Approaches to Cybercrime' (2009) 10 ERA Forum 409, 411.
[198] Europe - An information society for all - Communication on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 1999.

attacks on Critical communication infrastructure,[199] or even the framework decision of 2001 against fraud and counterfeiting of non-cash payments, that penalized computer-related fraud[200].

The legal basis for adopting legal acts in the area of criminal law, initially had to conceive crime as an obstacle preventing intra MS trade relations, and as a disrupting element for stable economic and social development. However CJEU has expanded the EU role in combating criminal activities, despite the lack in a clear con feral of the related competence. In its judgements of *Pupino*[201] and *Comission v Council*[202],the Court held that framework decisions in the area of criminal law affect national legal systems and that the deficit in Community competence did not prevent the EC from taking measures which relate to the criminal law of states. After the adoption of the Lisbon treaty, based on articles 83 and 84, could adopt directives regarding criminal offences and sanctions, only for crimes with a cross-border dimension, such as terrorism, human, drug, illicit arms trafficking and money laundering. Further, if considered necessary by the council, this scope could expand to other illicit activities, so as to ensure implementation of Union policies.[203]

As one of the first legal instruments adopted at EU level in regulating Cybersecurity, is the 2005 Framework decision with the intention of improving cooperation between judicial and other law authorities of the MS by approximating criminal laws of the MS in incidents of attack against information systems.[204] The same act promoted the use of contact points established under ENISA and the EC3, under its previous title 'High Tech Crime Center' in order to avoid repetition of efforts in combating criminal acts. Further, in order to comply its rules with the developments in the international sphere, EC in its proposal for the Framework decision, took in consideration the works and the scope of Budapest Convention of 2005 against cybercrime,[205] and included the approximation of laws against Cybercrime.[206]

For the purpose of integrating the former Police and Judicial Cooperation in Criminal Matters to the Area of Freedom, Security and Justice, the 2005 directive was appealed and replaced by the 2013 Directive on attacks against information systems, known as "Cybercrime Directive".[207] The said legal act, sets forth the minimum rules on the definition of criminal offences and penalties with respect to attacks against information systems. The adoption of common definitions contributes to the consistent approximation of rules between MS. Criminal behaviors include and legislated are the illegal access to information systems, illegal system and illegal data interference and illegal interception. On account the fast pace that cybercrime evolves, it was the intention of the directive to engulf other new forms of threats such as botnet attacks or the internet dimension of organized crime. [208]

In terms of harmful context online, EU has made significant attempts to protect Children from illicit activities in the web. The initial step was a Council decision of 2000[209], encouraging the combat against dissemination of child pornography online, the sentencing and the punishment of the respective offences. Under the same act, the establishment of specialized law enforcement

---

[199] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach (n 99).

[200] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment 2001 (OJ L).

[201] *Criminal proceedings against Maria Pupino* [2005] ECJ Case C-105/03.

[202] *Commission of the European Communities v Council of the European Union* [2005] ECJ Case C-176/03.

[203] Andrej Savin, 'Chapter 10: Cybercrime and Cybersecurity', *EU Internet Law* (Edward Elgar Publishing 2020) 363–365 <https://www.elgaronline.com/view/9781789908565.00016.xml>.

[204] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[205] Savin (n 203) 365.

[206] Gercke (n 197) 412.

[207] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (n 157).

[208] Odermatt (n 96) 362.

[209] Council Decision of 29 May 2000 to combat child pornography on the Internet 2000 (OJ L).

units and cooperation between law enforcement agencies of MS was envisaged, but also the reviewal of criminal laws in procedural terms so as to keep pace with technological advancements. In 2011 the Child Pornography Directive was adopted, which penalized several behaviors, abusive and exploiting for children, and regulated the process of sentencing. Under the said framework, acts such as the production and distribution of child pornography and all related activities were penalized. Also the criminal and civil liability of legal persons is recognized and ICT solicitation and "grooming" of children for sexual purposes has been incriminated. Respect to MS obligations, the directive-imposed law authorities with the task of promptly removing child pornography webpages if hosted in their territory as well as with the block of certain websites that are visited from within the MS.[210]

In addition, 2 new legal acts, a regulation and a directive3 have been proposed by the EC in 2018[211] and 2019[212], the first regarding the collection and the latter the use of electronic evidence for prosecution against criminals and terrorists. Further a new directive on non-cash means of payment is adopted, that improved law enforcement cooperation and action against fraudulent activities regarding non-cash means of payment and facilitated prevention and assistance to victims.[213]

In the battle against Cybercrime, EU has made significant developments, compared to NIS and certainly Cyber-defense. As depicted above, an elaborated scheme of legal acts is enlisted as a safeguard against cybercrime. In general the main European legal act against Cybercrime, the 2013 directive on attacks against information system is an efficient and coherent act covering the biggest threats connected to cybercrime and may contribute to harmonization of criminal legislations amongst the MS. Its practical value is to be tested by the CJEU and its jurisprudence will confirm the efficiency[214]. However cyber resilience involves more than a normative approach. A common culture of cybersecurity needs to culminated entailing the enhancement of trust to ensure data and information sharing, and a financial assistance towards MS needs to be provided in order to maintain an upper tier technological level of their law enforcement agencies. Besides the EUCSS, the European agenda on security, (EAS)[215] refers to a strategy and a system for EU initiatives in Cybersecurity. Therein, illicit behaviors, such as terrorism, organized crime and cybercrime, are considered as areas of cross-border element, in which EU can have a beneficial impact.[216] The following chapter would elaborate on Cyberdefense and the Union activity in that field.

---

[210] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[211] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters 2018.

[212] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings 2018.

[213] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA 2019.

[214] Edita Gruodytė and Mindaugas Bilius, 'Investigating Cybercrimes: Theoretical and Practical Issues' in Tanel Kerikmäe (ed), *Regulating eTechnologies in the European Union: Normative Realities and Trends* (Springer International Publishing 2014) 246 <https://doi.org/10.1007/978-3-319-08117-5_11> accessed 20 September 2022.

[215] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Agenda on Security 2015.

[216] Odermatt (n 96) 362.

C. Cyberdefense

In spite of the progress, EU has made in Cybersecurity and the impact it has produced to MS and internationally, as a significant actor in areas of Cyber-Resilience and Cybercrime, its Cyberdefense policy is still underdeveloped. Further any effort in that area is made in an unsystematic way, through partial measures taken overtime.[217] However, EU by 2014 begun to realize the danger of a Cyberwar, erupting in cyberspace and issued the first EU Cyber Defense Policy Framework[218], and by 2018 a second version of it. The documents integrated in the EU agenda, military-civil cooperation in projects such as R&T, or cyber-exercises or upgrading cyber capabilities in the chain of command CSDP. Also linked Cyberdefense issues to Union's CSDP and designated the necessary path in collaboration with EDA. These documents arose to be a reference policy document on Cyberdefense.[219]

Earlier, in 2017 the EC produced the European Commission Reflection Paper on the Future of European Defense, which prescribed three options for a security and defense Union and indicates the focal point of Cyberdefense. All three scenarios provided in the paper, took in consideration Cybersecurity and foresaw it as an area of cooperation among the MS, within the territory of the Union and internationally, since cyberthreats 'straddle the internal- external policy divide'[220]. As the EU integration continues and extends in areas of defense, Cyberdefense issues are to emerge and linger in the surface.[221]

Cyberdefense policy as an area, affiliates mostly with Common Security and defense Policy, which retains its governmental national character. Defense falls within the core of State sovereign powers, and EU attempts at extending competence in that field are mostly unsuccessful. The first steps towards Cyberdefense transpired in 2010 and attention was turned to cyber capabilities as a critical national security development area.[222] In this early stage, two main areas of action were emphasized, the first being the establishment of crisis response coordination mechanisms under the monitoring of EU and second refinement and education of national cyber capabilities.[223]Despite the reluctant stance of the MS in the area of CFSP, there has been consensus and improvements in the development of a Cyberdefense policy in the framework of CSDP. By 2013, the European Defense Agency(EDA), and the EC constructed and proposed a number of programs with the intention of enhancing EU capabilities in directing cooperation between MS defensive efforts.[224]

Published in 2013, the EUCSS[225] elaborated the relationship between MS efforts and considered that the leading purpose was the encouragement of MS in adopting comprehensive plans for coherent improvements in terms of defense, in transmitting cyber response into crisis response authorities across MS, in creating a robust cyber-security awareness and education system and in facilitating initiatives for collaboration between EU and private EU or non-EU cybersecurity participants. Regarding the last, the focus was turned to the formal cooperation between EU and NATO, and its respective agencies the EDA and NATO' Cooperative Cyber

[217] Wessel and Odermatt (n 114) 505. It is described by the author as a piecemeal approach
[218] Council of European Union, 'EU Cyber Defence Policy Framework' (2014).
[219] Lorenzo Pupillo and others, 'Strengthening the EU's Cyber Defence Capabilities' (26 November 2018) <https://papers.ssrn.com/abstract=3300625> accessed 21 September 2022.
[220] REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE 2017.
[221] Odermatt (n 96) 365.
[222] European Defence Agency, 'Capability Development Plan' (2010).
[223] Pupillo and others (n 219) 34.
[224] Whyte (n 106) 204–205.
[225] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88).

Defence Centre of Excellence (CCD COE). The last issue will be analyzed in the chapter regarding that cooperation later on.[226]

Owing to several fragmented national policies of the MS , for the installation of their own military cyber defense systems, the adoption of a broad, consistent and well-planed EU approach to Cyberdefense hasn't been achieved yet. The necessity for an Eu Cyberdefense policy is highlighted in the EUCSS, with central point the integrity of the communication and information systems of the MS, employed for the defense of MS. Within the same framework, the roadmap entailed the detection, response and recovery from Cyberthreats.[227] EU's approach to Cyberdefense is directed by a protective logic, and that can be affirmed by the fact that EU hasn't planned or expressed the intention of developing offensive cyber powers. Rather, the acts in the area aim at securing conventional military activities from Cyberattacks. Furthermore, due to EU not owing its military force, independent from the MS reach, it relies to MS for providing Cyberdefense for EU led operations. Albeit the distinct national approaches to Cybersecurity, capabilities and the level of protection its MS ensure for its territory, diverge and this hardens EU led activities in the context of CSDP, in relation to equipment and NIS protection.[228]

Another challenge for the adoption of Cyberdefense policy, is the form of the collaboration between the EU and the Cyberdefense actors. On behalf of the Union, an approach tantamount to others implemented for Cybersecurity, id est, enabling collaboration, the sharing of information, and increase in Cybersecurity awareness in the level of MS, would be desirable. Additionally, as EU role is being the intermediate amongst MS regulating the exchange of not only information but also the pooling of resources, the involvement of civilian actors in Cyberdefense is encouraged. EU military operations require the use of civilian actors and infrastructure, and the same technologies are used by the MS military activities.[229] Hence, sharing military capabilities could assist both financially the EU and MS but could improve Cyberdefense levels, if double efforts are avoided.

The aforementioned Cyber Defense Policy Framework is the most significant step in the field of EU Cyberdefense. Adopted after a proposal by the High representative of the Union for foreign affairs and security policy, the EC and the EDA, it designates two main purposes. The first relates to establishing a framework for European Council Conclusions on CSDP of November and December of 2013.The second purpose is prioritization for CSDP cyber defense and the recognition of the roles of the European actors in this field. More specifically, in the framework, a number of actors, partaking in the field are depicted. In terms of priorities, the support in the development of MS cyber capabilities and the protection of communication networks used in CSDP operations are of utmost importance. Further, falling in line with EUCSS, the involvement of civilian actors, related to Cyberdefense is promoted and the cooperation among EU institutions, MS, private sector and the academia is endorsed. Last, the cooperation with relevant external partners, such as NATO is stressed, in compliance again with EUCSS.[230]

From an institutional perspective, the two main actors introducing initiatives in the area of Cyberdefense are the EDA and the EU Military Staff(EUMS). EDA objective is to provide support in the enhancement of MS Cyber defense Capabilities, a task that CD Policy Framework imposed as to be executed in collaboration with MS and the European External Action Service(EEAS) in order to provide effective cyber capabilities. In the EDA's Capability development plan, the strategic manual based on for the identification of future capabilities, the Cyberdefense is the

[226] Whyte (n 106) 204–205.
[227] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n 88) 11.
[228] Odermatt (n 96) 366.
[229] Simon Duke, 'Capabilities and CSDP: Resourcing Political Will or Paper Armies' [2018] Research Handbook on the EU's Common Foreign and Security Policy 154, 167.
[230] Odermatt (n 96) 367.

amongst the top priorities.[231] Furthermore, its within its mandate to participate in training and exercises for cyber situational awareness, to set up a Cyber Defence Research Agenda, to provide detection services of advanced persisted threats for cyber-espionage, and to enable the creation of data protection software especially for military information. Additionally, EDA engages in conducting research of military Cyberdefense capabilities of the EU MS in order to detect and evaluate cavities or areas for more cooperation. In a study prepared in the auspices of the EDA, with factors such as doctrine, organization, training, material, leadership, the margins for further cooperation in incident response and the necessity of cultivation of a cybersecurity culture were confirmed. Also depicted a low degree of maturity in terms of doctrine, organization and training.

In the framework of EEAS, three teams participate and serve the Cyberdefense purpose. To begin with, the Intelligence Centre, as the intelligence European body, provides cyber intelligence capacity and analyzes hybrid threats, is known as the Hybrid Fusion Cell[232] To the actions of this service, national intelligence agencies contribute significantly. Additionally, in terms of nationwide action for Cyberdefense, the aforementioned CERTS or CSIRTS undertake the first responder role. At the EU level, it is the CERT-EU and at the MS level are the national CERTS, whose structure and capability deviates from state to state, whether they are state runed, or private owned. However there is limited participation in CERTS at the European level, as only 10 national CERTS, participate in the CERT-EU. This limited membership corresponds to trust issues and reluctance of MS to collaborate in areas of Defense. The trust building task is undertaken by the EGC group, which intends to enable and cultivate cooperation between governmental CERTS in Europe. Regional cooperation between CERTs of EU and neighboring states is constructed and provided by the CSIRT Network and internationally by entities such as the Forum of Incident Response and Security Teams (FIRST)[233]

Military activities in the area of Cyberdefense and the relationship between cybersecurity policies and Cyberdefense policies drafted for military applications, are shroud with a cloud of obscurity.[234] The other institution, EUMS, contributed to the EU Cyberdefense in policy making in order to guarantee that EU force is protected sufficiently by the MS, when it participates in military operations. As cybersecurity issues and Cyberdefense are inserted as elements to be asserted in CSDP missions and their stage, a higher amount of information on identifying cybersecurity risks is required and EUMS contributes to that. EU Cyberdefense is based in the cooperation among MS, and a pristine example of this is the inclusion in the PESCO framework, for the joint execution of various defense projects. PESCO'S mission is founded in the reasoning, that when the community responds to cyberthreats would improve resilience in cyber-attacks in general and amount to better results cumulatively in time of Crisis episode. In the auspices of PESCO, and serving its mandate, several projects frame Cybersecurity as its key components, such as the Cyber Threats and Incident Response Information Sharing Platform' and 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'.[235]

The triggering point of the unified European defensive stance towards a Cyber-Attack, is based in the solidarity clause under article 222 of TFEU[236]. In the light of the said provision the MS are required to combine their efforts against a terrorist attack or towards a natural or a man-made disaster taking place towards a MS. Even if there is no clear, explicit reference to a Cyber-attack, the EP submerged Cybersecurity and Cyberthreats within the pool of the solidarity clause. The EP concluded that in order to facilitate adequate enforcement of solidarity clause and include all significant threats, a proportional level of flexibility and consistency in defining them is needed.

[231] European Defence Agency (n 222).
[232] Annegret Bendiek, 'The EU as a Force for Peace in International Cyber Diplomacy' 5.
[233] Pupillo and others (n 219) 36.
[234] Christou (n 155) 139.
[235] Whyte (n 106) 205.
[236] Consolidated version of the Treaty on the Functioning of the European Union art 222.

Therein, the EP included attacks in cyberspace.[237] Further, again the EP proceeded to regard Cyber-attacks, as a justification in activating the mutual defense clause of art 42(7) of TEU.[238] In the same resolution, EP considered Cyber-attacks possible to enable the aforementioned clause, despite them not being armed attacks per se and since they intend to cause significant damage and disrupt core infrastructure of MS and originate from external sources.[239] Nonetheless, despite the EP good intentions in expanding both clauses to cover cybersecurity, the vague definitions in the activation requirements of 42(7), prevent the adoption of threshold criteria for discerning which cyber-attacks fall in its scope.[240] Also, in the event of a cyberattack without an recognizable threat actor, the responsibility to intervene of MS under the above clauses is unclear. That issue is rescued up to some point by the Solidarity Clause of article 222, that allows for acts to be adopted against terrorist threats.[241]

In conclusion, despite response obligation and promoted cooperation in the area of Cyberdefense, the whole attempt is fragmented. EU's Cyberdefense capacity is a piecemeal, broken down various institutions agencies and initiatives, permitting the apparition of obstacles to the prevention and preparedness attempt or to Cyberdefense operations The reason for that, is the recourse of focus towards the establishment of a standard approach in regulating digital society across MS. Cyberdefense and the adoption of a comprehensive scheme in terms of legal acts and policies is halted by its submission to the coherent framework that regulates cybersecurity and relevant issues. In respect of the two aforementioned clauses under EU primary law, an application of one to an incoming cyberthreat, will be driven by a political incentive and rather than a legal doctrine.[242] The lack of a complete framework works as a deterrent at EU, from acquiring a prominent role as an international actor in such field.[243] For the purpose of claiming a secure use of Cyberspace EU has to be bold and the establishment of a fully-fledged agency competent at these issues would be a significant first step. Such an entity would unify all the patchwork system, under the common goal of ensuring Cyberdefense.

D. Conclusion

Cybersecurity hard and soft law instruments signify the importance that Cyberspace holds for European agenda and hints the emergence of an EU Cybersecurity Law. However the prospect of Cybersecurity regulation seems to face a crossroad. Cyber threats, in the way the area conceived may shape political choices and promote integration, which is seen with the ENISA, becoming the permanent Cybersecurity agency of EU and the future adoption of a NIS 2 directive. Also, the regulatory framework of Cybersecurity faces a slow development. The reasons for can be found in the inherent trait of Cyberspace, not being able to be regulated, owing to the inapplicability of traditional legal notions such as territorial jurisdiction and its cross-border element surpassing the principle of Sovereignty and the lawmaking of the state.[244]

Throughout the years, EU has dedicated time and effort in producing ambitious cybersecurity policies and legal acts. Though this amounted to a remarkable quantity of policy and strategy papers, drafted by various instruments such as the EC and the EP, the issue of competence in legislating still remains a thorn to the Union's attempt to adopt legal acts, since there is no clear correlation of the measures adopted with the traditional notions of security. Unambiguously, the

[237] European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)) 2012 para 20.
[238] Consolidated version of the Treaty on European Union art 47(2).
[239] Wessel (n 84) 233.
[240] Pupillo and others (n 219) 36.
[241] Whyte (n 106) 206.
[242] Wessel (n 84) 507.
[243] Odermatt (n 96) 372.
[244] Günther Handl, Joachim Zekoll and Peer Zumbansen, 'Beyond Territoriality: Transnational Legal Authority in an Age of Globalization' [2012] Books 342–343 <https://digitalcommons.osgoode.yorku.ca/faculty_books/185>.

majority of EU legal acts in the Cybersecurity field correspond to internal EU policies, id est the NIS directive for the functioning of the internal market, or the fight against cybercrime, because of consumer protection. The social-economic direction of the legal acts is well-founded, on account of the EU competences, conferred under the treaties and the internal market being still the primal objective of EU law and an emblem of European Union successes.[245]

After the abolishment of the Pillar Structure of the Lisbon treaty, cooperation by DG was possible and for the first time there was a unification in Cybersecurity strategy including Internal Market, CFSP and AFSJ. In the internal dimension, EU competence in the internal market remained the same and cybersecurity rules had the same legal basis as before the Lisbon treaty reforms, id est articles 26 and 114 TFEU. In regards of AFSJ, the abolishment of the pillars included it in EU competences, and computer crimes were included in 83 TFEU. With that legal basis, CERT-EU and Europol EC3 were established. From an external perspective, the upgrade of the Chapter of Fundamental Rights, to the same level of the treaties, increased the scope of HR and included the CFSP and CSDP and EDA. This holistic cyber-security approach is unique and progressive, but at the same time, the priority given to the Digital Market, works backwards, as an obstacle for the Cyberdefense to be proclaimed as an autonomous distinct dimension of Cybersecurity.[246]Besides that, a result from the deficit in an explicit cybersecurity competence is the fragmentation in the system, since it is necessary to combine different dimensions of cybersecurity in order to derive a legal base from several competences.[247]

The European Cybersecurity terrain is in constant evolution, as the policy measures adopted, amount to modifications and adjustments to legal framework and the other way around. The outlines of this terrain are expanding due to flexibility in the context of cybersecurity, that on its own comes with a cost. While the ambiguity in the definition permits the engulfing of new technologies and policy issues, at the same, it might impede the regulating process in terms of depth in the area.[248]The EU Cybersecurity Policy making and its implementation as a framework is compound and multifaceted, both in terms of the issues to be dealt with and of the vertical and horizontal integration. Even if a broad set of acts is taken in the area of Internal Market and Cybercrime, there is still a significant need for more coherence of vision and action notably in Cyberdefense. Recently, there have been developments in modernizing the institutional system in charge of providing Cybersecurity for EU. The upgrade of the ENISA, to the frontline of Cybersecurity, the new competence conferred to European Council for imposing sanctions for Cyberattacks and the new EU-wide certification are steps towards increasing Cybersecurity resilience in the continent.[249]

Cybersecurity under International Law

International Law constitutes the only field of law, in the light of its global public goods can be managed and global public interest safeguarded. The presence of technology, expanding in a lurking manner all over the internet, which exceeds national borders, reduces the efficiency of regulation in the national level. Hence international rule is required to provide a lawful and effective mechanism so as to guarantee cybersecurity for the common benefit of all states. The absence of such legitimate and efficient protective framework in the international legal sphere, prevents, individuals, entities and societies from arising to their full capacity.[250]

---

[245] Wessel (n 119) 507.
[246] Tin Chie Man, 'The Use of Legal Competences for Cyber-Security Policy by the EU' 23.
[247] Odermatt (n 96) 508.
[248] Fuster and Jasmontaite (n 98) 112.
[249] Whyte (n 106) 208.
[250] Matthias C Kettemann, 'ENSURING CYBERSECURITY THROUGH INTERNATIONAL LAW' (2017) 69 Revista Española de Derecho Internacional 281, 281.

Despite the activity in single state level, as laws and practices are employed to attend to cybersecurity dangers, cybersecurity as an issue is of international magnitude. Cyberspace is a vast string of networks, unbound by borders and cybersecurity drawn dangers are roam and surpass military, political and geographical boundaries. Aspiring attackers can have high profile target and execute sophisticated precision strikes or release a virus online spreading across unspecified number of countries and affect millions of people. Due to the failure of single state policies and initiatives to establish a defensive cybersecurity mechanism against intruding offensive software unleased in the web, a recourse in the discussion for cybersecurity to international cooperation is taking place in governmental circles, private sector, civil society and academia.

Owing to the global range and character of information systems, international cooperation has undertaken a key role in protecting cybersecurity and fighting cybercrime. International effort in structuring and implementing a legal framework for data and information systems security, has initiated when the telecommunication and information networks became worldwide. Additionally, any attempt for cybersecurity measures in order to be effective, has include beside national policies and the involvement of private tech-industry such as IT entities and Internet service providers.[251]

The highly interweaved and tangled world of today is significantly hampered by Cyberspace and activities therein. Cyberspace has evolved into the pivotal field of international financial operations, political influencing and social networking. Since the end of the 90s, the usage of internet is estimated to have reached, 5.5 billion users worldwide.[252] In spite of the positive outcome produced by the expansion and establishment of cyberspace, that improvement did not emerge without costs or risks. Various individuals, entities or even states engage in nefarious online activities with the intention of disrupting the functioning of information systems or acquiring access to the information stored therein. While there have been initiatives and measures coming from a governmental perspective, the cross-border and transnational nature of Cyberspace motivated in a compulsory manner the international community to enter in discussions and in a legislating attempt with the aim of instilling fair behavior in cyberspace.[253]

The second part of this thesis will deal with activity in the international cybersecurity field and will focus on acts and policies adopted by international organizations, starting from UN and covering acts produced by CoE, OSCE and other international cooperation schemes. Following that part, the customary international law will be depicted and its application in terms of states due diligence will be discussed. Afterwards, the areas of international law, applicable to cyberspace but still unregulated would be depicted. Simultaneously, a comparison with the respective European policies and acts will be provided, in accordance with the comparative purpose of the dissertation.

1.Cybersecurity international institutional approach

A.United Nations on Cybersecurity

Cybersecurity issues were addressed in the UN for the first time in 1998, with the introduction of a draft resolution to UNGA by the Russian Federation regarding developments in the information and telecommunication field[254]. Therein, the effects of the spreading use of information technologies to the interests of international community were highlighted, the

[251] Filip Radoniewicz, 'International Regulations of Cybersecurity' in Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz and Tadeusz Zieliński (eds), *Cybersecurity in Poland: Legal Aspects* (Springer International Publishing 2022) 53 <https://doi.org/10.1007/978-3-030-78551-2_5>.

[252] 'World Internet Users Statistics and 2022 World Population Stats' <https://www.internetworldstats.com/stats.htm>.

[253] Rahul Prakash, 'The UN and Cyberspace Governance'.

[254] UNGA, 'Developments in the Field of Information and Telecommunications in the Context of International Security).' (n 66).

contribution of international cooperation for the optimum effectiveness of information systems was pointed and the negative and harmful use of these systems feasible to occur for reasons other than ensuring international stability and security was mentioned. In that early attempt, no reference international law and regulation of Cybersecurity was made.[255] In the following period, the early UN activity in the Cybersecurity did not produce significant results in resolving cyberspace issues, despite the accumulation of reports and the gradual rise of potential cyberattacks in the real world. The following incidents stirred up discussion within UN and provoked the adoption of initiatives to regulate Cybersecurity and ensure peace in the Cyberspace.

B.United Nations Security Council activity on Cybersecurity

UN security Council (UNSC) holds the prominent position within UN as the sole institution capable of producing binding international law. Up to date, no UNSC resolution has dealt with issues of Cyber-security, but only in its terrorism-related aspects. Under UNSC Resolution 1373 of 2001, the Counter-Terrorism Committee(CTC), after the 9/11 Terrorist attacks.[256] Amongst its works, is to research the exploit of ICTs by terrorist and terrorist groups. Specifically, the Committee, regarding Cybersecurity, examines whether member States to UN comply with their counter terror requirements imposed under resolutions 1373 (2001), 1624 (2005), and 2178 (2014) that relate with ICT. Additionally, its task is to hold meetings on cyber-related terrorist issues. In 2015, a meeting was convened with the agenda of prevention of recruitment of terrorist and terrorist acts via the internet, and in 2016 again on the topic of prevention of the use of ICT for terrorist purposes.

In the auspices of the UN Secretary-General and endorsed by the UNGA[257], the Counter-Terrorism Implementation Task Force was founded, with the mission of ensuring coordination of the activities regarding Resolution of 1373(2001). The Task force proceeded with establishing several working groups, one of them handling the issue of Internet use for Terrorist Purposes. Despite its initial mandate in response to 9/11, now its function extended to the broader cyber-security discussion and is composed of various bodies, such as Interpol, including Interpol, the Office of the High Commissioner for Human Rights and the United Nations Office on Drugs and Crime. Its mission expands into four objectives. First, it aims to identify and converge stakeholders on the abuse of the internet for terrorist purposes, in activities such as recruitment, training, operational planning and other means. Secondly, it investigates and asserts the internet use by terrorist and third it computes the threat and survey for combating it in national, regional and global levels. Lastly, it asserts the role that UN might assimilate.[258]

In its first report in February 2009, based on information provided by UN member states and on the conclusions of a stakeholders meeting, the Task force considered that no obvious internet terrorist threat existed at that moment. However, it induced the exchange for information and sharing of best practices, the assembling of a database for terrorist use of internet and researched possible legal measures for reducing the circulation of terrorist material online. At the second session with various stakeholders and the following report, it highlighted alignment of national legislations with regional legal texts such as the Budapest Convention on Cybercrime or the Commonwealth Model Law on Cybercrime or international instruments such as the Convention against Transnational Organized Crime. Its subsequent activity concentrated on the

[255] Geiss and others (n 1).
[256] UN Security Council (56th Year: 2001), 'Resolution 1373 (2001) /' <https://digitallibrary.un.org/record/449020> accessed 26 September 2022.
[257] Sess.: 2005-2006) UN General Assembly (60th, 'The United Nations Global Counter-Terrorism Strategy ': <https://digitallibrary.un.org/record/582462>.
[258] Christian Henderson, 'The United Nations and the Regulation of Cyber-Security', *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) 605 <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00041.xml>.

Internet and its use to counter Terrorism and specifically the effect of counter-narratives to discourage terrorist acts.[259]
Two Arria-Formula Meetings have been convened with cybersecurity being the main issue in deliberation. The first meeting in 2016, summoned by Spain and Senegal, and discussion was stirred around the threat of ICT use on international peace and security and the challenge in combating Cyberattacks such as the velocity they reach and their attribution to the perpetrators. Additionally, Council members were encouraged to shape policies to assess weaknesses in their Cybersecurity systems and practices to participate in international cooperation schemes and transnational agreements and share best practices and information. At the Second meeting, summoned on an initiative of Ukraine, Cyberthreats, interference with political processes and spreading of propaganda as elements of Hybrid wars were discussed.[260]

The UNSC initiatives in the area of Cybersecurity have been significantly formed by its membership. Due to Estonia holding a seat in the Council in the 2020-21 term, its concerns over Cybersecurity were given a major focus in the discussions of the council.[261] This is affirmed by Cybersecurity being the declared priority of Estonia and by it condemn to 2019 Russian Cyberattacks against Georgia, soon after it assumed membership.[262]

C.United Nations General Assembly resolutions on Cybersecurity

In spite of UNGA being deemed as one of the UN main organs for the maintenance of peace and Security, and not having binding legislative powers, its actions have been focal in the normative development of Cybersecurity. Its rule making function is executed by its six committees and three of them have dealt with aspects of Cybersecurity and engaged in negotiations for draft resolutions and promoted them to the plenary for adoption at the UNGA annual sessions each year.

The Disarmament and International Security Committee is the first UNGA committee that dealt with issues of Cybersecurity and it was the one that the Russian Federation submitted its draft resolution regarding international security[263]. Its key points were the dual use and military potential of ICTs, the inconsistence of ICT with maintaining international stability and security, the necessary for increased extensive cooperation in the field, cybercrime and cyberterrorism and preventing them and the adoption of common definitions for cyber related terms and the creation of international principles. Russia intention was the development of international legal frameworks that deter the use of information technologies for reasons inconsistent with international stability and security.[264] USA rejected that notion, as they argued that the rules that apply on kinetic weapons should apply similarly in Cyberspace.[265] The Russian proposal was seemingly received with suspicion by US and EU states, as the regulation of information security could evolve in a restrictive for freedom manner, in the pretense of information and telecommunications security. Even if it caused a division amongst the UN states, it received general support, and that is affirmed by the following draft resolution, with the same context and submitted by Russian Federation, which was voted against only by the US. During the Obama presidency in the USA, a significant switch happened in USA policy and USA changed its position towards the annually introduced resolution and ended in becoming co-sponsor of its draft, introducing some changes regarding

[259] ibid.
[260] ibid 606.
[261] Eneken Tikk and Niels Nagelhus Schia, 'Chapter 30 The Role of the UN Security Council in Cybersecurity: International Peace and Security in the Digital Age' 8.
[262] Henderson (n 258) 607.
[263] UN General Assembly (53rd Sess.: 1998-1999), 'Developments in the Field of Information and Telecommunications in the Context of International Security ': <https://digitallibrary.un.org/record/265311>.
[264] 'The Trouble with Cyber Arms Control' (*The New Atlantis*) 65 <https://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control> .
[265] ibid 67.

definitions and notions such as international concepts.[266] The resolution, keeps on being introduced to UNGA on an annual basis, with modifications, but the First Committee based its future resolutions on the works of the Groups of Governmental Experts, extensively referred in the following chapter.[267]

The Economic and Financial Committee could be perceived as irrelevant with Cybersecurity issues. However, in its "Global Culture of Cybersecurity" initiative, the second committee touched upon the issues of cyberwarfare and cybercrime, that are primarily the topics of the first and third committees respectively.[268] The three relevant resolutions of this committee made a reference to the resolutions produced by the first and the third committee. The first resolution focused on capacity building which was one of the GGEs goal, and had included as an annex, various elements that could synthesize a global culture of cybersecurity, covering areas such as awareness, responsibility, response, security design and management. These areas, titles as elements should be taken into account by the Member States. In the second resolution adopted in 2005, these elements were elaborated with the addition of protection of critical information security infrastructures.[269] More specifically actions such as establishing emergency networks regarding cyber-vulnerabilities, threats, and incidents, promoting partnerships and sharing of information between Public and Private Stakeholders, adopting legal acts on cybersecurity and training staff for effective investigations and prosecution for cybercrimes, were introduced. The third resolution was adopted in 2010 during the Obama presidency and the reverse in US policy.[270] In its context, it reiterated the aforementioned elements but included a voluntary self-assessment tool. This tool may be used by the Member States as they consider appropriate so as to contribute in their efforts to strengthen the cybersecurity levels of their critical information infrastructures. It is a system of indexes such as policy processes, stakeholder roles and responsibilities, public and private cooperation, legal frameworks and others which may be the subject of UN member States efforts.

The Social, Humanitarian and Cultural Committee is the third committee, in the auspices of the UNGA, which dealt with cybercrime, as the social and humanitarian dimension of Cybersecurity. It adopted a resolution in 2001, with its purpose being to structure a legal base for combating the criminal use of information technologies.[271] In order to achieve this objective, it specified *inter alia*, the significance of ten measures for fighting cybercrime and the illicit use of information technologies, such as the eradication of safe havens for cyber criminals or the improvement of state capacities to fight perpetrators of that kind. In the following resolution the same content was repeated and Member States were encouraged to take under consideration the proposed measures.[272] In 2013 another resolution was adopted in relation with Cybercrime, after the Edward Snowden revelations.[273] The focus turned to international human rights law and the right to privacy, and the violation that they might incur due to illegal monitoring and interception

---

[266] T Maurer, 'Cyber Norm Emergence at the United Nations—an Analysis of the Activities at the UN Regarding Cyber-Security [in:] Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project' (Discussion Paper 2011).

[267] Henderson (n 258) 585.

[268] UN General Assembly (57th Sess.: 2002-2003), 'Creation of a Global Culture of Cybersecurity ': <https://digitallibrary.un.org/record/482184>.

[269] UN General Assembly (58th Sess.: 2003-2004), 'Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures ': <https://digitallibrary.un.org/record/509571>.

[270] 'Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures ': <https://digitallibrary.un.org/record/674820> accessed 26 September 2022.

[271] UN General Assembly (55th Sess.: 2000-2001), 'An Effective International Legal Instrument against Corruption ': <https://digitallibrary.un.org/record/428858>.

[272] UN General Assembly (57th Sess.: 2002-2003), 'Creation of a Global Culture of Cybersecurity ': <https://digitallibrary.un.org/record/482184>.

[273] UN General Assembly (68th Sess.: 2013-2014), 'The Right to Privacy in the Digital Age ': <https://digitallibrary.un.org/record/764407> accessed 26 September 2022.

of communication and illegal collection of personal data. The resolution is reminder to the UN member States of their obligation to implement anti-terrorism measures but in consideration of International human rights law and the right to privacy. Essentially it asks of states to cease the violation of those rights and establish instruments that protect personal data against state surveillance. Following the same tone, in 2018 a resolution, proposed by Russia, regarding the criminal use of information and communication technologies.[274] For several member states, it was a repetition of work undertaken by the pen-Ended Intergovernmental Expert Group on Cybercrime, and for others it was an entry point for a new global cybercrime treaty. However a year later UNGA adopted a resolution with the context of establishing an opened-ended GGE in order to draft an international convention for fighting cybercrime.[275]

Ultimately, UNGA activity in cybersecurity has been extensive, in respect of principles, elements and the stance UN member states should follow. Nevertheless, a deduction on the above, can be that there is need for more comprehensive, deliberate and coherent regulation of cyber security. The exposure of declaratory policy in annual General Assembly meetings, should not replace decisive resolute action by states in other operational forums. Accordingly, the task of elaborating on existing potential Cyberthreats and cooperation schemes has been entrusted on the Groups of Governmental experts and one open-ended working group, which will discussed in the following section

D.Works of Group of Governmental Experts for Cybersecurity

The 9/11 attacks and the subsequent wars in Afghanistan and Iraq, redirected the focus from cyberattacks and security to counter terrorism. However, in 2003 the UNGA entrusted the Secretary-General with the task to compose a GGE in order to provide a report on imminent cyberthreats and the possibility of cooperative measures in addressing them.[276] Even if a substantive report was not published, the disagreement amongst the participant States in the GGE committee, regarding the employment of cyber means for military and national security signifies the reluctance of States to consent to de-weaponization of cyberspace.[277]

In 2007, global attention was immediately turned to the hostile cyber-attacks against Estonia, which was targeted by distributed DOS attacks originating from 175 states, but primarily Russia. The attacks on a NATO state Member, even if could not attributed to Russia clearly and officially, sparked a substantial change in perspective. The matter at hand, debated in the international legal community and at governmental level, was whether the cyber-operations of the 2007 attacks breached the UN Chapter Article 2(4) prohibition on the use of force and if that violation permitted action in collective self-defense under article 51 of UN Chapter.[278] UN responded to the now emerging Cyberthreat and summoned the 2009 GGE. The most important progress made in the second GGE, were the five recommendations it produced for the improvement in terms of trust building and other measures to mitigate the danger of misperception as a result from ICT disruptions. In particular, States were encouraged to engage in discussions regarding norms on State use of ICTs, in reduction of collective risk and the protection of national and international infrastructures. Secondly, under the report the adoption of measures for trust building, stability and risk reduction for State use of ICT and exchange of national views on the use of ICTs in conflict, on information on different national rules, security strategies and policies

[274] UN General Assembly (73rd Sess.: 2018-2019), 'Countering the Use of Information and Communications Technologies for Criminal Purposes ': <https://digitallibrary.un.org/record/1660536>.
[275] UN General Assembly (74th Sess.: 2019-2020), 'Countering the Use of Information and Communications Technologies for Criminal Purposes ': <https://digitallibrary.un.org/record/3847855>.
[276] UNGA, 'Resolution 58/32' (United Nations 2003).
[277] UNGA, 'Report by the Secretary in Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations 2005) UN Doc A/60/202.
[278] Geiss and others (n 1) 663.

were promoted. Third, it was proposed that efforts should be made in identification of measures for capacity building in less developed countries and in defining common terms for information security.[279] Despite the progress, there was no recognition of international law in the report.[280]

A sequent GGE was assembled in 2011, entrusted with the task of continuing upon the assessments and recommendations included in the second GGE report and its report was published in 2013.[281] Under that, the applicability of international law and especially the Charter of the UN was referred as essential for maintenance of peace and stability and for an open, secure, peaceful and accessible ICT environment. The principle of State Sovereignty and the international human rights law were highlighted, and States were stimulated not to make use of proxies for committing internationally wrongful acts or and not to permit the execution of hostile cyber operations from their territory, an adjusted version of the norm of due diligence. The apparent legal conclusions signify a change in the members of the UN stance as the GGE including five permanent members of the UNSC, considered the application of discrete elements of international law to cyber incidents.[282] UN Secretary-General remarked on that Report among else, that the misuse of ICT constitutes a threat to international peace and security and acknowledged that the reports of the GGE functions as a roadmap for attaching ICT security in the wider framework of international law.[283] The above affirmations set course for a fourth GG.

The fourth GGE report placed international law in a prominent position. [284]While restating the remarks of the previous GGE's reports, it quoted the principle of sovereign equality, the priority on peaceful dispute settlement, the prohibition on the threat or on the use of force, the non-intervention principle and the protection of Human rights. Additionally the States jurisdiction over cyber infrastructure on their territory was emphasized. An implied reference to the right of Self-defense was made in consistency with international law and the principles of International Humanitarian Law, humanity, necessity, proportionality and distinction were mentioned, without an explicit connection to the originating body of law. Ultimately, the reiteration of the previous GGE remarks on the applicable international rules and norms in cyberspace is noteworthy but at the same time, the deficit in a clear way of implementation of the international rules diminish its values. This is confirmed by the difficulties in discussion and the absence of certain important issues from the consensus report. The significant element of the GGE report was that it was endorsed by the UNGA, with a major shift in terms of language.[285] From "taking note" as in the previous GGE reports, to the "be guided by the 2015 report" validate the importance of GGE process and outcome.[286]

On the basis of this growth, a fifth GGE met in 2015, with little success, nevertheless. Representatives of the 2 of the permanent Security Council Members argued against the textual reference to 'self-defense' and 'international humanitarian law', albeit the affirmed applicability in the previous report. Also it failed to be included in the produced report the right of retaliating with countermeasures, as acts unlawful in their substance but in defense against another State's unlawful act. Unfortunately the whole GGE effort ended in failure as no consensus was achieved in drafting a report. Moreover, that left the ongoing legal debate over application of international

[279] UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations 2010) UN Doc A/65/201, 4.
[280] Geiss and others (n 1) 663.
[281] GGE (n 70) 98.
[282] Geiss and others (n 1) 663.
[283] Henderson (n 258) 595.
[284] UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) UN Doc A/70/174 174.
[285] UNGA, 'Resolution on: Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations 2015) 70/237.
[286] Henderson (n 258) 598.

law to cyberspace in a divergent motion rather than converging.[287] In the aftermath of the collapse, were the serious and disrupting Cyber Incidents of 2017, namely the WannaCry and Petya/NotPetya ransomware, and the data breaches of Equifax and Deloitte.[288] The collapse of the fifth GGE amounted to questioning the future of the legal debate, and stirred the broader discussion on how the GGE would proceed in the future. Others remarked that the whole GGE process was finished[289], others considered this ending as a stimulus for a more regionalized and fragmented regulation of cyberspace[290], other promoted an ongoing GGE process, or transferring the discussion under the auspices of a newly founded cyber committee of the UNGA[291] or to the sixth Committee of the UNGA or even promoting the question to the International Law commission.[292]

In December of 2018, UNGA established 2 separate processes for cybersecurity and international norms. On the one hand an open-ended working group (OEWG) was created, as it proposed by a number of countries, and all UN states participate therein, contributing to the discussion of improvements in ICT in the context of international security[293]. On the other hand, the UNGA chose the continuance of the debate within the framework of GGE.[294] Both of the committees embark on the same activity of researching the task of implementation of International Law in Cyberspace. However the OEWG has a broader mandate including existing and potential cyber threats, as well as the discussion regarding institutional dialogue and international concepts for global IT systems. Also, OEWG has to examine whether changes to previous GGE reports are essential or other additional rules of behavior are needed. A difference with the previous GGEs is that while there was an agreement in general applicability of international law and its norms in the GGE's reports, there is a dispute within OEWG for specifications on applicability of international norms. For instance, the applicability of international humanitarian law, the right of self-defense, the attribution for cyberattacks or the need for a new international cyber convention are issues highly disputed and unregulated. Having two parallel UN processes with similar mandate might be unreasonable, as states may elicit in practices such as forum shopping. However, the two groups, can assert the level and the range of consensus amongst UN member states, on the critical role of international law, for adjusting the conduct of State and non-State entities in cyberspace.[295]

E. ECOSOC

The Economic and Social Council is the third intergovernmental UN institution that dealt with Cybersecurity issues, in its capacity as the major body for coordination, policy review and

[287] 'UN GGE on Cybersecurity: The End of an Era?' <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> accessed 25 September 2022.
[288] Tim Maurer Taylor Kathryn, 'Outlook on International Cyber Norms: Three Avenues for Future Progress' Carnegie Endowment for International Peace <https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704> accessed 25 September 2022.
[289] Fosca D'Incau Soesanto Stefan, 'The UN GGE Is Dead: Time to Fall Forward – European Council on Foreign Relations' (*ECFR*, 15 August 2017) <https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/>.
[290] Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5 Journal of Cybersecurity.
[291] Theodore Christakis, 'Reinventing Multilateral Cybersecurity Negotiation after the Failure of the UN GGE and Wannacry: The OECD Solution' (*EJIL: Talk!*, 28 February 2018) <https://www.ejiltalk.org/reinventing-multilateral-cybersecurity-negotiation-after-the-failure-of-the-un-gge-and-wannacry-the-oecd-solution/>.
[292] 'ESIL Reflection: The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? – European Society of International Law | Société Européenne de Droit International' <https://esil-sedi.eu/esil-reflection-the-codification-of-the-international-law-applicable-to-cyber-operations-a-matter-for-the-ilc/> .
[293] UNGA, 'Resolution 73/27' (United Nations 2018) 73/27 27.
[294] UNGA, 'Resolution 73/266' (United Nations 2018) 73/266 266.
[295] 'Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive' (*Just Security*, 28 February 2020) <https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counterproductive/> .

dialogue and recommendation on economy, society and environment. Activity in the issue at hand has produced in two of its functional commissions , the one on Crime Prevention and Criminal Justice (CCPCJ)and the second on Narcotic Drugs, in the dimension of Cybercrime.

The First commission, starting from the end of the 1990 place cybercrime at a place of notice for the UNGA and requested the conduct of research regarding effective measures to combat the criminal use of information systems. Another significant contribution of that committee was in 2002, the reference of the term "cyber" while calling for a UN convention of cybercrime by 2004. Also, due to the works of the committee, aspects of cybercrime were placed under the microscope of the UNGA, such as the exploit of children online, economic fraud and identity related crimes, organized crime and trafficking committed by the use of computers. Furthermore, the CCPCJ, as requested by ECOSOC and UNGA set an open-ended intergovemental expert group on cybercrime, with the mandate to provide a comprehensive study of Cybercrime, measures adopted in diminishing it by other MS, the international community and the Private sector, best practices implemented by them, technical assistance and international cooperation and national and international legal responses to it. The second commission addressed Cybercrime from the point of use of the internet for the sale of illicit drugs. In all its resolutions, the topic of drug trafficking online was discussed in reference to its extensions such as the protection of young adults and children from drugs sold through the web or enhancing cooperation initiatives for preventing sale of drugs to individuals online.[296]

F. International Telecommunications Unit

Besides the main intergovernmental bodies within the UN chapter, several subsidiary institutions and agencies have produced input in the area of Cybersecurity. The International Telecommunication Union, seated in Geneva, holds the position of the most vigorously functioning body in the safekeeping attempt for Cyberspace via aligning legal norms of various countries and by setting international regulations.[297] Drawing legal basis from article 22 and 57 of UN chapter, the ITU is the UN specialized agency for ICT and regulates mostly the technical dimension of cybersecurity. Aside its central role in establishing technical standards, ITU focuses on specific initiatives in the area of Cybersecurity, promoting the wider agenda of its Member States. The" Global Cyber-Security Agenda" was published in May of 2007 by the ITU Secretary-General who characterized it as the international framework for Cybersecurity.[298] Under the agenda a high-level group of experts was established.

After three meetings, a report was produced, and concentrated in the adoption of legal, technical and procedural measures, capacity building an international cooperation. Further, the group proceeded with several recommendations, such as drafting an exemplary legislation for Member states to adopt and using the cyber-crime legislation kit developed by the ITU as a basis for lineament of cybercrime laws. In addition, the development of a Cybersecurity Readiness Index, a system for national infrastructure protection and the cultivation of a Cybersecurity culture were encouraged.

Cybersecurity in the ITU agenda has been promoted at a high degree due to interference the ITU Secretary-General. During the 2010 "World Telecom Development Conference" (WTDC), his proposal was a "no first attack vow" for cyberspace, he also recommended that Member States should refrain from providing safe haven to cyberterrorists[299] in their country and provided five principles for Cyber peace.[300] Another input of ITU to cybersecurity, is the release

[296] Henderson (n 258) 610.
[297] Radoniewicz (n 251) 64.
[298] ibid 66.
[299] Richard Hill, 'Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT', *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (2015) 81.
[300] ibid 78.

of updated guidelines to fortify online protection for children, in collaboration with United Nations Children's Fund, and Child Online Protection Initiative. ITU intervention in children protection is perceived as an attempt of trust building in that area to expand to the larger cybersecurity picture as a spillover effect.[301] Under the 2017 WTDC, the Buenos Aires Action Plan was adopted and on it builds the current ITU cybersecurity initiative. It provides a pool of information for Member States along with tools to improve cybersecurity nationally so as to increase security and instill trust in ICT use.

G.Conclusions on the UN Cybersecurity Framework.

The above chapter provided a limited outline on the activities of UN in the context of Cybersecurity. Achievements in normative development in the area are apparent in the high number of UGNA resolutions agreed, the increased number of sponsors, the contemporary ongoing work of the GGEs and the OEWG, and the contribution of a variety of organs and agencies to regulating the issue at hand. A significant shift in UN activity in the area is visible and impetus towards the establishment of something substantial and momentous within the UN is seemingly preparing. The general applicability of International Law, the need for improved cooperation schemes, not just among states but including other stakeholders, for commonly acceptable State behavior online, for trust building procedures, transparency, and technological capacity building are issues at the center of the discussions and debates within the GGEs but also hold a distinct place in the agenda of the other UN organs. However, it is sufficiently clear by the divisions within the UN and especially within the GGE and the OEWG, in respect of the direction the emerging regulatory framework should have, which would eventually lead to the governing model of cyberspace, that there is lack of consensus and a divergent shift in the motivation of states towards the nature of cyberspace and cybersecurity regulation.

From a comparative perspective, the UN framework has similarities and significant differences with the EU one. As in the EU, there has been a recourse towards Cybersecurity and the dangers of Cyberspace in the UN agenda from the eve of the millennium, and this focus has been intensified after the first decade, as it is seen with the number of UNGA resolutions, the GGEs convened and the UNSC initiatives. Additionally in terms of primarily law and legal texts, there is no clear reference to the primary texts of the two objects in comparison, the UN chapter and the EU treaties, the notion of cybersecurity. UN correlates Cybersecurity to its mandate in maintaining of peace and security under the UN chapter, without a clear reference to cybersecurity. Accordingly, in the EU treaties there is no clear reference to Cybersecurity or its dimensions, even after the Lisbon treaty reform of 2009. EU Rulemaking in the Cybersecurity area draws legal basis from articles related to internal Market. A difference is the intention of the Regulation. UN regulatory attempt at cyberspace was motivated by ensuring peace and security from the start. For EU, the initial motivating factor was an economic one and particularly the stability in the functioning of the internal market. In that pretense, it later moved towards a more security-themed legislation

From an institutional perspective, both transnational organizations occupy their majority of organs with Cybersecurity tasks. The UNSC, the UNGA, and the ECOSOC have devoted significant effort and initiatives with the intention of establishing legal norms and policies for Cybersecurity. This is affirmed by the number of GGEs and the ongoing ones for Cybersecurity and Cybercrime. The ITU, as subsidiary UN organ has promoted Cybersecurity in its own terms and contributed to the whole scheme. Along the same lines, EU legislating trio EP, EC and Council of European Union have produced a significant number of legal acts, regulating several aspects of Cybersecurity. However, the distinctive EU element to UN, in that regard, is that EU has created ENISA an agency, which was upgraded to institution, with the exclusive mission of ensuring

[301] Maurer (n 266) 30.

Cybersecurity, and the EC3 for combating Cybercrime. There is no UN organ devoted absolutely to Cybersecurity.

In terms of legal acts, there is considerable difference between EU and UN, rooted in the nature of both organizations. EU is a regional supranational organization, with limited intergovernmental elements. As such in the areas where it has competence, it produces binding legal acts to all its MS. As mentioned above, there are a number of legal acts (NIS directive, directive for attacks against information systems regulating the different aspects of Cybersecurity and the legislative activity appears to be severe in the future, such as the adoption of NIS 2 Directive. On the contrary, UN adopted acts, such as UNSC and UNGA resolutions frame international law and are considered binding for its members, depending on the nature of the resolutions. For instance resolutions adopted under chapter VII of the Charter, are considered binding, according with article 25 of the Chapter. But the majority of UN adopted acts in the area of Cybersecurity are UNGA resolutions, or recommendations by other organs, lacking binding powers.

2. Council of Europe and the Budapest Convention against Cybercrime

Cybercrime, as an aspect of Cybersecurity has been the focal point in numerous initiatives with the intention of aligning legislation, adopting common definitions and improving transnational cooperation. The most significant, of these initiatives, holding extensive recognition internationally is the Convention on Cybercrime of the Council of Europe, known as Budapest Convention, that entered into force in 2004.[302]It is the first multilateral and most pertinent international treaty in the area of Cybercrime, and contrasting to other CoE instruments is open for participation to all States and hence it can be applied worldwide.[303] The timing of its adoption corresponds with the rise of IoT and the augmented importance of Electronic Commerce and Intellectual Property, enhanced by the unbound nature of Cyberspace and the cross-bordered nature of cybercrimes and marks the effort in regulating it at the European Continent.[304]

The convention imposes the obligation for MS to introduce in their national legislation, the substantive provisions under it and facilitate cooperation in criminal areas. It has a triple goal. Firstly, to conceptualize and define illicit behavior online, and thus harmonize national legislations, with establishing a common base of offences. Second, it constitutes transnational cooperation in regards with criminal investigations and proceedings. Third, it unfolds roads for international cooperation.

Regarding the substantive part, the illicit activities set out under the convention are divided into four categories. Within the first category, offences against the confidentiality, integrity and availability of computer data and systems are entailed, such as illegal access and interception, and production and dissemination of criminal enticing hardware and software. The second category includes computer related offences such computer forgery and fraud. Following that it is the content related offences, such as crimes related to child pornography and infringements of intellectual property and related rights. There is an additional protocol annexed to the convention, that criminalizes behavior of disseminating racist and xenophobic material online. Moreover, it comprises provisions on the attribution on criminal acts, as well as aiding and abetting and on corporate liability.[305]Undoubtedly not all possible illicit acts online are encompassed in this

[302] Convention on Cybercrime 2004 (ETS No 185).

[303] Philipp Kastner and Frédéric Mégret, 'Chapter 12: International Legal Dimensions of Cybercrime', *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) 255 <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00022.xml>.

[304] Savin (n 203) 365.

[305] Radoniewicz (n 251) 57.

enumeration, but as it is stated in the convention Explanatory report, this set of offences indicates a minimum consensus and does not exclude extensions in domestic legislations.[306]

There is a procedural part under the Convention as well. The procedural provisions, institute powers and procedures for criminal investigations of the crimes including but not limited to the crimes of its substantive part. That is to say, the procedural part intents to apply not only to Convention itself, but to act as a harmonizing factor of the parties thereto, for the procedural law to computer crimes. Under that part of the Convention, international cooperation is enhanced. Intern alia, States are obliged to order and obtain the preservation of computer data, or to ensure its disclosure. Also, crime related computer data is searched and seized by the competent state authorities and, traffic data can be collected or recorded and content data can be intercepted by law authorities or by enlisting a service provider. These provisions lack the innovative element, that is inherent to technological aspects, but they follow the attempt of the convention to adjust the already established international criminal law instruments to the internet age, with the objective to permit the intervention of authorities as rapid as possible. The procedural part is subject to a safeguard provision, that ensures protection of HR and liberties, into implementation of the said part. The levels of protection have to be consisted with international law such as the European Convention on Human Rights and the International Covenant on Civil and Political Rights. Albeit, again the Convention leaves a margin of discretion for state parties to enforce a more protective for HR regime, of their choice.[307]

Following the objective of relevant international legal acts, to enhance cooperation between States, for cybersecurity purposes, there are provisions set out in the conventions instilling cooperation in areas of mutual assistance for investigations, proceeding and collection of evidence and on extradition. The convention advices its parties to collaborate in criminal matters applicable to the cyberspace in all possible ways.[308] Among else, States should rely on expedite means of communication such as email, must select a 24/7 point of contact for immediate assistance and must be on alert for immediate actions on preservation of data or disclosure of it. In connection with extradition, falling behind other international instruments dealing with transnational crime such as the Palermo convention, it places an *aut dedere aut judicare* clause, requiring the state parties to either extradite the perpetrator or start proceedings before their national courts.[309] Additionally, it contains the possibility of extradition of set out offences therein, under two conditions, that they are punishable by laws of bother parties and for a sentence of deprivation of liberty at least for a year. That provision works as substitute in case no other bilateral treaty exists between the parties.

A.Conclusion

The advantage of the Cybercrime convention is its open character, meaning that it permits countries not parties to Council of Europe, to accede and its flexible clauses, being optional at least some of them. Considering the former, by September of 2022, sixty-seven states have ratified it, the last being Sweden, almost all CoE member States have ratified it and the convention was signed by four countries outside the EU continent (Australia, the Dominican Republic, Israel, Panama) and acceded by other eighteen. The latter, facilitates the adoption of the Convention with the reservations on certain provisions and therefore the signatories are able to settle the obligations set out thereunder, by adjusting them their own legal acts and national jurisprudence.[310] Nevertheless, despite the beneficial way it has affected the combat against criminal behavior online, it can be subjected to criticism for several reasons. It promotes the establishment of a massive surveillance

[306] OF EUROPE COUNCIL, 'Convention on Cybercrime. Explanatory Report' para 30.
[307] Kastner and Mégret (n 303) 262.
[308] Savin (n 203) 374.
[309] Kastner and Mégret (n 303) 264; Budapest Convention art 24(6).
[310] Radoniewicz (n 251) 57.

apparatus, penalizes activities that previously were not considered harmful and places severe standards on computers that are in constant development. Software, banned by the convention due to their data altering capacities, may be out of use, even if they have an innocent use. To sum up, the Budapest Convention depicts a conventional, regionalized approached on the basis of the territoriality principle with the intention of increasing the capacity of States in regulating Cybercrime.

In its comparison with EU law, the Budapest Convention constitutes a binding legal act for its parties. Similarly, EU law and the secondary legal acts dealing with issues of cybercrime are equally binding for EU member States. In terms of context, equally with the Cybercrime Convention, the Cybercrime directive harmonizes criminal law related to attacks on information systems amongst the EU member states and provides with a set of criminal offences that correspond to ones promulgated under the Budapest Convention. Accordingly, the directive penalizes in another legal act, the Child Pornography directive, acts executed online against underage adults. That is also a content related crime for the Budapest Convention. However there are differences amongst the texts. For instance, under the Convention, illicit access is punishable only when is supplemented with the intention of obtaining data or in the case of a networked computer system. Contrary to that, the directive does not impose such requirement.

3. Organization for Security and co-Operation in Europe

The Organization for Security and Cooperation in Europe (OSCE) has not entailed Cybersecurity in its areas of interests. Nevertheless, the issues of security in Cyberspace are considered in OSCE activities as it is affirmed by decisions adopted by the Committee of Ministers. The first two relate with combating the use of Internet for terrorist purposes and elaborate on the exploit of Internet by terrorist Groups with intentions to recruit members, collect and transfer funds, conduct their operations or propaganda. Further, under the decisions, the acts provided therein have to comply with the international obligation States have for the protection of Human rights and right to privacy, freedom of expression of opinions and views. Also in order to attain the combat against terrorism, enhanced cooperation and exchange of information are facilitated. The other two decisions, relate with OSCE works in diminishing the risk of conflict arising from the use of information and communication technologies.[311]

In comparison with OSCE, European union has developed its own set of rules in the combat against Cyberterrorism. Under Directive 2017/541[312], MS are obliged to remove content containing public provocation for committing a terrorist act, when the host of the content is within their territory. Further, if the content is uploaded outside of their control area, they are required to block access to it for users. Lastly, transparency and protection of HR under the chapter are to be honored during the procedures implementing the directive. The directive is supposed to be complement by a regulation that has been proposed in 2018 and it is in the phase of legislation.[313] Its aim is to set uniform rules for the prevention of distribution of terrorist content. Under the proposed legislation a distinct set of rules is proposed, one addressed to DSP, that host websites regarding the prevention and removal of terrorist content and the other regards MS for adopting measures to identify and remove the content. During deliberations in the EP, a severe dispute took place. A number of the proposed provisions raised questions and disagreements regarding definitions, referrals and proactive measures. Also a lack in the adoption of proper safeguards and

[311] ibid 60.

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

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

inconsistence with the E-Commerce directive are referred. In spite of difficulties in its adoption, the initiative towards combating the dissemination of Terrorist content online aligns with OSCE activity.

4.Nato on Cybersecurity

Both EU and NATO are major international actors on from an economic, political and military perspective. Accordingly both face Cybersecurity Threats, Cybersecurity attacks and other challenges in the Cyberspace. Hence both have acknowledged the significance of Regulation of Cyberspace and have developed their own Cybersecurity policies. In a similar way to EU, NATO has established its own procedures and policies in the field of cybersecurity. However, under NATO terminology, Cybersecurity, for EU, translates to Cyberdefense. The shift in NATO focus on issues on cyber issues increased significantly after the Estonian attacks of 2007. Besides the technical issues, political and international legal matter have arisen within the Alliance since 2007.[314]

Post the Estonian Cyber Crisis, it was evident and stressed by NATO officials that a central coordination and central Roles in the area of Cyberdefense of the Alliance was needed. At that time, the conceptualization of cyberspace and the conception of an attack against a Country through cyberspace and not in the already known traditional dimensions of land, air, sea and space, was a progress of its own for NATO. That acknowledgement contributed to upgrading Alliance's defense infrastructures for military communications and IT systems after the 2010 Lisbon Summit.[315]In 2011, the new Cyber Policy for NATO was signed by the Defense Ministers of NATO Member States, that outlined the Cyberdefense Policy and the relevant action plan. Under the said plan, two institutions regarding Cyberdefense were established, the NATO Cyber Incident Response Capability and the Cyber Threat Awareness Cell, by 2012. During the 2014 Wales summit declaration, a new enhanced cyber defense policy was enacted, whereas its was clarified that Article 5 of the Washington Treaty, could be invoked for a major digital attack and the NATO forces could mobilize as collective defense.[316] Additionally, the improvement of Cyberdefense capabilities, education, training and exercise activities were encouraged.[317]

Since NATO does not have an established operating cyber defense force, its already functioning institutions and organs deal with the political, operational, technical challenges of Cyberdefense. Set out under article 9 of the North Atlantic Treaty, the North Atlantic Council (NAC) has the decisive competence regarding the NATO responses to attacks of any kind. It is assisted in topics related to Cyber issues by the Cyber Defense Committee and by the Cyber Defense Management Board (CDMB). In 2012, among the institutional structure within NATO, the NATO Communication and Information Agency, (NCIA) was established by merging several existing agencies. This Agency servers the main provider for communications, command and control and supports NATO in terms of IT. Also has the competence of planning for NATO's defense capacity in terms of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture, exercises, and training, and acquisition of state-of-the-art technology. Further NCIA acts as the NATO first line of Cyberdefense and hosts both the NCIRC team and the NATO's Information Security Operations Centre

Even if it lies out of the NATO institutional framework, the NATO Cyber Defense Center of Excellence (CCD COE) in Tallin, Estonia provides assistance in Cyber related areas to NATO. Under its works, doctrinal and legal concepts are produced, training and exercise programs are

[314] László Kovács, 'Cyber Security Policy and Strategy in the European Union and NATO' (2018) 23 Land Forces Academy Review 16, 6.
[315] Kovács (n 314).
[316] Luukas K Ilves and others, 'European Union and Nato Global Cybersecurity Challenges' (2016) 6 Prism 126, 129.
[317] John R Deni, 'NATO's New Trajectories after the Wales Summit' (2014) 44 The US Army War College Quarterly: Parameters 8, 3,5.

conducted and technical research and experiments take place. A product of its works was the Tallin Manual, which served as the main authority on the applicability of armed conflict to cyberspace. Following that, the Tallin Manual 2 was published examining the application of International Law to Cyber Operations. Again, outside of NATO command, there are strong ties with entities trading in Cybersecurity. An initiative named as NATO Industry Cyber Partnership (NICP) is in charge of providing relationships with the industry. Moreover a response team to imminent Cyber Attacks, similar to CERT-EU, is established in order to provide 24 hours a day assistance and protection against attacks to NATO critical infrastructure.

In terms of Institutions, NATO has developed a comprehensive framework of organs and agencies, that are been engaged in Cybersecurity activities, similar to EU. Amongst the European Union organs, ENISA is in charge of Network and Information Security, EC3 within Europol contributes to fighting cybercrime, EDA, EFMS and the EEAS deal with Cyberdefense. Also EU has its own response team for cyber incidents the CERT-EU, which collaborates with the rest of CSIRT's of MS. From a substantive perspective, NATO act that it is the only binding is its founding treaty. NATO's cyber policy has been shaped based on it and article 5 is of high importance for Cyberdefense. After the 2014 Wales Summit, it was affirmed that a cyber-attack may constitute a reason for invoking article 5, as the self-defense provision of the Washington treaty. In NATO's practice until now, article 5 is perceived as the other side of coin of article 51 of UN chapter.[318] The notion of an armed attack is indicated in this case, and NATO'S policy depicts at the very least that a cyber-attack could be conceived as an armed attack, inducing the right of individual self-defense or collective defense under the UN chapter. However, it is not clarified which cyber-attacks can constitute this extent of action or the threshold of the armed attacked which correlates to a cyber-attack. The lack of detailed explanation of which cyber-attack constitutes an armed attack is straightforward and relates to empowering the deterrence value of NATO's attitude. In the same manner, in the event of a cyber-attack, the following invocation of NATO collective response power will be decided on a case-by-case basis by the North Atlantic Council. Towards the legal obligation of providing assistance to the State being the target of a Cyberattack, under this framework it is impossible to foresee, whether the article 5 would be implemented.[319] European legal acts in the area of Cyber Defense is of the progressed amongst the aspects of Cybersecurity. The reason of that lies to Cyberdefense being in the core of the CFSP, where still MS hold the decision-making power, since it relates with their Sovereignty.

A.EU and NATO COOPERATION

Enhanced EU-NATO cooperation in the area of Cybersecurity came at a time when both organizations faced direct opposition to their integrity and existence, from the rise of Asian Superpowers and Eurosceptic populist waves from within of EU. The cooperation is beneficial as both political interest and technological expediency reached a common point in order to tackle the common challenge for security in the cyberspace. That cooperation would be evolved in two directions, the first would address the related hybrid warfare efficiently and the other will compel the rest of the world in shaping regulatory frameworks for cyberspace and other innovative technologies such as AI and IoT.[320]

Both Organizations act as guarantors of security, stability and prosperity in Europe. In the two joint declarations of 2016 and 2018, it was agreed that there would be enhanced cooperation

[318] Aurel Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats' (10 June 2019) <https://papers.ssrn.com/abstract=3401995>.

[319] Steven Hill, 'Chapter 24: NATO and the International Law of Cyber Defence', *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) 519–521 <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00037.xml>.

[320] Peter Poptchev, 'NATO-EU Cooperation in Cybersecurity and Cyber Defense Offers Unrivalled Advantages' (2020) 45 Information & Security: An International Journal 35, 36.

between them in several areas. In those areas, the purpose is to achieve cooperation rather than contest, and complementarity rather than repetition of efforts. Further this cooperation will be beneficial for each organization pertaining to its own tasks and efforts, whether is evasion and deterrence to cyberattacks or collective defense. The merge of Sovereignty and common use of defense resources would be positive for international and regional stability. This is further enhanced by the district arsenal both institutions hold for ensuring security. Amongst the agreed cooperation areas lies Cybersecurity. The objective of the cooperation in combating cyber and hybrid threats, is to attain a proper symmetry between legal measures and procedures on the one hand and deterrence on the other.[321]

In the global context of big States using their cyber capacity to progress their interests, smaller ones in improving their cyber capabilities for claiming a higher position, non-state actors such as international companies and proxy hackers and deep-rooted clash on the freedom of the internet, there are 5 issues that delimit EU-NATO cooperation. First, the manner of intelligence sharing between the two organizations is debatable. The second relates to the necessity to avoid repetition of the same cyber-operations and operative coinciding. The third concerns the lack of flexibility of institutions in handling the swiftness of cyber-attacks. The fourth, has to do with the adoption and implementation of policies and initiatives irrelevant to the issue of Cybersecurity. Last, the issue of exacerbation in operational responses to potential attacks restricts more the EU-NATO cooperation and the reason for that are the grey zones in legislation. The majority of cyber-activities happen below the limit, out of NATO competence, and beyond the EU capacities.

A multistakeholder approach is called by the EU's Cybersecurity strategy for the Digital decade, structured on multilateral procedures and activities. This is an affirmation of the necessity for a strategic framework for cooperation, that permits and incites both the implementation of international law and the adoption of norms of state behavior and confidence building. Despite the respect of international of Law on Cyberspace by the EU MS, there is no common conception regarding the notions and terms applied in the cyber domain among the MS. For instance, there is no consensus for when a Cyberattack constitutes a violation of Sovereignty. The starting point for reaching agreement over the vagueness in cybersecurity concepts, could be the Norms on responsible state behavior in Cyberspace, elaborated by the GGE of 2015 and endorsed by the UNGA.[322]

The benefits of enhanced cooperation between EU and NATO, extend to a whole spectrum of concerns, such assuming leadership in digital transformation of the world, protection of HR and online freedoms. A fertile ground for further cooperation is the conjunction of cyber, hybrid and information influence operations. These three areas exceed the institutional setting and division of competences among MS and the NATO organization. In addition, a multiparty attempt to regulate the combination of these three areas, demands a thorough delineation of the tasks in addressing these and the means and their nature, civilian or military.[323]

5.Customary International Law applied on Cybersecurity and Due Diligence

Most of the cyber-attacks do not supersede the point after, law of armed conflict is activated. Hence, there are questions raised, that remain unanswered, regarding the extend do States are required to shelter their networks and information systems or to start criminal proceedings against cyber attackers or even extradite them. In respect of this issue, excellent

[321] Isabel Ferreira Nunes and others, 'EU-NATO Cooperation' (National Defense Institute of Portugal 2021) <https://www.jstor.org/stable/resrep39891> accessed 27 September 2022.

[322] Un Secretary-General and UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ': <https://digitallibrary.un.org/record/799853>.

[323] Ilves and others (n 316) 6.

guiding jurisprudence can be found in the judgements of ICJ such as the *Corfu channel* case.[324] However, these cases cannot be enforced per se, rather analogy is needed to be made. The rule of due diligence for has received significant consideration for including it in the Tallin Manual 2.[325] According to the Manual, A State is under the obligation of due diligence, in not permitting its territory or cyber infrastructure within its control to be exploited for cyber operations, with harmful effects to the rights or serious consequences for other State. In order for the State to comply with its obligation, it has to adopt all measures that suffice to terminate such activities.[326]

The primary sources of international law are treaties, general principles of law and custom, the third of which in order to apply in a binding manner, requires *opinio juris*, meaning that that this norm is a state practice honored in a sense of legal obligation. The subsidiary sources of international law are judgments and academic work. Due to the contemporary nature and fast paced development of cyberspace and its aspects, there is an absence in international regulation such as treaties that set out the rights and obligations of State in their Cyber-related activities.[327] On account of this lack of treaty regime and the tedious, treaty-making procedures, a recourse to contribution of customary international law related to due diligence is reasonable.

A Judgement of ICJ that may be relevant to customary international cybersecurity Law is *Nicaragua v. United States* case *(Nicaragua),* regarding the dispute over US participation to the rebellion affair in Nicaragua. In that case the ICJ found that State obligations deriving from customary international law, have to stem from coherent and extended State practice executed out of the sense that this act or omission is required by international law(*opinion juris*).[328] When State practice and *opinion juris* are combined with a significant number of States performing in the same manner, without explicit refutation by a number of other States , customary international obligations are born. That combination suggests that there is a consensus amongst the international community regarding the binding character of that state practice, under international law.

However, the evidence of *opinion juris* in the cyber context is a challenging task. Already mentioned above, there are few international cybersecurity legal frameworks and the rapid technological advancements prevent States from adopting a time extensive and coherent practice. As the temporal rule is problematic, the alternative is the recognition of broad principles of wide international acceptance, which can be demonstrated by treaties.[329] Still, the existing legal frameworks in the international sphere, rarely touch upon cybersecurity, rather focus on certain aspects such as cybercrime. Nonetheless, using as a compass cybercrime international agreement such as the Budapest convention, for framing *opinion juris*, regarding obligations that may arise under those treaties such as incorporating cybercrimes into national legislation, indicates that there is an international consensus. That consensus suggests that the penalization of cybercrimes in national legislation is perceived as international obligation. Additionally declarations provoking the ratification of such binding treaties, can evidence the international consensus on the issue. Yet the pursuit of *opinion juris* regarding Cybersecurity is exacerbated by the multidimensional Cyberthreat that entails cybercrime, cyberespionage , cyberterrorism and cyberwarfare. Due to the widespread element of Cybersecurity issues, the deficit in *opinion juris* is enhanced, because cyber espionage is unregulated outside of the law of war. The issue of a customary international law on Cybersecurity, owing to the shortage of multilateral legal acts can be clarified under relevant ICJ jurisprudence on due diligence.[330]

---

[324] *The Corfu Channel case (UK v Albania)* (1949) Rep 4, 22.

[325] Schmitt and NATO Cooperative Cyber Defence Centre of Excellence. (n 74) r 7.

[326] Geiss and others (n 1) 671.

[327] Scott J Shackelford, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17 Chi. J. Int'l L. 1, 5.

[328] *Military and Paramilitary activities in and against Nicaragua (Nicaragua v United States of America)* (International Court of Justice).

[329] Mitu Gulati, 'How Do Courts Find International Custom' [2013] Duke Law.

[330] Shackelford, Russell and Kuehn (n 327) 8.

A.ICJ Jurisprudence on Due diligence for Cybersecurity

The notion of Cybersecurity Due Diligence can be defined as the "review of the governance, processes and controls, that are in place to secure information assets"[331] From the UN, perspective due diligence is indicated as the voluntary non-binding norm of responsible State Behavior, under which States should not deliberately permit the use of their territory for internationally wrongful acts using ICTs.[332] Due diligence in cybersecurity can be perceived as the customary national and international obligations of the State, to devise and implement practices and mechanisms efficient for promoting Cyberpeace through improving its ICT infrastructures. This obligation is imposed upon the State in favor of other States and non-State actors. Albeit ICJ has not established cybersecurity due diligence requirements, its previous related judgements function as precedents and provide guidelines in implementing due diligence in an adjusting to cyber related disputed. The cases were brought before ICJ, long before the emergence of cyberattacks or other cyberthreats, but their applicability can still be found in the context of cyberspace. Therein, three international obligations were identified that might apply to cyberspace and these are the duty to warn, the "no-harm" principle and the non-intervention principle.

The first Case is the aforementioned above *Corfu Channel Case*.[333] The background of the case related to the sinking of two British warships due to mines at an international strait located in Albanian Territorial water. GB started proceedings with the ICJ against Albanian government on grounds of violation of the right of innocent passage and of the duty of Albanian government to notify the British of the mines existence. The Court held that Albanian government should have been aware of the mines existence and therefore were obliged to warn the British warships. The basis on its decision was the general and well recognized principle, that it is "every state obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"[334]. This obligation can be applied in the cybersecurity context as in a duty between States , that the host State must warn the other States that operate in its networks of exposures and Cyberthreats that is aware of. An extension to that could be a duty to warn for all vulnerabilities that a State is aware of in other State networks.

The second Case which corresponds to the "no-harm" principle and it is the *Trail Smelter* Case.[335] The dispute related to the release of environmentally danger materials across the US-Canadian border, questioning the context of obligations of neighboring states. In this instance, the early conflict of territorial sovereignty and contemporary notions of jurisdiction on activities with effects domestically is discussed. The Arbitral Court found that a State has no right to use or permit the use of its territory that may cause injury or damage to the territory of another state when that damage is substantial and supplemented by clear and convincing evidence. The "no harm principle", conceived in the case, despite being related to environmental harm, it may find broader application, for State obligations to avoid engaging into or forbid domestic activities that could amount to severe international repercussions. Adjusted to Cybersecurity context, activities in Cyber Domain of one State , that could exceed its boundaries and infect other states, if so, may constitute a violation of the offending State due diligence duty based on the "no harm" principle. The offending state is obliged beforehand to diminish the threat, and not to prevent it or

---

[331] Tim Ryan, 'Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks Http://Blog.Kroll.Com/2015/Cyber-Due-Diligence-Pre-Transaction- Assessments-Can-Uncover-Costly-Risks/.' (*KROLL CALL*, 28 January 2015) <http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction- assessments-can-uncover-costly-risks/.>.

[332] Antonio Coco and Talita de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771, 772; Secretary-General and Security (n 322).

[333] *The Corfu Channel case (UK v Albania)* (n 324).

[334] *ibid 22.*

[335] *Trail smelter (United States, Canada)* [1965] Arbitrary Court 3 RJAA 1905.

compensate the caused damage.[336] Similar with environmental pollution, overuse of cyberactivity can have negative side effects such as spam messages causing problems in bandwidth. Contrary to that argument, due to the difficulties in attribution of cyber-originating harms and controlling them in the cyberspace, the principle in question could be inapplicable in the cybersecurity, in case of States with low levels of cyber capabilities.[337]

The third case is again an already mentioned one, the Nicaragua Case, which is hazier and potentially more profound, regarding the cybersecurity due diligence obligation in ICJ Jurisprudence. Under the case, the principle of non-intervention and the importance of State Sovereignty were acknowledged. The court held that States are obligated under international law to refrain from involvement in the in the interior affairs of other states, in case that intervention relates with the choice of a political, economic ,social and cultural system or a foreign policy.[338] The principle of non-intervention causes a tension in the context of cybersecurity, that is a part of a great debate, with States claiming several degrees of control over the freedom in cyberspace and other stakeholders of the cyberspace such as individuals and the private sector, advocate the global network commons.[339] The notion of what constitutes cyber non-intervention is still vague. Except from the cyber operation that surpass the threshold of the armed conflict, most of the cyberactivity can evolve in an invading way against State Sovereignty. Also affirmed by the Tallin Manual cyber operations that are below the verge of armed conflict are still interventions, such as the cyber weapon Stuxnet, destined to target Iranian Nuclear facilities.[340]

The inherent characteristic of an intervention to constitute a breach to State sovereignty is that it has to be coercive towards State activities. As committing economic espionage is facilitated with the use of cyber technology, the possibility of it being perceived as coercive intervention is considered, since it may hamper the economy of the foreign State.[341] Further, a cyber-intervention executed indirectly may violate a State's international obligation. For instance the Arab Spring revolutions of the 2010, were assisted partly and mobilized indirectly through the use of social media, owned by US companies, which served liberal views of the west such as free speech and activists exploited their far-reached abilities in preparation of their fight.[342] This was not attributable to US government though. An interesting case that relates to a cyber intervention is the production and free circulation of the software TOR, that allows secure and anonymous online communication online. Hence it can be used by individuals that reside in countries with strict law on freedom of expressions online. TOR was developed by USA navy and it was the US policy to permit the free distribution of the software online. This could constitute a cyber intervention under the principle in discussion. On the other side, having the above concepts as examples for intervention , there is a consensus regarding the international obligations imposed not upon the offending state to cease the emission of the Cyber intervention but the victim state has to alleviate itself from the intervention. For instance Iran and other countries , either blocked Twitter within their network or specifically demanded it to censor content within their territory, based on the speed-restricting policies they impose. That indicates a de jure open Internet as the default , and if another State intends for a more restrictive web, it should be one to take action.[343]

---

[336] Coco and de Souza Dias (n 332) 794.

[337] Shackelford, Russell and Kuehn (n 327) 11.

[338] *Military and Paramilitary activities in and against Nicaragua (Nicaragua v. United States of America).* (n 328).

[339] James A Lewis, 'Why Privacy and Cyber Security Clash' [2011] America's cyber future: security and prosperity in the information age 123.

[340] Jordan Peagler, 'The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law Notes' (2014) 31 Arizona Journal of International and Comparative Law 399, 414.

[341] Catherine Lotrionte, 'Countering State-Sponsored Cyber Economic Espionage under International Law' (2014) 40 NCJ Int'l L. & Com. Reg. 443.

[342] Gilad Lotan and others, 'The Arab Spring| the Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions' (2011) 5 International journal of communication 31.

[343] Shackelford, Russell and Kuehn (n 327) 16.

To sum up, the three principles and the corresponding case law of the ICJ can find application within the context of Cybersecurity. However, there needs to be a further clarification regarding what constitutes a cyber intervention. Regarding the development of Customary international law for Cybersecurity, since the temporal dilemma is inherent to technology, the solution would be brought by the development of more international legal acts regulating Cybersecurity, so more legal bases can be found for universally accepted legal obligations. In the perspective with EU law now, there is a small volume of jurisprudence of the CJEU touching upon issues related to Cybersecurity. One of the most prominent is the Google VS Spain regarding of the right to be forgotten.[344] The CJEU ruled that European citizens are entitled to demand from commercial search firms, that collect data for profit reasons, to remove links to private information if asked and the information is no longer relevant. Also the Court held that the right to privacy supersedes the value of economic interest and the public interest in access to information.

Concluding Remarks

The research over Cybersecurity legal frameworks requires first and foremost the complete understanding of the notion of Security from the legal perspective along with Peace and its subsets State, Collective and Human Security, in order for the contemporary challenge of Cybersecurity to be clarified. In this regard, peace and security signify the primary aim of UN Chapter, for the achievement of stability, avoidance of war, protection of Human rights and prosperity for all mankind. The subcategories of security, State, Human and Collective security each one with its individual focus, all instill the notion of security and its necessity for the State, the individual and the international community respectively. Cybersecurity has been in the spotlight in the last decade with several cyberattacks taking place, inflicting State infrastructures, private entities and individuals alike and causing physical damage to information systems and economic harm to private entities and individuals alike.

Despite the attention turned on it there is still no consensus amongst the stakeholders, id est states, academia, international community and regional organization in respect of its notion. The concept of Cybersecurity for each "occupant" complies with their function and personal agenda. Hence, Cybersecurity for EU is conceived from a financial perspective. Its adjacent terms such as cyber-warfare or cyber-surveillance are not defined either in a commonly accepted manner. This disunity exacerbates the whole regulatory procedure, even if it is attempted at global or national level. A further intimidating factor in the regulatory attempt, is its complex and multifaceted dimension, which in addition to the cross-border element and fast-paced development, surpass governmental and supranational traditional *modus operandi.* The challenges continue in the form of legal notions being transformed for their introduction to cybersecurity norms. Nonetheless, States and international organizations managed to structure legal systems regulating Cybersecurity. USA, Russia and China are the most important state actors in the Cyberdomain. Regional organizations such as the African Union, ASEAN, or Shanghai Cooperation Organization have made significant steps in terms of Cyberspace regulation.

The most comprehensive framework is adopted from the European Union, in terms of Institutions and Legal acts. Cybersecurity has become a priority in the EU agenda. Numerous policies have been adopted. The EUCSS, the 2020 EU Security Union Strategy, the 2020 New Cybersecurity strategy, are a strong indication of the policy shift towards the Digital world and an affirmation of the Cyberdomain presence in our everyday lives. Institutional wise, a noteworthy amount of work of EU main organs and agencies is devoted in the area of Cybersecurity. Despite the lack of an explicit conferral of competence related to Cybersecurity under EU primary law, EU managed by drawing legal basis to other shared or exclusive competences to produce substantial work in terms of legal acts. The legislative branch of EU, and especially EC has

[344] *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECJ Case C-131/12.

contributed to the drafting and adoption of related legal acts. The Directorates-General under EC partake in the policy making and assist in cyber related activities. The establishment of ENISA and its following upgrade to the main Cybersecurity EU agency signifies the aforementioned shift. Its gradual granting of more powers and tasks with legal acts such as the Regulation 526/2013 and the NIS directive in 2016 and last the Reg 2019/881 correspond to the severity Cybersecurity issues are confronted in the EU. In the fight against Cybercrime, EU established again a competent agency the EC3, in the auspices of Europol, that facilitate purpose of coordination and cooperation and exchange of information and efficient practices between national law enforcement authorities. The CERT-EU scheme acquired a coordinating role for the CSIRTs of the Member states and became the European safeguard against Cyber-attacks.

In terms of substantive Law, the EU has created a broad and meticulous legal framework engulfing the majority of Cybersecurity dimensions. In the aspect of NIS, there is the NIS directive which succeeded in imposing obligations to digital services providers and empowering ENISA. EU in that area is considering a second improved version NIS. The proposed directive is a sign of the fast-paced technological developments and the fact that law is always on the trail of technology. In the fight against Cybercrime, in spite of its limited competences EU has adopted the Cybercrime directive, which legislates computer related criminal acts, imitating the Budapest Convention. As far as Cyberdefense is related, the EU has made the least important progress, in legislating. This correlates to the CFSP, which still remains an intergovernmental competence for the EU, as it lies in the heart of Sovereignty. Despite that, EU has established EDA, EUMS and has promoted cooperation in the field of Cyberdefense with other international organization such as UN or NATO. Ultimately, as regards to institutions and legal Acts, EU offers a more comprehensive and efficient framework, which apparently will grow stronger and more reliable in the future.

The international legal framework for cybersecurity is severely more fragmented than the European one. Despite that, significant work has been done in the auspices of UN. UNSC and the Task force established under it ,have contributed considerably in the fight against Cyberterrorism and in the rising threat of ICT technology. UNGA, along with its three committees has touched upon Cyberdefense, Cybercrime and Cyberwarfare. Above all, under the UN umbrella, the six GGE and the OEWG have furnished with proposals, initiatives and policies the UN institutions covering with their work the majority of Cybersecurity issues. ECOSOC made minor substantive change and introduced the word Cyber in the UN terminology. ITU covered the technical side of Cybersecurity and promoted relevant initiatives, calling for cooperation, capacity building and the adoption of technical and legal measures. Also developed the cybercrime legislation kit and invigorated the fight against Cyberterrorism. UN legal acts, even if some of them are binding, do not produce the same impact as the European ones, which EU MS are required to implement, unless they are subjected to sanctions.

The only international legal treaty that is of wide acceptance and is binding for its signatory parties in the area of Cybersecurity is the Convention for Cybercrime, in the auspices of CoE. The Budapest convention sets forth a number of computer related crimes, procedural measures and instills transnational cooperation for the prevention of cybercrime. EU MS are parties to the convention. OSCE works in Cybersecurity deal with Cyberterrorism and the use of internet for terrorist purposes. EU in that respect has adopted a similar act and is in deliberations in adopting a second one. Both these will act as a deterrent for Cyberterrorist intentions. NATO's contribution to regulating Cybersecurity is of the highest significance. In its auspices, the Tallin Manuals have been developed and drafted. These acts, serve as guidelines for the implementation of international law to the Cyberspace. Just as significant is the possible cooperation between NATO and EU in the area of Cybersecurity. The pooling of resources, the exchange of information, the avoidance of duplication of efforts are positive outcomes that would work collectively for the common task of Cybersecurity.

Customary international law on Cybersecurity can be cultivated, despite the obstacles that are inherent qualities of technology. The cross-border trait of Cyberoperations and the swift

technological advancements work adversely to the extensive state practice and the *opinio juris* that are necessary to shape customary international law. However the temporal dilemma can be overlooked, if there are international obligations set out in other international treaties, which will indicate that there is *opinion juris*. An area where customary international law is necessary in cyberspace is due diligence. For it, the adjusted application of three principles, the duty to warn, the no harm-principle and the principle of non-intervention, drawn from the ICJ caselaw is necessary. Hence the international obligation of due diligence will be recognized for Cyberspace as well.

To sum up, in my opinion between the two legal frameworks in comparison the more comprehensive and efficient one is the European. The reason for this is linked with the nature of the European Union. It is a supranational organization, whose members have surrendered several of their sovereign powers. That alone permit EU to adopt innovative and extreme measures with binding force for the MS. Moreover EU, has the legal infrastructure and experience in rule making and the resources to employ personnel and academics in preparing and enforcing the Cybersecurity policies. Nevertheless, the impact of international community in regulating Cybersecurity is not negligeable. The cross-border element of Cyberspace exceeds European boundaries. Hence, the existence of rules in other parts of Earth, is necessary, since a Cyberattack might commence from anywhere, travel the web and spread even within EU. Therefore a stronger, universal and of wide acceptance legal instrument for Cybersecurity is needed.

Bibliography:

1.Books, Essays, Articles, Discussion Papers

Bendiek A, 'The EU as a Force for Peace in International Cyber Diplomacy'

Bertuzzi L, 'EU Countries to Call for the Establishment of a Cybersecurity Emergency Fund' (*www.euractiv.com*, 8 March 2022) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-call-for-the-establishment-of-a-cybersecurity-emergency-fund/> accessed 9 September 2022

Christakis T, 'Reinventing Multilateral Cybersecurity Negotiation after the Failure of the UN GGE and Wannacry: The OECD Solution' (*EJIL: Talk!*, 28 February 2018) <https://www.ejiltalk.org/reinventing-multilateral-cybersecurity-negotiation-after-the-failure-of-the-un-gge-and-wannacry-the-oecd-solution/>

Christou G, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (Springer 2016)

Coleman JS, Frankel B and Phillips DL, 'Robert Nozick's Anarchy, State, and Utopia' (1976) 3 Theory and Society 437

Commission on Human Security, 'Human Security Now : Protecting and Empowering People /' vii

COUNCIL OE, 'Convention on Cybercrime. Explanatory Report'

Council of European Union, 'EU Cyber Defence Policy Framework' (2014)

'Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures ': <https://digitallibrary.un.org/record/674820> accessed 26 September 2022

Deni JR, 'NATO's New Trajectories after the Wales Summit' (2014) 44 The US Army War College Quarterly: Parameters 8

Dewar RS, 'Cyber Security in the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern' (PhD Thesis, University of Glasgow 2017)

'DHS Lexicon | Homeland Security' <https://www.dhs.gov/publication/dhs-lexicon> accessed 4 September 2022

Dragomir A-V, 'WHAT'S NEW IN THE NIS 2 DIRECTIVE PROPOSAL COMPARED TO THE OLD NIS DIRECTIVE.' (2021) 9 SEA: Practical Application of Science

Duke S, 'Capabilities and CSDP: Resourcing Political Will or Paper Armies' [2018] *Research Handbook on the EU's Common Foreign and Security Policy* 154

'ESIL Reflection: The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? – European Society of International Law | Société Européenne de Droit International' <https://esil-sedi.eu/esil-reflection-the-codification-of-the-international-law-applicable-to-cyber-operations-a-matter-for-the-ilc/> accessed 25 September 2022

European Defence Agency, ‘Capability Development Plan’ (2010)

Farwell JP and Rohozinski R, ‘Stuxnet and the Future of Cyber War’ (2011) 53 Survival 23

Fawn R and Larkins J (eds), *International Society after the Cold War. Anarchy and Order Reconsidered* (Macmillan Publishers (incl Palgrave, Picador) 1996)

Fuster GG and Jasmontaite L, ‘Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights’ in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity* (Springer International Publishing 2020)

Geiss R and others (eds), *The Oxford Handbook of the International Law of Global Security* (First edition, Oxford University Press 2021)

Goodrich LM, Hambro EI and Simons AP, *Charter of the United Nations: Commentary and Documents* (3d and rev. ed edn, Columbia University Press 1969)

Gruodytė E and Bilius M, ‘Investigating Cybercrimes: Theoretical and Practical Issues’ in Tanel Kerikmäe (ed), *Regulating eTechnologies in the European Union: Normative Realities and Trends* (Springer International Publishing 2014)

Gulati M, ‘How Do Courts Find International Custom’ [2013] Duke Law

Handl G, Zekoll J and Zumbansen P, ‘Beyond Territoriality: Transnational Legal Authority in an Age of Globalization’ [2012] Books

Hemmings AD, Rothwell DR and Scott KN (eds), Antarctic Security in the Twenty-First Century: Legal and Policy Perspectives (Routledge 2012)

Henderson C, ‘The United Nations and the Regulation of Cyber-Security’, *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00041.xml>

Hill R, ‘Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT’, *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (2015)

Hill S, ‘Chapter 24: NATO and the International Law of Cyber Defence’, *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00037.xml>

Kastner P and Mégret F, ‘Chapter 12: International Legal Dimensions of Cybercrime’, *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) <https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00022.xml>

Lewis JA, ‘Why Privacy and Cyber Security Clash’ [2011] America’s cyber future: security and prosperity in the information age 123

Man TC, ‘The Use of Legal Competences for Cyber-Security Policy by the EU’

Management Board, ‘ENISA Programming Document 2017-2019’ (ENISA 2016)

Manjikian M, ‘The United States: A Declining Hegemon in Cyberspace?’, *Routledge Companion to Global Cyber-Security Strategy* (Routledge 2021)

Maurer T, ‘Cyber Norm Emergence at the United Nations—an Analysis of the Activities at the UN Regarding Cyber-Security [in:] Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project’ (Discussion Paper 2011)

Melzer N and Research UNI for D, *Cyberwarfare and International Law* (UNIDIR 2011)

‘New EU Cybersecurity Strategy’ (European Commission - European Commission)

‘New Rules to Boost Cybersecurity and Information Security’ (*European Commission - European Commission*)

‘Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive’ (*Just Security*, 28 February 2020) <https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counterproductive

Nunes IF and others, ‘EU-NATO Cooperation’ (National Defense Institute of Portugal 2021) <https://www.jstor.org/stable/resrep39891>

Odermatt J, ‘The European Union as a Cybersecurity Actor’ [2018] *Research Handbook on the EU’s Common Foreign and Security Policy* 354

Prakash R, ‘The UN and Cyberspace Governance’

Programme) U (United ND, ‘Human Development Report 1994’ [1994] UNDP (United Nations Development Programme)

PRZETACZNIK Jakub, ‘Russia’s War on Ukraine: Timeline of Cyber-Attacks’ (European Parliamentary Research Service 2022) <https://policycommons.net/artifacts/2476881/russias-war-on-ukraine/>

Public M, ‘Buzan, Waever and De Wilde 1998 Security - A New Framework for Analysis’

Pupillo L and others, ‘Strengthening the EU’s Cyber Defence Capabilities’ (26 November 2018) <https://papers.ssrn.com/abstract=3300625>

Radoniewicz F, ‘International Regulations of Cybersecurity’ in Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz and Tadeusz Zieliński (eds), *Cybersecurity in Poland: Legal Aspects* (Springer International Publishing 2022)

Renard T, ‘The Rise of Cyber Diplomacy: The EU, Its Strategic Partners and Cybersecurity’ [2014] European Strategic Partnership Observatory Working Paper 7

Robinson N, ‘European CyberSecurity Policy’ [2010] *Cybersecurity* 159 (CRC Press 2011)

Rothwell D, Scott K and Hemmings A, ‘The Search for “Antarctic Security”.’ (2012), *Antarctic Security in the Twenty-First Century: Legal and Policy Perspectives.* (Routledge 2012)

Ryan T, ‘CyberDue Diligence:Pre-Transaction Assessments Can Uncover Costly Risks Http://Blog.Kroll.Com/2015/Cyber-Due-Diligence-Pre-Transaction- Assessments-Can-Uncover-Costly-Risks/.’ (*KROLL CALL*, 28 January 2015) <http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction- assessments-can-uncover-costly-risks/.>

]Sanchez G, ‘Case Study: Critical Controls That Sony Should Have Implemented’ [2015] SANS INSTITUTE <https://www.sans.org/white-papers/36022/>

Sari A, ‘The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats’ (10 June 2019) <https://papers.ssrn.com/abstract=3401995>

Savin A, ‘Chapter 10: Cybercrime and Cybersecurity’, *EU Internet Law* (Edward Elgar Publishing 2020) <https://www.elgaronline.com/view/9781789908565.00016.xml>

Schmitt MN and NATO Cooperative Cyber Defence Centre of Excellence., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017)

Simma B and others (eds), *The Charter of the United Nations: A Commentary* (Third edition, Oxford University Press 2012)

Soesanto FD Stefan, ‘The UN GGE Is Dead: Time to Fall Forward – European Council on Foreign Relations’ (*ECFR*, 15 August 2017) <https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/>

Taylor TM Kathryn, ‘Outlook on International Cyber Norms: Three Avenues for Future Progress’ Carnegie Endowment for International Peace <https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704>

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, ‘SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Overview of Cybersecurity’

Thakur R, The United Nations, Peace and Security: From Collective Security to the Responsibility to Protect (2nd edn, Cambridge University Press 2016)

‘The Trouble with Cyber Arms Control’ (*The New Atlantis*) <https://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control>

Tikk E and Nagelhus Schia N, ‘Chapter 30 The Role of the UN Security Council in Cybersecurity: International Peace and Security in the Digital Age’ *ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY* (Routledge 2020)

UN GGE on Cybersecurity: The End of an Era?’ <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> accessed 25 September 2022

UNODA, ‘Disarmament Study Series: No. 33 – Developments in the Field of Information and Telecommunication in the Context of International Security’ (United Nations 2011)

Vissagio L, ‘Hacking the Infrastructure Cyber-Attack, Physical Damage’

Wessel RA, ‘Towards EU Cybersecurity Law: Regulating a New Policy Field’ [2015] *Research Handbook on International Law and Cyberspace* 403

——, ‘European Law and Cyberspace’, *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) <http://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00036.xml>

Wessel RA and Odermatt J, 'The European Union's Engagement with Other International Institutions' [2019] *Research Handbook on the European Union and International Organizations* (Edward Elgar Publishing 2019)

'What We Do - Communications Networks, Content and Technology' (*European Commission - European Commission*) <https://ec.europa.eu/info/departments/communications-networks-content-and-technology/what-we-do-communications-networks-content-and-technology_en> accessed 15 September 2022

White ND, 'The Ties That Bind: The EU, the UN and International Law' (2006) 37 Netherlands Yearbook of International Law <https://nottingham-repository.worktribe.com/index.php/output/1019752/the-ties-that-bind-the-eu-the-un-and-international-law> accessed 28 August 2022

Whyte C, 'European Union: Policy, Cohesion, and Supranational Experiences with Cybersecurity', *Routledge Companion to Global Cyber-Security Strategy* (Routledge 2021)

Wilt H and Klip A, '*Harmonisation and Harmonising Measures in Criminal Law'* [2003] Nederlands Tijdschrift Voor Traumatologie

'World Internet Users Statistics and 2022 World Population Stats' https://www.internetworldstats.com/stats.htm

2. Journals:

Bederna Z and Rajnai Z, 'Analysis of the Cybersecurity Ecosystem in the European Union' (2022) 3 International Cybersecurity Law Review 35

Bendiek A, Bossong R and Schulze M, 'The EU's Revised Cybersecurity Strategy' (2017) 47 Stiftung Wissenschaft und Politik (SWP) Comments

Bossong R and Wagner B, 'A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU' (2017) 67 Crime, Law and Social Change 265

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 211

——, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 Journal of Conflict and Security Law 429

Carrapico H and Barrinha A, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 JCMS: Journal of Common Market Studies 1254

Caspar A, Antonov A and for European Integration Studies C, 'ZEI Discussion Paper C 253: Towards Conceptualizing EU Cybersecurity Law' (2019) C 253 / 2019

'Certain Expenses of the United Nations' (1962) 151 ICJ REP

Chiara PG, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) 36 International Review of Law, Computers & Technology 118

Coco A and de Souza Dias T, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771

Cole MD and Schmitz S, 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape' (31 December 2019) <https://papers.ssrn.com/abstract=3512093> accessed 18 September 2022

Cram L, 'The European Commission as a Multi-organization: Social Policy and IT Policy in the EU' (1994) 1 Journal of European Public Policy 195

Dunn-Cavelty M and Suter M, 'Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection' (2009) 2 International Journal of Critical Infrastructure Protection 179

Finlay L and Payne C, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 AJIL Unbound 202

Fleck D, 'Searching for International Rules Applicable to Cyber Warfare—a Critical First Assessment of the New Tallinn Manual' (2013) 18 Journal of Conflict and Security Law 331

Gercke M, 'Europe's Legal Approaches to Cybercrime' (2009) 10 ERA Forum 409

Ghafur S and others, 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS' (2019) 2 npj Digital Medicine 98

Henriksen A, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5 Journal of Cybersecurity

Herzog S, 'Revisiting the Estonian Cyber Attacks' (2011) 4 Journal of Strategic Security 49

Ilves LK and others, 'European Union and Nato Global Cybersecurity Challenges' (2016) 6 Prism 126

Javier Solana, 'Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -' (EEAS 2008)

Johnstone I, 'Security Council Deliberations: The Power of the Better Argument' (2003) 14 European Journal of International Law 437

Kettemann MC, 'ENSURING CYBERSECURITY THROUGH INTERNATIONAL LAW' (2017) 69 Revista Española de Derecho Internacional 281

Kosseff J, 'Defining Cybersecurity Law' 103 IOWA LAW REVIEW 47

Kovács L, 'Cyber Security Policy and Strategy in the European Union and NATO' (2018) 23 Land Forces Academy Review 16

Lotan G and others, 'The Arab Spring| the Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions' (2011) 5 International journal of communication 31

Lotrionte C, 'Countering State-Sponsored Cyber Economic Espionage under International Law' (2014) 40 NCJ Int'l L. & Com. Reg. 443

Markopoulou D, Papakonstantinou V and de Hert P, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 105336

McKune S and Ahmed S, 'Authoritarian Practices in the Digital Age| The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda' (2018) 12 International Journal of Communication 21

Niemann A and Zaun N, 'EU Refugee Policies and Politics in Times of Crisis: Theoretical and Empirical Perspectives: EU Refugee Policies in Times of Crisis' (2018) 56 JCMS: Journal of Common Market Studies 3

'Nigel D. White,Collective Security Law(The Library of Essays in International Law), Ashgate, 2003, 589 Pp. Hardback, ISBN 0754622355' (2006) 10 Journal of International Peacekeeping 203

O'Connell ME, 'Cyber Security without Cyber War' (2012) 17 Journal of Conflict and Security Law 187

Oosthuizen GH, 'Playing the Devil's Advocate: The United Nations Security Council Is Unbound by Law' (1999) 12 Leiden Journal of International Law 549

Orji UJ, 'The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability' (2018) 12 Masaryk University Journal of Law and Technology 91

Peagler J, 'The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law Notes' (2014) 31 Arizona Journal of International and Comparative Law 399

Poptchev P, 'NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages' (2020) 45 Information & Security: An International Journal 35

Rossi LS, '"Same Legal Value as the Treaties"? Rank, Primacy, and Direct Effects of the EU Charter of Fundamental Rights' (2017) 18 German Law Journal 771

Sanchez G, 'Case Study: Critical Controls That Sony Should Have Implemented' [2015] SANS INSTITUTE <https://www.sans.org/white-papers/36022/>

Saqib N and others, 'Mapping of the Security Requirements of GDPR and NISD' (2020) 7 EAI Endorsed Transactions on Security and Safety

Schmitz-Berndt S and Schiffner S, 'Don't Tell Them Now (or at All) – Responsible Disclosure of Security Incidents under NIS Directive and GDPR' (2021) 35 International Review of Law, Computers & Technology 101

Shackelford SJ, Russell S and Kuehn A, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17 Chi. J. Int'l L. 1

Sliwinski KF, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35 Contemporary Security Policy 468

Spector P, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017) 111 AJIL Unbound 219

Stadnik I, 'What Is an International Cybersecurity Regime and How We Can Achieve It' (2017) 11 Masaryk University Journal of Law and Technology 129

Stewart E and Mulvey G, 'Seeking Safety beyond Refuge: The Impact of Immigration and Citizenship Policy upon Refugees in the UK' (2014) 40 Journal of Ethnic and Migration Studies 1023

Sullivan JE and Kamensky D, ‘How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid’ (2017) 30 The Electricity Journal 30

Trautman LJ and Ormerod PC, ‘Wannacry, Ransomware, and the Emerging Threat to Corporations’ (2018) 86 Tennessee Law Review 503

Weber RH and Studer E, ‘Cybersecurity in the Internet of Things: Legal Aspects’ (2016) 32 Computer Law & Security Review 715

3. Legal acts and Caselaw

GGE U, ‘Report on UNGA Res 68/243’ (United Nations 2013)

Secretary-General U and Security UG of GE on D in the F of I and T in the C of I, ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ’:

Sess.: 1998-1999) UNGA (53rd, ‘Developments in the Field of Information and Telecommunications in the Context of International Security ’:

Sess.: 2000-2001) UNGA (55th, ‘An Effective International Legal Instrument against Corruption ’:

Sess.: 2002-2003) UNGA (57th, ‘Creation of a Global Culture of Cybersecurity ’:

——, ‘Creation of a Global Culture of Cybersecurity ’:

Sess.: 2003-2004) UNGA (58th, ‘Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures ’:

Sess.: 2005-2006) UNGA (60th, ‘The United Nations Global Counter-Terrorism Strategy ’:

Sess.: 2013-2014) UNGA (68th, ‘The Right to Privacy in the Digital Age ’:

Sess.: 2018-2019) UNGA (73rd, ‘Countering the Use of Information and Communications Technologies for Criminal Purposes ’:

Sess.: 2019-2020) UNGA (74th, ‘Countering the Use of Information and Communications Technologies for Criminal Purposes ’:

‘Tunis Agenda for the Information Society’

UN General Assembly, ‘International Covenant on Civil and Political Rights’ (United Nations 1966) vol 993

——, ‘International Covenant on Economic, Social and Cultural Rights’ (United Nations 1966) 993

UN General Assembly (3rd sess. : 1948-1949 : Paris E), ‘Universal Declaration of Human Rights’

UNGA, ‘Resolution 53/70’ (United Nations 1999)

——, ‘Resolution 58/32’ (United Nations 2003)

——, ‘Report by the Secretary in Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (United Nations 2005) UN Doc A/60/202

——, ‘Resolution 65/41’ (United Nations 2010)

——, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (United Nations 2010) UN Doc A/65/201, 4.

——, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (2015) UN Doc A/70/174

——, ‘Resolution 70/237’ (United Nations 2015) 70/237

——, ‘Resolution 73/27’ (United Nations 2018) 73/27

——, ‘Resolution 73/266’ (United Nations 2018) 73/266

United Nations, ‘Charter of the United Nations’ (United Nations 1945)

Year: 2001) USC (56th, ‘Resolution 1373 (2001) /’ <https://digitallibrary.un.org/record/449020> accessed 26 September 2022

Commission of the European Communities v Council of the European Union [2005] ECJ Case C-176/03

Criminal proceedings against Maria Pupino [2005] ECJ Case C-105/03

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECJ Case C-131/12

Military and Paramilitary activities in and against Nicaragua (Nicaragua v United States of America) (International Court of Justice)

The Corfu Channel case (UK v Albania) (1949) Rep 4, 22

Trail smelter (United States, Canada) [1965] Arbitrary Court 3 RJAA 1905

United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union [2006] ECJ Case C-217/04

Communication From the Commission To The Council And The European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre 2012

Communication From the Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime 2000

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach 2001

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Digital Agenda for Europe 2010

Communication From the Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Single Market Strategy for Europe 2015

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' {SEC(2009) 399} {SEC(2009) 400} 2009

Communication from the Commission to the European Parliament, the Council, the European Economic and Eocial committee and the Ecommittee of the Regions the European Agenda on Security 2015

Communication From the Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions On The Eu Security Union Strategy 2020

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector 1997

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA 2013

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 2016

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

Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA 2019

Europe - An information society for all - Communication on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000, 1999

European Parliament resolution of 22 November 2012 on the EU's mutual defense and solidarity clauses: political and operational dimensions (2012/2223(INI)) 2012

European Parliament resolution of 23 November 2016 on the implementation of the Common Security and Defence Policy (based on the Annual Report from the Council to the European Parliament on the Common Foreign and Security Policy) (2016/2067(INI)) 2016

Joint Communication to The European Parliament And The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU 2017

Joint Communication to The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013

Proposal for a Directive of The European Parliament And Of The Council concerning measures to ensure a high common level of network and information security across the Union 2013

Proposal for a Directive of The European Parliament And Of The Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings 2018

Proposal for a Directive of The European Parliament And Of The Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 2020

Proposal for a Directive of The European Parliament And Of The Council on the resilience of critical entities 2020

Proposal for a Regulation of The European Parliament And Of The Council on European Production and Preservation Orders for electronic evidence in criminal matters 2018

Proposal for a Regulation of The European Parliament And Of The Council on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, 2018

Reflection Paper on The Future Of European Defence 2017

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact 2018 (OJ L)

Consolidated version of the Treaty on European Union 2012 (OJ C)

Consolidated version of the Treaty on the Functioning of the European Union 2012 (OJ C)

Convention on Cyber Security and Personal Data Protection 2014

Convention on Cybercrime 2004 (ETS No 185)

Council Decision of 29 May 2000 to combat child pornography on the Internet 2000 (OJ L)

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems 2005 (OJ L)

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) 2004 (OJ L)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) 2016 (OJ L)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2019 (OJ L)

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance 2013 (OJ L)

2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment 2001 (OJ L)