The EU's legal approach to protecting critical infrastructure from state-sponsored cyberattacks: a comparative study of the UK, Italy and Bulgaria

Eva Saeva

Student number: 160588521

Programme: 8230P PhD SLAW (PT)

Supervisors: Sylvia de Mars and Colin Murray

Newcastle Law School

Doctoral thesis

2024

Table of Contents

Chapter 1: INTRODUCTION

1.1.Background to Thesis

1.1.1. Addressing cyber threats: national and international developments

This thesis examines the EU's legal approach to cybersecurity. It analyses the long road the EU has walked towards regulating cybersecurity and the challenges – both internal and external - it encountered along the way and which shaped its regulatory framework. It focuses on malicious state-sponsored cyber operations targeting the critical infrastructure (CI) sectors.

The developments in the EU regulatory landscape follow the attempts and developments at international level to address the topic of cybersecurity and cyberspaces' regulation. Although these topics have only come to prominence in the political and regulatory agenda at international level in the 2010s, "hackers" – with the term initially having a positive connotation as people that were skilful at computer programming - emerged in the 1950s at the US Massachusetts Institute of Technology's Artificial Intelligence Laboratory.[1] Computer viruses, predecessors of those malicious viruses of today, have emerged in the early 1970s,[2] with the term "virus" used for the first time in 1984 to refer to a self-replicating code.[3] Soon the misuse of computer devices reached a level regulators could no longer ignore: by 1990 about 200 viruses were identified.[4] The majority were not state-sponsored – at the time cyberattacks, as we would define them today, were attacks aimed at personal and economic gain.

Thus, computer misuse regulation began to appear across legislative frameworks worldwide: regulators were slowly but steadily realising that already existing norms were proving insufficient. For instance, Canada added "unauthorized use of computer" to the Criminal Code in

[1] Susan W Brenner, '25 - History of computer crime' in Karl De Leeuw and Jan Bergstra (eds), *The History of Information Security* (Elsevier Science B.V. 2007) 706.
[2] Jun Osawa, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?' (2017) 24 Asia-Pacific Review 113, 114.
[3] Brenner 709.
[4] Ibid 710.

1985;[5] the US followed suit in 1986 adopting the Computer Fraud and Abuse Act,[6] and the UK adopted the Computer Misuse Act in 1990.[7] Similarly, Italy amended its Penal Code in 1993,[8] Russia introduced its Criminal Code in 1996,[9] China introduced its Penal Code in 1997,[10] Germany amended its Criminal Code in 1998,[11] and Bulgaria amended its Penal Code in 2002[12] – all introducing new provisions regulating computer misuse.

At international level, on the other hand, the first efforts to address the rising threat came from the Organisation for Economic Co-operation and Development (OECD) which focused on harmonising computer crime-related legislative frameworks across its Member States. Its 1986 report recommended that states criminalised attacks on computer systems, the latter's use to commit fraud or forgery, and to infringe software copyrights and gaining unauthorised access to a computer system.[13] In 1989, the Council of Europe also adopted a report on Computer related crime focusing on the same issues (but copyright), adding other criminal acts such as damage to computer data or computer programs, computer sabotage, unauthorised interception, unauthorised reproduction of a topography, unauthorised reproduction of a protected program, and, optionally, the alteration of computer data or programs, computer espionage, unauthorised

[5] Canadian Criminal Code 1985 342.1 (1) states that if a person is proven guilty of using a device with the intent to "fraudulently" obtain access to, intercept or commit an offence, they will be "liable to imprisonment for a term of not more than 10 years".

[6] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers focuses on espionage, unauthorised access to a computer with the purpose of committing a financial fraud, intentionally damaging a computer via a program or a code.

[7] UK Computer Misuse Act 1990 lists unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised modification of computer material.

[8] Italian Penal Code addressed unauthorised access to a computer or electronic systems, unauthorised possession and distribution of access codes to computer or electronic systems, dissemination of programs aimed at damaging or interrupting computer systems, unauthorised interception or interruption of computer or electronic communications, installation of equipment designed to intercept, prevent or interrupt computer or electronic communications, falsification, alteration or suppression of the content of computer or electronic communications, interception of computer or electronic communications, damage to computer or communications systems, computer fraud, and interception of computer or electronic communications.

[9] Russian Criminal Code 1996 Chapter 28 Crimes in the Sphere of Computer Information regulates illegal access to information in computers, their systems and networks; creation, distribution and use of computer malware; and violation of rules of operation of computers, their systems and networks.

[10] Xingan Li, 'Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime ' 9 International Journal of Cyber Criminology 185, 187. The Chinese Penal Law specified that computer crime is a crime in which computer information systems are targets of the crime.

[11] German Criminal Code 1998 regulated computer fraud, data espionage, alteration of data and computer espionage.

[12] Bulgarian Penal Code 1991, amended in 2002, regulated accessing information systems illegally, assessing classified state information, tampering with computer data, publishing personal data, and implanting malware and viruses.

[13] Organisation for Economic Co-operation Development, *Computer-related Crime: Analysis of Legal Policy* (Organisation for Economic Co-operation and Development 1986).

use of a computer, and unauthorised use of a protected computer program.[14] The UN also addressed the topic for the first time in 1990 with its Congress on the Prevention of Crime and the Treatment of Offenders resolution, which affirmed that international action required a "concerted effort by all Member States" and called for the intensification of efforts on effectively combating computer abuses.[15]

The first major international breakthrough though followed in 1997 when the Council of Europe took the initiative again and, after four years of preparatory work, adopted the first ever international legally-binding measure: the Convention on Cybercrime 2001, which regulates illegal access, illegal interception, data and system interference and misuse of devices, "content-related offences" such as child pornography and copyright infringements offenses.[16]

1.1.2. The era of state-sponsored cyberattacks

Whilst governments were trying to find ways to tackle the rising threats individually and collectively, some of them realised that cyberspace and cyber operations could be used as advantageous political instruments in their relations with allies and adversaries alike. Orchestrating cyber operations became an important tool in the governmental arsenal of the most developed countries. By the mid-1990s, the possibility of cyber warfare was already on the agenda of international security affairs specialists.[17] In 1998, one of the first (low-level) state-sponsored attacks was documented: Moonlight Maze, which targeted US military technologies and was believed to be Russian-sponsored.[18] In the early 2000s, the Beijing-sponsored Titan Rain targeted unclassified information across many US government organisations.[19] Then, a sudden change in the international political agenda took place – the 9/11 terrorist attacks shifted the attention of policy makers away from cyber activities, and, despite the adoption of some

[14] Council of Europe's European Committee on Crime Problems, *Computer-related crime* (1990) 5.
[15] United Nations, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (A/CONF.144/28/Rev.1 edn, 1990) 141.
[16] Council of Europe, *Convenition on Cybercrime* (2001)
[17] Michael N. Schmitt, 'The Law of Cyber Warfare: *Quo Vadis?*' (2014) 25 StanL& Pol'y Rev 269, 269.
[18] Quentin E. Hodgson, Yuliya Shokh and Jonathan Balk, *Many Hands in the Cookie Jar: Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response* (RAND Corporation 2022) 11.
[19] Ibid 25.

(predominantly non-binding) measures at EU level, the topic was not considered an important issue until the first major cyberattack on Estonia in 2007 brought the topic back onto their political agendas.[20]

The debates that followed this cyberattack at international level – both political and scholarly – mainly focused on what laws would apply to this new domain of war: cyberspace was declared by the US as the operational domain for defence activities such as air, land, sea and outer space in 2011.[21] The EU – seemingly – agreed that cyberspace had become the fifth domain of war in 2015[22] and officially stated so in 2018.[23]

1.1.3. Addressing cyber threats: the EU developments

In this international environment, the EU first addressed information and communication technologies (ICT)-related threats back in the 1990s with two European Commission Communications, one on Information Security in 1991 and one on Growth, Competitiveness and Employment in 1993.[24] Security, however, was not the Commission's main concern - the economic impact of cyber threats was.[25] Only in June 2001 did security begin to get significant attention – the European Commission published a Communication which saw security as a "key priority", a "key challenge for policy makers" and a "commodity".[26] But these "key" issues were not followed up on as, as indicated above, the 9/11 attacks rearranged Western governments' priorities. Only in 2004 did the topic appear back on the EU's agenda: the EU adopted the Regulation establishing the European Network and Information Security Agency (ENISA) which became responsible for the "high and effective level of network and information security within the Community (…) for the benefit of the citizens, consumers, enterprises and public sector

[20] Schmitt 269.
[21] Department of Defense, *Strategy for Operating in Cyberspace* (July 2011) 5.
[22] European Defence Agency, *Fact Sheet on Cyber Defence* (10 February 2015) 1.
[23] Council of the EU, *EU Cyber Defence Policy Framework (2018 update)* (19 November 2018) 2.
[24] European Commission, *Proposal for a Council Decision in the Field of Information Security* (1990);
European Commission, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century: White Paper* (1993) 107.
[25] Helena Carrapico and Benjamin Farrand, 'Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy' (2020) 42:8 Journal of European Integration 1111, 1115.
[26] European Commission, *Communication on Network and Information Security: Proposal for A European Policy Approach COM(2001)298 final* (June 2001) 2.

organisations of the European Union"[27], the 2004 European Commission Communication on Critical Infrastructure Protection in the fight against terrorism, underlying the link between the terrorist threat and the growing concerns about cyberattacks performed against the CI sectors,[28]and the 2006 European Commission Communication on Secure Information Society aimed to "revitalise the European Commission strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach".[29] Through what Carrapico and Farrand have called a "layering process",[30] which saw the adoption of other relevant, non-binding, but still very important steps over the next few years – e.g. the 2007 European Parliament Resolution on Estonia,[31] the 2010 Communication on the Internal Security Strategy[32] – the EU was constructing its policy views and regulatory approach to malicious state-sponsored operations. Indeed, computer crime was also included in Article 83(1) of the Treaty on the Functioning of the European Union in 2009.[33]

1.1.3.1. The EU's cybersecurity strategic framework

Historically, security has always been a prerogative of the nation-state. National security and defence have never been a competence of the EU. However, by the early 2010s, cybersecurity was beginning to gain prominence at international level and discussions on the imminent arrival of cyber 9/11[34] and cyber Pearl Harbor[35] were taken seriously also in the EU. The first

[27] 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, Article 1 1.
[28] Communication from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final of 20 October 2004.
[29] European Commission, *Communication on A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" {SEC(2006) 656}* (May 2006)
[30] Carrapico and Farrand 1116.
[31] European Parliament, *Resolution on Estonia (P6_TA(2007)0215)* (24 May 2007).
[32] European Commission, *Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673 final)* (22 November 2010).
[33] Treaty on the Functioning of the EU Article 83 1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension (…)
These areas of crime are the following: (…) **computer crime** and organised crime. (…) [emphasis added]
[34] 'U.S. homeland chief: cyber 9/11 could happen "imminently"' (*Reuters*, 24 January 2013) <https://www.reuters.com/article/idUSBRE90N1A4/> accessed 29 December 2023.

Cybersecurity Strategy of the EU was adopted in 2013.[36] To "address cybersecurity in a comprehensive fashion", it split "activities" into three main pillars: network and information security (NIS), law enforcement and defence.[37] It also included the proposal for a Network and Information Systems Directive (NIS Directive).[38] When the research for this thesis was commencing, there was little evidence that the defence pillar would effectively take off as a standalone legislative approach in the EU. As an alternative, the development of an EU-level cyber diplomacy approach was taking considerable shape in 2017 and this study therefore focused on it. The three pillars were later abolished with the EU Cybersecurity Strategy 2020 which adopted a more "thematic" approach by focusing on resilience, capacity building and advancing an open cyberspace,[39] which reflect the legislative efforts both in NIS and the cyber diplomacy fields. Cyber defence was once again featured, but because it has remained in an embryonic form until the end of the research period of this thesis, this thesis does not focus on EU developments in this area.

A) Regulating cybersecurity: the first legally binding steps

The European Commission argued that a legally binding approach to network and information security would protect the EU consumers, businesses and governments from cyber incidents, and would create a climate of "mutual trust" that would ensure "adequate preparedness" at national level.[40] After 3 years of negotiations the very first EU cybersecurity law was adopted: the NIS Directive 2016. It introduced cybersecurity risk management and incident reporting mechanisms for companies providing services for the critical infrastructure (CI) sectors and invited Member States to re-organise their own institutional cybersecurity architectures. The EU was therefore

---

[35] David E. Sanger and Nicole Perlroth, 'Cyberattacks Against U.S. Corporations Are on the Rise' (*The New York Times*, 12 May 2013) <www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html> accessed 29 December 2023.

[36] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (7 February 2013).

[37] Ibid 17.

[38] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union (NIS Directive Proposal) 2013.

[39] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* (16 December 2020) 5.

[40] NIS Directive Proposal 7.

giving a clear indication that it wanted to lead the cybersecurity regulatory approach – which would come at the cost of the MS having to agree that this rather niche area of national security needed to become an area of shared competence with the EU. This was not an easily accepted turn of events by some of the more powerful MS, such as the UK, as will be seen. One of the key elements this thesis analyses is – therefore – the contestation of power between the EU and its MS and the role of the latter in shaping the EU cybersecurity regulatory approach.

B) Regulating cybersecurity: subsequent regulatory steps

A manifestation of the (developing) EU strategic approach thus included legal measures such as the NIS Directive 2016, the Cyber Diplomacy Toolbox 2017, the Cybersecurity Act 2019, the Regulation establishing a Cybersecurity Competence Centre and Network 2021, the NIS2 Directive 2022 and the upcoming Cyber Resilience and Cyber Solidarity Acts. Cybersecurity has also been extensively and increasingly featured in the latest ICT-related legislation such as the GDPR 2016, European Electronic Communications Code 2018, the delegated Regulation to the Radio Equipment Directive 2022, the Digital Operational Resilience Act 2022, and the upcoming Artificial Intelligence (AI) Act, among others. As President von der Leyen announced in 2019, because "cybersecurity and digitalisation are two sides of the same coin", the former has become a "top priority".[41]

1.1.4. Scope of thesis

Against this background, this thesis focuses on state-sponsored attacks on CI sectors and how the EU is building its regulatory framework to deter them. It does not focus on cyber criminality in terms of the law enforcement pillar identified by the EU. It focuses on the NIS pillar – and what it morphed into with the latest EU cyber strategy – as the "internal" dimension of the EU

[41] European Commission, 'Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme' (27 Novembre 2019) <https://ec.europa.eu/commission/presscorner/detail/it/speech_19_6408> accessed 15 January 2024.

approach. As a related sub-topic, the thesis also investigates the EU diplomatic approach to this specific type of cyberattacks - which provides the "external dimension". The aim is to provide a thorough analysis and an integrated picture of the effectiveness of the EU cybersecurity regulatory regime as regards malicious foreign orchestrated cyberattacks on EU soil.

1.2. Research questions

The thesis therefore aims at investigating the following main research question:

What has influenced (facilitated, challenged – and, consequently, deterred) the development of the EU approach to cybersecurity, both internally and externally? This question enables an exploration in further detail of the way the EU approach was shaped and evidences the various variables – internal and external – that influenced the development of the regulatory approach. The "internal" challenges refer to the different security objectives the MS and the different levels of preparedness (legal, technical and operational) had and how these had to be overcome for the MS to agree on an EU-led regulatory approach. The "external" challenges refer to the constant state-sponsored attacks on CI sectors across the EU MS.

To provide the full picture of the EU's legislative efforts towards protecting the CI sectors from state-sponsored cyberattacks, the thesis also looks into the following research sub-questions:

a) *Does the EU's legal approach to cybersecurity effectively interact – and if so, how – with the international efforts to regulate cyberspace*? Cyberspace is a borderless domain: if states approached its regulation individually, this it would create an asymmetric rhetoric and, ultimately, no effective way of tackling state-sponsored cyber threats. This applies to the international community as much as it applies to the EU. This research sub-question therefore addresses how the EU positions itself in the wider regulatory debates and whether its regulatory efforts are heading in the same or similar direction as other international ones.

b) *Has the EU legal regime on cybersecurity proved sufficient in addressing state-sponsored attacks to CI sectors*? This research sub-question will analyse the measures the EU has adopted and whether their implementation across the MS could act as a deterrent for malicious state-sponsored attacks. The questions will thus explore the NIS regulatory framework, as well as the cyber diplomacy and cyber defence frameworks.

c) And ultimately – *can the EU claim the role of a cybersecurity regulator?* This sub-question requires an assessment of the findings of all other research questions so as to determine whether the EU's regulatory framework demonstrates enough robustness, adaptability to this ever-changing domain, to claim the role of a cybersecurity regulator, whose framework is fit to deter effectively malicious foreign-sponsored cyber activity..

1.3. Research method

This thesis is the outcome of a part-time PhD and is therefore the product of a 7-year long research period. Such a long time for research, especially on an ever-evolving topic like cybersecurity, allowed for a more thorough and in-depth analysis, where arguments, discussions and legal frameworks' changes over the course of time have been followed closely. The thesis' cut-off point for analysis is in June 2023, so as to ensure that findings could be thoroughly analysed without having to constantly update the text with the newest regulatory developments. Therefore, this thesis might not have fully engaged with some relevant work (whether primary or secondary) published after the cut-off point.

1.3.1. Methodology

To address the main research question and sub-questions set out above, and to explore if, and if so, why there was a need for an EU-level legal approach to cybersecurity, as well as to explore what factors led to the shape of the EU-level framework, a comparative doctrinal analysis was used. Three case studies have been chosen to showcase three different levels of cybersecurity legal preparedness among the MS. The UK, now a former member state, represents those

Member States with well-developed regulatory frameworks. Italy represents those Member States with some level of preparedness, whereas Bulgaria represents those Member States with the least developed frameworks. This comparative approach best fits the aims of the thesis as one of the key reasons why the EU decided that it should lead the cybersecurity agenda was precisely the different levels of MS' preparedness.[42] The comparative analysis is also supported by the analysing how the securitisation process of the field has occurred in the EU and to what extend its MS have endorsed the EU's advancements in the filed: securitisation theory is therefore referenced (but not tested or challenged as not needed for the purpose of this research).

To achieve the goals set by the comparative study, a desk-based approach was adopted. Research therefore focuses on EU and national laws, international statues and conventions, and international and EU soft law as primary sources. Namely, the thesis will focus on the NIS Directive, the respective national transposition laws (the UK's NIS Regulations, the Italian Legislative decree 65/2018 and the Bulgarian Cybersecurity Act (BCSA)) and also explores pre-existing laws and subsequent legislative steps at national and EU level. Other EU recommendations, Communications, and Decisions on the topic of cybersecurity, as well as the non-binding UN reports adopted by the Group of Governmental Experts, will be examined where appropriate. Secondary sources include academic work in the field of cybersecurity, with focus on, but not limited to, both scholarly works addressing the international efforts of regulating cyberspace and scholarly work on the EU's efforts. Tertiary sources include relevant scholars' blog posts, practitioners' interviews, parliamentary debates and news reports.

1.3.1.1. Case studies

As mentioned, three Member State case studies have been selected to reflect three different levels of cybersecurity preparedness prior to the introduction of the NIS Directive. The UK was among the very few MS that had well-developed cyber capabilities and significant legislation regulating them. Bulgaria, on the other hand, was at the other end of the spectrum, with scarce capabilities and very little legislation. Italy - with its existing secondary legislation on

[42] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 5.

cybersecurity - represents the "mid-level" preparedness, as its regulatory framework could be positioned between those of the UK and Bulgaria.

Examining each state highlights the divergent security objectives these different MS had prior to the adoption of the NIS Directive, and, more importantly, their significantly different views on interpreting cyber threats. The EU had to overcome these inconsistencies between its MS if it wanted to be able to deter the constantly increasing state-sponsored malicious activity on EU soil. Moreover, only by finding the EU-voice among the many different MS voices could the EU become a strong international regulator for cybersecurity which "exports" laws - which the EU has done with regulation in so many other areas. Examining the EU approach from a MS perspective therefore allows for a more thorough analysis, as the MS legislative frameworks were the foundation upon which the EU one was built.

1.4. Original contribution

The topic of cybersecurity has become of ever-growing importance in the seven years it took for this thesis to be completed. Whilst academic work at the start of this investigation focused mainly on what would constitute cyber warfare and whether – and if yes, which – international legal norms would be applicable to this new military domain, in more recent years, scholars have begun focusing also on the EU regulatory developments in the field. Therefore, this thesis will add to a growing scholarship on the EU's approach to *collective cybersecurity*. However, whilst the topic has been analysed mostly from the angle of disciplines such as politics or IR, this study focuses on the legal aspects of how cybersecurity has been regulated in the EU – both *by* the EU and within its Member States. It therefore fills two gaps in existing literature: first – on the role of the MS in shaping the EU regulatory agenda, and second – on the effectiveness of the latter when it comes to CI protection from state-sponsored attacks.

1.4.1. The MS as a key factor in shaping the EU cybersecurity regulatory regime

The thesis takes a bottom-up approach rather than the often used top-down approach in existing literature, and considers the MS's preparedness (legal, technological and operational), views, objectives, interests, activities, fears and bilateral arrangements in and outside of the EU as key factors in creating the EU cybersecurity legislation. By having the MS as a "starting point", the thesis demonstrates how the EU approach was "birthed" and "grew" from the MS's continuous efforts and work, disproving arguments in favour of an EU overly regulating cybersecurity, echoed at times by some of the larger MS,[43] and how it is the MS themselves that are predominantly responsible for the final EU "product". The thesis, in fact, argues that the MS's role has been one of the most important factors in shaping the EU regulatory agenda. It therefore investigates the latter from the prism of the MS, whose role so far has been somewhat downplayed by the existing scholarship, and offers a different perspective as to why the EU cybersecurity laws have been drafted the way they are. Existing literature has not debated enough – and as a standalone issue - the role of the MS as obstructors in the shaping of EU legal regime.

The comparative approach adopted in this study underscores the divergent preparedness and different security objectives among the MS: while the UK's role has been addressed to an extent in the literature, Italy and Bulgaria have been given peripheral importance and not studied enough as being among the *factors* responsible for the development of the EU's legislation. This work therefore fills this gap and demonstrates that even the smaller states, such as Bulgaria, played a significant role. It also highlights the continuous desire for power – both by the EU and by its MS – how it impacted on the EU regulatory agenda, thus adding to the literature on division of competences between the EU and its Member States.

[43] Catherine Stupp, 'Commission should 'walk the walk' on cybersecurity, German chief says' (*EURACTIV*, 9 April 2018) <https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/> accessed 9 January 2024

1.4.2. The effectiveness of the EU cybersecurity regulatory regime

The second contribution the thesis makes is on the effectiveness of the EU regime. The latter is not analysed from the perspective of potential gaps in the NIS Directive's implementation and enforcement across the MS, although these will be addressed in detail. The EU regime is also not analysed *in general*. The main purpose of the thesis is to consider, despite the existing gaps and inconsistencies that have been revealed along the way, the overall effectiveness of the EU legal regime in relation to the protection of the EU's CI sectors from state-sponsored attacks, and whether the EU's regulatory framework is proving effective in deterring malicious operations on EU soil.

Literature on this is rather thin, as when NIS Directive is being considered, it almost always is about the overall scope and objectives, which are not limited to state-sponsored attacks on the CI sectors. This thesis will therefore fill this gap. Here, again, the MS play two key roles: the first is related to the correct implementation and enforcement of the NIS-pillar cybersecurity laws, as weak links can have a cascading effect on other, more prepared, MS. The second, is related to the cyber diplomacy field, which also bears the burden of the divergent MS perspectives on attributing cyberattacks. Both issues will be addressed in detail as literature has not discussed in significant detail whether the EU has become a strong cybersecurity regulator despite years of continuous challenges from within.

1.5. Thesis structure

To respond to the main research question and sub-questions and to address the gaps identified in the literature, the thesis has been structured into five substantial Chapters, alongside this introduction and a conclusion, which will be presented in the form of a final, analytical Chapter, presenting the findings and conclusive arguments of this study.

Chapter II: From cyber warfare to cybersecurity: defining the thresholds of cyberattacks is a theoretical 'background' Chapter: to better understand the EU's legal approach to cyber threats and place it into the bigger picture of international development of norms regulating cyber

issues, an overview of the international cyber law status quo needs to be provided. The Chapter focuses on state-sponsored attacks and the scholarly debates about the applicability of international law to cyber operations falling above and below the threshold to *use of force.* The Chapter also follows the curve state-sponsored cyber operations underwent since the attacks on Estonia in 2007 and splits the content into two main parts: *Phase one: Jus ad bellum and jus in bello in cyberspace*, and *Phase two: Peacetime state-sponsored cyber operations below the use of force threshold*: cyber wars, which were feared after Estonia's attacks never really materialised and state-sponsored attacks have proved to be more impactful when falling below the *use of force* threshold. The Chapter analyses different long-standing principles - the cornerstones of contemporary international law - such as violation of sovereignty, the principle of non-intervention, the *use of force*, proportionality, countermeasures - and discusses how they can be violated by these new phenomena called cyber threats. It then proceeds with the definitions of four types cyberattacks under 4-prong classification criteria: international cybercrime, cyber espionage, cyber *use of force* and cyber armed attack by providing examples of such incidents (where available). The Chapter concludes with a discussion on attribution, a topic that has undergone considerate developments in the seven years of this study. The next Chapter investigates the overarching topic of this thesis.

Chapter III: The EU *vs* its MS or the EU *and* its MS: the challenging road to developing cybersecurity legislation will in part answer the main research question and sub-question a). It looks into the long road the EU has walked towards regulating cybersecurity. Security has traditionally been a matter of internal affairs the EU does not have competence to regulate. *Cybersecurity* however, is different as the borderless nature of cyberspace challenges the traditional perception of *national* security: an attack against one member state could quickly spread to the other MS creating a destructive spill-over effect. As a consequence, when a threat becomes cross-border, the matter moves up on the EU regulatory agenda.

By briefly analysing existing scholarship on securitisation theory, the latter will be applied to the cyber field, further expanding existing but scarce literature on *collective cybersecurity* with particular focus on the legal framework. Then, the role of the single MS will be analysed – those MS which were the most vocal during negotiations on the NIS Directive 2016.

Whilst an EU-level regulatory approach to tackling cyber threats was seen as the way forward by the EU, its own MS challenged this view. The Chapter will therefore analyse the internal tensions between the EU and its MS and between the MS themselves - and the long process towards the securitisation of the field at EU-level. Two of the MS analysed in this thesis stand out in this discussion – the UK and Bulgaria, as two states with very opposing views on who should be in the leader's position – the EU or the MS. The Chapter debates the relevant arguments on both sides providing (when available) scholarly work supporting both positions. Finally, it also discusses the EU's cyber diplomacy posture, the "external" dimension of its cybersecurity framework, and how it shapes the overall cybersecurity regulatory agenda.

Once the broader scene has been set, the thesis delves into the case studies, thereby answering sub-question b). All three Case Study chapters follow the same structure: the Chapters first address the legal frameworks prior to the adoption of the NIS-Directive: those laws and provisions that have tackled cybersecurity-related issues to some extent, such as those on computer misuse, on the telecommunications sector and electronic communications more specifically, and on the powers attributed to the MS' respective intelligence agencies in countering cyberattacks and, in the case of the UK, performing them. The three respective strategic approaches and their development is reviewed next, and a comparison is drawn between the interpretation of the different types of cyber threats. Then an analysis of the novelties introduced by the NIS Directive's transposition laws follows – from the new cybersecurity requirements for the CI sectors' operators, the newly established bodies, to the newly attributed responsibilities to already existing bodies – and how the new law fit with the already existing frameworks. Each Chapter thus evaluates the newly assigned capabilities for cross-border cooperation and information sharing among the MS, as well as reporting of and responding to incidents. Each case study will also address at least one recent cybersecurity breach and what it tells about the effectiveness and implementation of the NIS transposition laws. Ultimately, the aim of the case studies is to compare the MS's regulatory efforts in the field of cybersecurity thereby drawing a conclusion on what their overall preparedness pre- and post-NIS Directive tells about the EU regulatory efforts more generally.

Chapter IV: Member States cybersecurity legal frameworks: the UK analyses the UK legal regime pre- and post-Brexit as well as pre- and post-NIS Directive. The UK, a "global leader" in cybersecurity,[44] was one of the MS with better cybersecurity preparedness prior to the adoption of the EU cybersecurity law. This is one of the reasons why it kept challenging the EU-level regulatory efforts. However, despite having laws regulating equipment interference and interception of electronic communications (e.g. Investigatory Powers Act (IPA) 2016), and despite having the capabilities to perform these on devices located abroad, its framework lacked a law for CI protection from cyberattacks. The NIS Directive, transposed via the NIS Regulations 2018, therefore was of evident importance. This case study also stands out as the only state possessing both cyber defence and cyber offense capabilities, and for having respective national agencies for performing such operations – the NCSC and the National Cyber Force, both having the GCHQ as parent orgaisation. This too speaks for the solid level of understanding the UK had on cyber issues and supports the fears the UK had during the EU laws' negotiation process: a legally-binding EU-led approach to cybersecurity would entail being forced to engage and exchange information with states which were much less prepared.

Overall, the aim of this Chapter is to showcase a member state with a high level of preparedness and how the implementation process of the EU laws happened at national level and how these impacted the national capabilities and legal framework.

What makes this case study particularly interesting is also the fact that the UK left the EU in the middle of the research process of this thesis, making it a former member state. As such, however, the UK still bears the legislative signs of a MS: the NIS transposition law continues to be the only law on CI protection in the UK. The Chapter will thus also analyse the effect Brexit had on the development of the UK regulatory regime and the novelties it introduced in terms of new bodies and institutional responsibilities. It offers a brief analysis of the EU-UK relationship in the field of cybersecurity post-Brexit and also debates the impact Brexit has had on the development of the overall EU regulatory regime.

[44] Ellie Templeton and Dr Robert S. Dewar, 'The post-Brexit EU-UK relationship; an opportunity or challenge for cyber security?' (*Geneva Centre for Security Policy*, 17 September 2021) <https://www.gcsp.ch/global-insights/post-brexit-eu-uk-relationship-opportunity-or-challenge-cyber-security> accessed 20 December 2023.

Chapter V: **Member States cybersecurity legal frameworks: Italy** is the second case study, offering a medium level of preparedness. Italy had two PM decrees (which became known as Monti decree and Gentiloni decree)[45] adopted prior to transposing the NIS Directive, in 2013 and 2017 respectively. But these were administrative acts, so secondary level-type of legislation. The Italian NIS transposition law - Legislative decree 65/2018 - in fact did not seem to take them into consideration. This case study therefore presents an example of a MS with a complex regulatory framework, where institutional architecture was extremely burdensome and incident notification and handling required a multi-step approach. On this, Italy was very different from the UK which had defined these issues without further complications. The Italian case study thus demonstrates the difficulties in adopting new EU pieces of legislation when there is little preparation at national level.

The Chapter follows also post-NIS Directive developments, namely the Cybersecurity Perimeter – a law, accompanied by a set of PM decrees – which got Italy on the fast track of cybersecurity legal developments without waiting for the EU. The Chapter therefore debates the possibility of Italy taking the vacant chair left by the UK in playing a key role in shaping the EU cybersecurity agenda, but concludes that the maturity level of its legal framework is still not up to speed to succeed in this.

Chapter VI: **Member States cybersecurity legal frameworks: Bulgaria** is the final case study, offering a low level of cybersecurity preparedness. Prior to the adoption of the NIS Directive transposition law – the BCSA 2018, Bulgaria did not have any sector-specific legislation, but merely some provisions in somewhat topic-related laws. Lack of technical, operational – as well as legal – knowhow transpire from the analysis conducted in this Chapter. This provides evidence as to why the UK was reluctant to engage with cross-border cooperation and endorse an EU-led approach: it would entail cooperating with states like Bulgaria which were not prepared to affront the challenging cyber threats landscape. It also showcases why Bulgaria pushed for an EU-led regime: being a state which lacked well developed regulatory framework, Bulgaria needed someone more powerful to pull the wagons. The need for a

[45] The two PM decrees were named after the PMs that put forward their adoption. In 2013 this was Monti and in 2017 – Gentiloni.

supranational-level support was essential so Bulgaria could meet the security challenges of the 21st century. The BSCA was therefore a welcomed step towards setting the cybersecurity regulatory agenda in Bulgaria.

Chapter VII: Conclusion assesses the findings drawn from the case studies and answers sub-question set out in letter c). This final Chapter summarises and showcases the contribution to knowledge of this work. The comparative study evidences the profound differences and mismatches between the MS, their legal preparedness and, more importantly, their different views in defining and interpreting key cyber threats. EU-level action was clearly needed to address these discrepancies and support the MS in mitigating state-sponsored cyberattacks. The role the NIS Directive played was therefore very important. In the years to follow, in the post-Brexit EU, there has been more agreement and more willingness to work towards an EU-level approach by the MS and the EU leadership on the matter has been largely accepted. This is due not only to the UK leaving the EU, but also to the better understanding of the issue of cybersecurity and its cross-border nature. The Chapter argues that the EU has achieved its goal to become a leading regulator in the NIS field despite being continuously challenged by its own MS. However, for its *cybersecurity* framework to be fully impactful, its cyber diplomacy policy also needs to be developed: when it comes to state-sponsored cyberattacks knowing how to protect the systems and networks of the CI sectors is key, but calling out malicious foreign activity in cyberspace is also essential – and currently the EU is lagging behind on this.

Thus, so far, considering the entirety of its framework on foreign sponsored cyberattacks, the EU has not managed to "export" its regime: other states, among which also the UK, remain ahead at least on the attribution side and have been much more vocal on calling out states and their malicious activity. The Chapter concludes with a recommendation for the EU to become more coherent and assertive in further developing its regulatory agenda, which will be key to ensuring that its voice is heard globally, if it wants to become a *cybersecurity* regulator.

Chapter II: From cyber warfare to cybersecurity: defining the thresholds of cyberattacks

2.1. Introduction

Over the course of the last 50 years, computer security has been consistently gaining more and more importance at international level. Computer viruses have existed since at least the 1970s and have preceded the internet.[46] What has also preceded the world wide web, which is the internet the way we know it today, is the term "cyberspace", which was first used in 1982 by science-fiction author William Gibson in his short story Burning Chrome.[47] Cyberspace has since been defined as "the entirety of the data stored in, and the communication that takes place within, a computer network, conceived of as having the properties of a physical realm; the environment of virtual reality".[48]

A great facilitator of everyday life, governments would soon come to realise that cyberspace offered many possibilities: it has become the foundation of modern life. But it also posed threats. However, the initial focus that was given to cyberspace in the 1990s shifted as policymakers' attention was absorbed by international terrorism in the aftermath of 9/11 and cyber threats were accorded peripheral importance until the first major cyberattack on a nation-state – in Estonia in 2007 – brought the topic back onto the global stage.[49] On the EU stage, however, cyber threats, whilst not considered a top of the agenda priority at the time, continued to be on the discussion table even before the Estonia attacks, as seen in Section 1.1.3. That said, in2001 the US declared that cyberspace had become the fifth domain of war together with air, land, sea and space already,[50] whilst the EU followed suit only in – unofficially[51] – 2015 and officially in 2018.[52] The Estonia attack hence uncovered a largely unmapped area in the field of international and – despite the (mostly non-binding) EU measures - in the field of EU law, and policymakers and

[46] Osawa 114.
[47] Jeff Prucher, *Brave New Words: The Oxford Dictionary of Science Fiction* (OUP 2007) 31;
Thomas Jones, 'William Gibson: beyond cyberspace' (*The Guardian*, 22 September 2011) <www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace> accessed 15 January 2024.
[48] Prucher 31.
[49] Schmitt 269.
[50] Department of Defense 5.
[51] European Defence Agency 1.
[52] Council of the EU 2.

security experts were caught off-guard. Estonia's incident was hence of great relevance for the development of contemporary international and EU law as it triggered an alarm and subsequently evidenced legal lacunas, the lack of knowledge about the cyber domain, and the possibility of malicious foreign-sponsored cyber operations.

This first Chapter will be scene-setting, providing the theoretical background to the thesis. This background is needed to better understand the EU's legal developments in the field of cybersecurity. With its very ambitious cybersecurity regulatory agenda developed in the last ten years, the EU faced a world in which various state and non-state actors had already tried to come to grips with what threats existed in the cyberspace, how they were to be legally defined and how they could be legally responded to. Chapter III will consider the EU's approach to regulating cybersecurity, for which Chapter II is important context.

Chapter II will analyse the bases of what we perceive today as cybersecurity and state-sponsored cyberattacks. The aim of Section 2.2. is to analyse the curve the debate has followed: from the possibility of waging war in cyberspace (called "Phase One" in this Chapter), to the low-level, but consistent state-sponsored cyber operations aiming at disruption, rather than destruction ("Phase Two", the status quo). The analysis will hence begin with the discussion on the applicability of international law, specifically *jus ad bellum* and *jus in bello,* to cyber operations, and will discuss key issues such self-defence in cyberspace, which dominated the scholarly debate in the aftermath of the attacks against Estonia (Sections 2.2.2.1. through 2.2.2.1.iii)) These sections will focus on issues such as violation of sovereignty, the principle of non-intervention, and the possible resources for response by a victim state such as countermeasures. The Chapter will then move to analysing the applicability of international law to those attacks falling below the threshold of *use of force* (Section 2.2.2.2.) that have dominated experts' discussions in the last years. Despite what used to be a largely unmapped field in international law merely ten years ago, and being much less one now, grey zones persist and are a "fertile ground for an escalatory spiral".[53] Chapter III will then analyse how the development of international law has impacted the EU's own views on regulating cybersecurity.

[53] Micheal N. Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42 The Yale Journal of International Law Online 1, 21.

Section 2.3. will discuss next the spectrum of cyberattacks, classifying them into four types: international cybercrime, cyberespionage, cyber *use of force* and cyber armed attack, and will focus on defining the threshold between non-harmful and harmful state-sponsored cyberattacks. The Chapter will end with a discussion on attribution and responsible state behaviour in cyberspace (Section 2.4.), completing the mapping of the international efforts for cyber operations' regulation. The aim is to provide the theoretical background against which the EU attribution capabilities will be compared to in Chapter III.

Ultimately, the aim of this Chapter is to set out how the international community has dealt with cyber-related definitions and applicable laws, which will make possible to explore the EU's approach – in what ways it has followed the trends outlined in this Chapter and in what ways it has carved its own path.

2.2. Cyberspace's regulation: an overview

The first self-replicating computer worm, called "the Creeper", was written in 1971 and was not malicious.[54] This type of computer virus however, while becoming known worldwide, would not in itself qualify as an international cyberattack (in the sense this thesis is adopting, as will be seen in Section 2.3.1.: it was not state-sponsored and was not politically motivated. Since then, cyberattacks have become more serious, more numerous, and, most importantly, used by governments as a policy instrument and to demonstrate superiority in the field of cybersecurity. This generated contentious discussions at international level on issues such as sovereignty over cyberspace, the potential applicability of international law (and more specifically, international humanitarian law), and who can regulate cyber operations. The following sections will analyse these discussions in detail, providing an overview of their development over the years, providing the necessary background for understanding the EU's won legal approach to cybersecurity (discussed in Chapter III).

[54] Osawa 115.

2.2.1. Sovereignty over cyberspace

Before the dawn of widespread state-sponsored cyberattacks, security experts posed the question of how cyberspace could be governed. Back in the 1990s some scholars, called "exceptionalists", argued that a nation-state cannot govern over the cyber domain. In his "Declaration of the Independence of Cyberspace" written in 1996, "cyberlibertarian" John Perry Barlow declared that governments have no sovereignty over it.[55] According to the cyberlibertarian rhetoric it was the power of technology and the power of individuals that were at cyberspace's core: the new virtual world enabled "the creation of new forms of community and identity that do not rest on an appropriation of traditional space".[56] The opposing theory was sustained by the "sovereigntists", who admitted that cyberspace was, in fact, virtual, but enablers of its existence such as routers, cables, transmitters and other digital equipment, were not. And most importantly – much[57] of this equipment was physically located within the territory of nation-states.[58] The authors of the Max Planck Encyclopaedia of Public International Law took the same view, stating that "[s]tate activity in cyberspace is thus limited by the traditional rules on sovereignty and territorial integrity".[59] This second theory has since prevailed over the exceptionalists' one: despite different approaches and perceptions of the advantages and disadvantages of the use of politically-motivated cyberattacks among the international community, the later seem to have silently agreed upon the sovereigntists theory.

[55] John P. Barlow, 'A Declaration of the Independence of Cyberspace' <http://editions-hache.com/essais/pdf/barlow1.pdf> accessed 15 January 2024.
[56] Mihaela Kelemen and Warren Smith, 'Community and its 'virtual' promises: a critique of cyberlibertarian rhetoric' (2001) 4 Information, Communication & Society 370, 371.
[57] Underwater fibre optic cables are not, in fact, located within the territory of a state.
[58] Sean Watts, 'Cyber Law Development and the United States Law of War Manual' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE 2016) 49.
[59] Rudiger Wolfrum (ed) *The Max Planck encyclopedia of public international law*, vol II (OUP 2013) 989.

2.2.2. Applicability of international law to cyber operations

International law has seen great development over the last two centuries. The laws of war, in particular, were the first part to be codified.[60] After two devastating wars, world leaders finally agreed on limiting the right to declare war on another nation-state. The prohibition of the *use of force* has been considered among the major achievements of international law in the previous century:[61] "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".[62] Clearly, the way the term *use of force* was implemented and understood has changed through the many centuries of human history.[63] All the same, there have been numerous violations (which will not be discussed here for reasons of space) of this rule in the years since 1945: "international law is weak in the face of state power".[64] This analysis will only focus on its most recent developments with regards to the rise of state-sponsored cyberattacks.

In the immediate aftermath of the Estonia attacks scholars and decision-makers focused their attention predominantly on the possibility of cyber war. The debate, therefore, focused on whether and how one of the bedrock principles of international law – territorial sovereignty – could be violated in cyberspace, whether there was indeed the possibility of cyber *use of force*, and if yes - what types of cyberattacks would constitute it; and whether there could be cyberattacks that would cause violence, major destruction and harm that would be equal to an *armed attack* in the physical world.

[60] Michael A. Meyer (ed) *Armed conflict and the new law : aspects of 1977 Geneva protocols and the 1981 weapons convention* (London : British Institute of International and Comparative Law 1989) 8.
[61] Rudiger Wolfrum (ed) *The Max Planck encyclopedia of public international law*, vol X (OUP 2013) 618.
[62] UN Charter 1945 Article 2(4).
[63] For more detailed information on the development of *use of force* before the codification of the laws of war, view Ian Brownlie, *International law and the use of force by States* (Oxford, Clarendon Press 1963).
[64] David Armstrong, Theo Farrell and Hélène Lambert, *International law and international relations* (2nd edn, CUP 2012) 125.

2.2.2.1. Phase One: *Jus ad bellum* and *jus in bello* in cyberspace

In his analysis of the post-Estonia order in cyberspace, McGraw declared that due to the "systematic vulnerability of modern systems", cyber war, despite being "over-hyped", was inevitable.[65] Scholars, in fact, expected the new technologies to completely change the face of conflict.[66] Doom-laden warnings of an inevitable "cyber 9/11" or "cyber Pearl Harbor" proliferated.[67]

Despite some scholars arguing against these theories, with Rid outright stating that cyber war was not going to happen[68] and Arimatsu claiming, in 2012, that none of the cyberattacks to date amounted to cyber warfare,[69] "cyber war" quickly became the centre of debates and, as a consequence, also what laws would apply to it.[70] Experts realised that the legal ground upon which computer-generated warfare could be based was uncertain: customary international law (e.g. the principles of sovereignty), the laws of war, the UN Charter or the other international treaties (e.g. WTO agreements or laws of the sea) did not explicitly address the issue.

Despite the US declaring that cyberspace has become the fifth domain of war some scholars were reluctant to agree.[71] Delerue argued that in terms of technical accuracy, cyberspace was not an "environment" like land, sea, air and land and humans cannot be "deployed" to cyberspace.[72]

---

[65] Gary McGraw, 'Cyber War is Inevitable (Unless We Build Security In)' (2013) 36 Journal of Strategic Studies 109, 109.

[66] Lennart Maschmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations' (2021) 46 International Security 51, 51.

[67] , 'U.S. homeland chief: cyber 9/11 could happen "imminently"';
Sanger and Perlroth.

[68] Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 JStrategic Stud 5.

[69] Louise Arimatsu and Mary Ellen O'Connell, 'Cyber Security and International Law' (*Chatham House*, 2012) <www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf> accessed 26 November 2016.

[70] Micheal N. Schmitt (ed) *Tallinn Manual on the International Law applicable to Cyber Warfare* (CUP 2013) 3.
But this is hardly the first occasion where the development of new powerful weaponry has initiated such disputes. As a comparison, nuclear arms development also caused vigorous discussions. Having these new weapons demonstrated wealth, advanced scientific capability, technological superiority and above all – great power. The Treaty of the Non-Proliferation of Nuclear Weapons (NPT) entered into force 25 years after the use of the bomb in 1945. The full text of the NPT can be found here: <www.un.org/disarmament/wmd/nuclear/npt/text> (accessed 7 December 2023).

[71] Thomas Rid, *Cyber War Will Not Take Place* (OUP 2013) 165.
François Delerue, *Does International Law Matter in Cyberspace?* (CUP 2020) 11;

[72] Delerue 11.

Because of this, it could not be argued that cyberspace was a new legal domain.[73] It was not, he continued, a new domain for the purpose of international law, as cyber activities take place in the four areas of land, sea, air and outer space, and hence the applicability of international law to cyberspace ought not to be questioned at all.[74] Other scholars questioned adopting such a hard-edged approach to the topic, and it has not been reflected in state practice.

At the decision-making table things did not look much different: disagreements and no clarity prevailed. In 2009, then-Secretary-General Ban Ki-Moon urged the Advisory Board on Disarmament Matters of the UN to reflect on cyber warfare's influence on international security.[75] But a breakthrough came only in 2013 with the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security's (hereinafter UN GGE) report with "recommendations to promote peace and stability in state use of ICT".[76] The UN GGE report included a breakthrough statement - that existing international law and the UN Charter did indeed apply to cyberspace - but it left the question of how exactly they would apply to a "further study".[77] The report, however, confirmed that the principle of sovereignty applied to "State conduct of ICT-related activities".[78] Acknowledging the relevance of this bedrock principle of international law, which has the territorial integrity of states at its core, to the borderless cyberspace, was a major success and significant step forward in providing some clarity.

At the scholarly level, an important step forward towards shedding some light on the issue of the applicability of international law to cyber operations was the first *Tallinn Manual on the International Law Applicable to Cyber Warfare* (commonly known as the *Tallinn Manual*) of 2013. It addressed only the legal aspects of cyber warfare, and hence had a limited scope: "cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace" were not included in the analysis as, according to the authors, *jus ad bellum* and *jus in bello*

[73] François Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?' (2019) 52 Israel law review 295, 302.
[74] Delerue 12.
[75] United Nations, *Pay More Attention To Cyberwarfare, Verification, Secretary-General Advises In Remarks To Advisory Board On Disarmament Affairs* (18 February 2009).
[76] United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security* (2013) 2.
[77] Ibid 2 and para 19.
[78] Ibid para 20.

would not be applicable to them.[79] The authors provided an answer to the long-standing question of whether new laws needed to be created specifically for this emerging phenomenon: they unanimously agreed that the existing international law norms and in particular *jus ad bellum* and *jus in bello* did apply to cyberspace, rejecting "any assertions that international law is silent on cyberspace in the sense that it is a new domain subject to international legal regulation only on the basis of new treaty law".[80] In other words, they agreed with the position, advanced by the UN GGE in 2013. Moreover, the contributors not only unanimously agreed that certain cyberattacks could cross the threshold for *use of force* and *armed attack* as defined by article 2(4) and article 51 of the UN Charter respectively, but they argued that this had indeed happened with the Stuxnet worm (discussed below), which, according to them, amounted to *use of force*.[81]

Despite the UN GGE report, and the contribution made by the Tallinn Manual, in late 2014 the then-US President Obama labelled the cyber domain as a "wild west"[82] – implying, possibly, that it was a lawless space. Scholars were fast to disagree, arguing that there was no such thing as "normative void" with regards to performing an attack in the digital world.[83] This idea was further advanced the following year, when the 2015 UN GGE's report stressed the significance of cooperation "to prevent harmful ICT practises".[84] It also confirmed that the norms of non-intervention applied to cyberspace.[85] The applicability of international law and the UN Charter to cyber operations were also re-confirmed.[86] Despite the lack of clarity as to how exactly international law applied to cyberspace, the report seemed a promising sign that states were getting further in their negotiations. In 2017 however, the UN GGE failed to reach an agreement on the final report because of diverging views on precisely how the laws of armed conflict, countermeasures and self-defence would apply to cyber operations.[87] Cuba and Russia publicly expressed their discontent with the final report, thereby blocking it.[88] This friction in the

[79] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 4.
[80] Ibid 13.
[81] Ibid 45.
[82] The White House Office of the Press Secretary, 'Remarks by the President in Year-End Press Conference' (19 December 2014) <www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference> accessed 15 January 2024.
[83] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 5.
[84] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015).
[85] Ibid para 28 (b).
[86] Ibid para 24 *et seq*.
[87] Delerue 5.
[88] Delerue 306.

negotiation process demonstrated that despite years of debates, states still did not see the applicability of international law to cyberspace in the same way[89] and had different interpretations of specific norms of international law.[90] Although minor disagreements could be overcome, having profoundly divergent interpretations of international law norms and specifically as regards countermeasures and self-defence, was a rather more challenging obstacle. Any type of reaction by a state claiming to have been a victim of another state's cyberattacks needs to be in line with existing international law for it to be lawful and to avoid unnecessary escalation. However, *not* agreeing on what exactly would be lawful response under international law was a huge gap, as what was seen as "lawful" by some states, apparently was seen as unlawful by others. If this is indeed the case, and if representatives of these two groups appeared to be at the opposite endings of a cyberattack, *any* response would essentially lead to escalation.

As a consequence of these diverging views, some states – including some EU Member States (MS) - advanced their own official positions on the applicability of international law. The US was first to adopt such a position in 2012 (with three more so far, adopted in 2016, 2020 and 2021); the UK followed suit in 2018 (and more recently in 2021 and 2022); Estonia did in 2019 and 2021; France and the Netherlands did in 2019; the Czech Republic, Finland, Iran, Israel and Australia did in 2020; Italy, Germany, Russia, Romania, Japan, Norway did in 2021; and finally, Sweden and Poland did in 2022.[91] In light of the focus of this thesis, only the positions of Italy, the UK will be considered in substantive detail in this Chapter.

A) Defining the consequences of cyber operations

i) Violation of sovereignty

Back in 1999, the US Department of Defense published an Assessment which addressed the issue of violation of sovereignty stating that "[a]n unauthorized electronic intrusion into another

[89] Ibid 310.
[90] Delerue 2.
[91] NATO CCD COE, 'National Positions' <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions> accessed 15 January 2024.

nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, **but such issues have yet to be addressed by the international community**" [emphasis added].[92] The US was hence advancing ideas for the interpretation of international law norms much earlier than any of the EU MS or the international community in general.

Scholarly work on how exactly a state's territorial sovereignty can be violated in cyberspace has seen much disagreement. Labelled a "chief" question,[93] and "the most fundamental" of all international law principles,[94] the debate reflects the state-level disagreement, with states having different views on the meaning and legal nature of the principle in general and how exactly it can be violated.[95] The key to determining the applicability of this "universal" principle lies in state practice or specific treaty rules.[96] That certain cyber operations *can* and *do* violate it has been unanimously agreed by the authors of the Tallinn Manual.[97] But which exactly operations would do it has been a challenging issue to agree upon.[98] The analysis conducted by the Tallinn Manuals' authors considered two things: whether there has been interference with governmental functions and the extent to which the victim state's territorial integrity has been infringed.[99] According to some, a violation would occur only if it causes "damage", whereas according to others, the mere "placement of malware that causes no physical damage (…) constitutes a violation of sovereignty".[100] Hence, physical damage, injury or loss of functionality of, for instance, targeted critical infrastructure, was declared a straightforward violation of sovereignty.[101] The topic which proved difficult was what "other consequences" would constitute violation.[102] Tallinn Manual 2.0 provided some needed clarification noting that "[c]yber

[92] Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (November 1999) 18.
[93] Gary P. Corn and Robert Taylor, 'Concluding Observations on Sovereignty in Cyberspace. Sovereignty in the age of cyber' (2017) 111 AJIL Unbound 282, 282.
[94] Schmitt, 'Grey Zones in the International Law of Cyberspace' 4.
[95] Dmitry V. Krasikov and Nadezhda N. Lipkina, *Sovereignty in Cyberspace: A Scholarly and Practical Discussion* (Advances in Social Science, Education and Humanities Research 2020) 160.
[96] Corn and Taylor 285.
[97] Micheal N. Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas Law Review 1639 1642)
[98] Ibid 1647.
[99] Micheal N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2 edn, CUP 2017) Rule 4 (10).
[100] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 16.
[101] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 4 paras 11-13.
[102] Ibid Rule 4 (14).

operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law".[103] More recently, many scholars have weighed in on these issues and have advanced the view that attacks against the healthcare sector (in view of the COVID pandemic) could in some cases be considered as violations of sovereignty as undermining the provision of healthcare could interfere with the right of a sate to exercise its functions within its own territory.[104]

In the meantime, several states have addressed the violation of sovereignty in their positions on the applicability of international law to cyberspace. In 2021 Italy published its position paper, but its references to sovereignty were rather generic: "[t]he principle of sovereignty is a primary rule of international law, the violation of which amounts to an internationally wrongful act".[105] The UK adopted a different approach whereby sovereignty was considered only as a principle from which other principles and rules are derived and not a binding rule in international law itself.[106] In his speech "Cyber and International Law in the 21st Century", the then-Attorney General Jeremy Wright argued that it was not possible to "extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position, therefore, is that there is no such rule as a matter of current international law".[107] As experts have argued, this implies the cyber operations that fall below the threshold of non-intervention can only be considerate unfriendly, but not a violation of international law norms.[108]

Just considering the contrasting positions of these two states (which shared EU membership until the UK's Withdrawal in January 2020) demonstrates how difficult it is for states to reach a common conclusion on the applicability of international norms to cyber operations. When the

[103] Ibid Rule 4 (1).
[104] François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' (13th International Conference on Cyber Conflict (CyCon)) 20;
Marko Milanovic and Micheal N. Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic' (2020) 11 Journal of National Security Law & Policy 253.
[105] Ministero degli Affari Esteri e della Cooperazione Internazionale, *Italian Position Paper on 'International Law and Cyberspace'* (November 2021) 4.
[106] Foreign Commonwealth & Development Office, *Policy paper on Application of international law to states' conduct in cyberspace: UK statement* (3 June 2021).

[107] Report of the Study Group co-organised by the University of Bologna University of Milan and University of Westminster, *International Law and Cyberspace* (February 2021) 2.
[108] Ibid 2.

very interpretation of some of the bedrock principles of international law differs, even among like-minded states, it is difficult to imagine that at international level states would ever agree. So the "chief" question will most likely not see a solution in the near future since, as very often happens in cyberspace, states use the floating threshold to their advantage. Section 2.3., which reflects on the different types of attacks, will aim at putting forward a perspective on the principle and how it can be violated in cyberspace using real-life state-sponsored cyber operations. Here, it also needs to be observed, that in terms of violation of sovereignty in cyberspace, the EU has not yet taken an official position (as will be seen in Section 3.4.).

ii) The principle of non-intervention

The principle of non-intervention has not been given enough importance by scholars and decision makers not only when it comes to its applicability to cyber operations in general,[109] but also when it comes to its violation by malicious state-sponsored attacks.[110] As a "derivative of the concept of sovereignty",[111] the meaning of the principle remains "unclear", but in general terms, interference by a state in another state's internal or foreign affairs is a violation of the principle[112] – if there is an element of "coercion".[113] Schmitt agreed that for a violation of the principle to occur, as well as to be qualified as internationally wrongful act, the element of coercion was indeed crucial.[114] Lotrionte added further granularity, arguing that in order to evaluate whether a non-forcible but yet wrongful act has taken place in cyberspace, there are a few elements that need to be taken into consideration: coercion, its level of intensity, its scale and effects, its objective and its legality.[115] She also stated that while not all "forms of cyber operations that involve political, economic, or ideological interference violate the non-intervention principle", an operation that will certainly count as coercive cyber economic

[109] Catherine Lotrionte, 'Countering state-sponsored cyber economic espionage under international law' (2015) 40 North Carolina Journal of International Law and Commercial Regulation 443, 492.
[110] Ibid 447.
[111] Schmitt, 'Grey Zones in the International Law of Cyberspace' 7.
[112] Rudiger Wolfrum (ed) *The Max Planck encyclopedia of public international law*, vol VI (OUP 2013) 289.
[113] Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I' (*EJIL:Talk!*, 1 November 2013) <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/> accessed 6 December 2016.
[114] Schmitt, 'Grey Zones in the International Law of Cyberspace' 8.
[115] Lotrionte 497.

espionage.[116] Where the threshold for intervention lies however, she concludes, is "uncertain" and only the emergence of dominant state practice will determine it over time.[117] Because indeed, it is difficult address the limits of non-intervention in a non-tangible reality.

For example, Italy put forward a position that largely aligned with the scholarly views above: a cyber operation would violate the principle of non-intervention "when it attempts to coerce" or lead a state "to do something it would not have done.[118] Without the element of coercion an operation would not violate the principle – though that would not make its "wrongfulness" less relevant.[119] The Italian position also gave examples that could potentially violate the principle – ransomware, "where a user's critical data is encrypted to prevent the user from accessing files, databases, or applications unless a ransom is provided" or altering electoral results.[120] While it is clear why the latter made the list, it is not clear with the former: ransomware is one of the most common cyberattacks and, as it name implies, means paying a ransom in order to – in this case – restore data. The fact that it is state sponsored does not make its impact any different. Most cyber operations, such as distributed denial of service (DDOS), malware, spyware, etc. (referenced also in Section 2.3.) suggest damage being inflicted upon certain types of data, meaning that the original data, or access to it, needs to be restored if the victim is to recover from the incident. The difference with ransomware is that the ransom must be paid to the attacker to enable this to happen. Indeed, it is not uncommon that a government orchestrates a ransomware attack, as seen with the North Korean WannaCry attack (Section 2.3.1.1.) If there is a sub-contractor involved, the issue becomes rather more complicated – whether the international law principle of non-intervention, applicable to state-on-state operations, can be violated by a third party (a non-state actor for instance) will be addressed below.

[116] Ibid 503.
[117] Ibid 539.
[118] Report of the Study Group co-organised by the University of Bologna University of Milan and University of Westminster 120.
[119] Ibid 120.
[120] Ibid 121.

- Violation of sovereignty and the principle of non-intervention: examples in cyberspace

In the recent past there have been examples of attacks that have arguably constituted violation of the non-intervention principle, and one in particular stands out – the allegedly Russian hack of the US Democratic National Committee (DNC) in the summer of 2016.

The DNC hack is a good example of the grey zones regarding coercion and the principle itself as experts have not managed to agree on whether the operation was coercive.[121] The hack saw thousands of the Democratic party member's emails being leaked to the public, revealing embarrassing backroom correspondence and subsequently, presumably undermining the trust supporters have in the party and thus influencing the outcome of the elections.[122] Because the emails were in fact not interfered with, some argued it was a case of a cyber espionage (addressed below), seemingly not unlawful under international law.[123] The DNC, however, argued that it influenced the outcome of the elections,[124] and choosing a "political system" "freely" lies in the basis of every state's sovereignty, as stated in the *Nicaragua case*.[125]

Considering this unprecedented case, international lawyers and analysts found it difficult to decide whether the operation violated any laws and if it did – which ones. As Crootof maintains, the US government never explicitly declared that the intrusion was a violation of international law.[126] She argued that had the attack hit the voting system and therefore directly influenced the political situation in the country, it would have violated the non-intervention principle.[127] But it did not. According to other scholars, legal norms were indeed violated. Watts sustained that it

[121] Schmitt, 'Grey Zones in the International Law of Cyberspace' 8.
[122] Spencer Ackerman and Sam Thielman, 'US officially accuses Russia of hacking DNC and interfering with election' (*The Guardian*, 8 October 2016) <https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election> accessed 21 January 2024.
[123] Schmitt, 'Grey Zones in the International Law of Cyberspace' 8.
[124] NCCIC and FBI, *Grizzly Steppe - Russian Malicious Cyber Activity* (29 December 2016).
[125] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (1986)* International Court of Justice para 205.
A quick overview of the case: in 1984 Nicaragua filed an Application against the US regarding a dispute relating to responsibility for military and paramilitary activities in and against Nicaragua. The Court issued provisional measures in May 1984, requiring the US to immediately cease and refrain from any action restricting access to Nicaraguan ports, and the laying of mines. The Court also stated that the right to sovereignty and to political independence possessed by Nicaragua should be fully respected and should not be jeopardized by activities contrary to the principle prohibiting the *threat* or *use of force* and to the principle of non-intervention in matters within the domestic jurisdiction of a State.
[126] Rebecca Crootof, 'International cybertorts: Expanding state accountability in cyberspace' (2018) 103 Cornell law review 565, 570.
[127] Ibid 615.

was indeed difficult to determine whether the hack was a violation of the non-intervention principle, but even if it was not, it was still a violation of the US sovereignty, "assuming [it] involved nonconsensual intrusion into cyber systems located in the U.S.".[128] Whether there has been a violation of sovereignty is hence still an open discussion and the case demonstrated how difficult it is to agree weather a cyber operation has violated international law norms.

The next subsections will discuss the potential ways for a victim state to respond to malicious cyber operations: international law does not leave such states powerless and provides "multiple options" short of war, conducted in cyberspace or in the physical world.[129] These include the right to self-defence, countermeasures, retortions and measures invoked under a plea of necessity.

B) Defining the lawful responses

i) Self- defence

Even though offensive and highly disruptive attacks have been increasing, what would constitute a lawful response to a cyberattack is yet another question in the field. In 1999, the US Department of Defense (DOD) highlighted that it was "far from clear" how the international community would interpret the applicability of the doctrines of self-defence and countermeasures to "computer network attacks".[130] Establishing a framework on how to conduct hostilities in cyberspace is extremely difficult and defining the limits of what constitutes a lawful response is so complex, that some scholars fear that any effort to do so could lead to conflict escalation.[131] Undoubtedly, the response would depend on the nature of the offensive intrusion. However, it is – still - extremely challenging to define the offensive cyberattack in the first place. Schmitt has argued that the key to understanding the right of self-defense in cyberspace is rooted

[128] Sean Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*Just Security*, 14 October 2016) <www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/> accessed 6 December 2016.
[129] Catherine Lotrionte, 'Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law' (2018) 3 The Cyber Defense Review 73 91.
[130] Department of Defense Office of General Counsel 23.
[131] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 20 para 16.

in understanding the meaning of the term *armed attack*, which, however, remains undefined under international law.[132] Lotrionte also observed that to determine the "appropriate legal self-defence response" identifying the perpetrator was crucial, as was determining whether the attack had reached the threshold for an armed attack.[133] The issue is aggravated also by the fact that for instance the U.S. (one of the most targeted countries[134]) considers *use of force* and *armed attack* as largely the same thing, an operation to which the same threshold applies – a view not shared by the majority of the international community.[135] The Tallinn Manual 2.0 maintains that "when measures falling short of a use of force cannot alone reasonably be expected to defeat an armed attack", both cyber and kinetic operations that cross the threshold to *use of force* should be allowed.[136] At the same time, states targeted by a *use of force* operation that does not amount to an armed attack, can respond lawfully for example by countermeasures or actions consistent with the plea of necessity.[137]

ii) Countermeasures

It seems that contemporary scholarship has preferred to focus on self-defence as a response to a hostile cyber operations and the concept of countermeasures has not been discussed enough.[138] Labelled "one of the most important self-help remedies of State responsibility",[139] countermeasures are actions that would otherwise be unlawful, but that are lawful when taken in response to – and are proportionate to[140] - an internationally wrongful act;[141] in other words, countermeasures are actions taken in response to other actions that have broken international

[132] Schmitt, 'Grey Zones in the International Law of Cyberspace', 15.
[133] Lotrionte 90.
[134] The US is the fifth most attacked country according to Kaspersky, 'Cyber threat real-time map' <https://cybermap.kaspersky.com/> accessed 15 January 2024.
[135] Schmitt, 'Grey Zones in the International Law of Cyberspace' 15.
[136] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 72 para 3.
[137] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* Rule 11 para 11.
[138] Micheal N. Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' (2014) 54 Virginia Journal of International Law 697, 698.
[139] Eric Talbot Jensen and Sean Watts, 'A cyber duty of due diligence: Gentle civilizer or crude destabilizer?' (2017) 95 Texas Law Review 1555, 1558.
[140] Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' 723.
[141] Ibid 703.

law. A countermeasure can never amount to *use of force*,[142] and can only be adopted by the victim state[143] against the perpetrator state.[144] They are different from reprisals in that countermeasures are lawful, but "unfriendly" actions.[145] They are also different from the plea of necessity which could be used by a state to "safeguard an essential interest against a grave and imminent peril" and against an act that seriously impairs "an essential interest of the State".[146] In cyberspace, a countermeasure could be for instance a "hack back" operation, provided that the responsible party has been identified. However, countermeasures can be used only after the victim has asked the perpetrator to stop.[147] They also need to cease immediately after the perpetrator state has ceased with breaking international law.[148] Here, the proportionality test would be challenging, as due to the connectivity of systems the actual impact of malware, which might spread outside the real target, cannot be measured.[149] Since attribution is a key element of countermeasures, when using the latter particular attention should be given to the possibility of escalation.[150] Without attribution countermeasures would be "extraordinarily risky".[151] A cyber operation targeting a diplomatic service by intercepting classified documentation, for instance, cannot qualify as countermeasure.[152] Countermeasures will be further discussed in light of the possibility of using them when targeted by a state-sponsored cyberattack (Sections 2.3. through 2.3.4.).

[142] International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001), Article 50.
[143] Marco Roscini, 'Cyber Operations as Nuclear Counterproliferation Measures' (2014) 19 Journal of Conflict and Security Law 133, 143.
[144] Ibid 148.
[145] Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' 701.
[146] International Law Commission Article 25.
[147] Ibid Article 52.
[148] Jeff Kosseff, 'Retorsion as a Response to Ongoing Malign Cyber Operations' (12th International Conference on Cyber Conflict (CyCon) 2020), 16.
[149] Roscini 148.
[150] Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' 715.
[151] Jensen and Watts 1564.
[152] Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' 723.

iii) Retortions

Scholarship has dedicated very little attention to the option of retortion as a response to malicious cyber operations. Described as "unfriendly but legal act[s]",[153] and "cyber responses that do not cause effects that would violate international law",[154] retortion entails declaring representatives of the perpetrator state and/or the actual hackers that have performed the attack, if known, as persona non grata, and freezing their assets or blacklisting them from entering the country. If the victim state is an EU MS, the blacklisting could be extended to the Schengen zone or the whole EU. The difference between countermeasures and retortion, Kosseff observed, is that absent the cyberattack, countermeasures would violate international law, whereas retortion would not.[155] A retortion is also the more "flexible" option for a response in the sense that using it would not require an in-depth analysis of whether the operation had breached international law.[156]

Retortions have become essential during Phase Two (Section 2.2.2.2.), as they are "a flexible framework to respond to this persistent, low-level aggression".[157] Also, attribution would not necessarily be a hurdle, as individuals, acting for example as a proxy to a state's operation, can be lawfully sanctioned "based on mere suspicion of involvement".[158] The US has used retortions on a number of occasions (see Section 2.3.2.1.).

2.2.2.2. Phase Two: Peacetime state-sponsored cyber operations below the *use of force* threshold

The overview of cyber operations in Section 2.3. demonstrated that in the first years since the Estonia attacks the focus was very much on *whether* existing international law applies to cyberspace, with *how* exactly it applies causing major discussions and little breakthrough. The focus was also on those cyberattacks that could potentially cross the threshold to *use of force* and

[153] Kosseff 9.
[154] Durward E. Johnson and Michael N. Schmitt, 'Responding to Proxy Cyber Operations Under International Law' (2021) 6:4 The Cyber Defense Review 15, 22.
[155] Kosseff 11.
[156] Ibid 16.
[157] Ibid 11.
[158] Johnson and Schmitt, 22.

scholars and decisionmakers debated more on the military aspects of cyberspace. How existing international law would apply to malicious state-sponsored attacks falling below the threshold of *use of force* was given secondary importance. This sub-section will demonstrate the evolution in scholarly and policymakers' views as well as the evolution in international law's interpretation, an "inevitable" phenomenon as regards cyberspace.[159]

After the initial shock of the cyberattack against Estonia, with time scholars acknowledged that the feared cyberwars "failed to manifest in practice"[160] and that state-sponsored cyber operations would not necessarily cause the major havoc that had been expected, but rather would come to be conducted below the *use of force* threshold. In most cases, Maschmeyer observed, cyberattacks would hardly shift the global balance of power.[161] This is partially true because the state-sponsored attacks of today happen in the "grey zones" of international law. Schmitt has identified a list of six key grey zones: sovereignty, intervention, attribution, due diligence, the *use of force* and self-defence, and attacks in international humanitarian law.[162] Müller and Harnisch have further identified a state providing cyber assistance to a targeted state as a 'grey area of "undeclared cyber non-belligerency"'.[163] These will all be addressed in detail in the remainder of this Chapter.

This scholarly work was clearly a manifestation of what was happening at the decision-making table. At the UN level, 2021 was a year of great success, after four years of unsuccessful attempts to further advance the applicability of international law to cyber operations. The Open-ended Working Group on developments in the field of information and telecommunications in the context of international security report (hereinafter OEWG), finally published its report.[164] The report was a success because all 193 participating parties managed to move forward after the

[159] Schmitt and Vihul 1640.
[160] Maschmeyer 52.
[161] Ibid 86.
[162] Schmitt, 'Grey Zones in the International Law of Cyberspace'.
[163] Martin Müller and Sebastian Harnisch, 'With a little help from my friends? Cyber assistance and Ukraine's successful cyber defence' (*European Repository of Cyber Incidents*, February 2023) <https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Opinion_piece_Feb_2023_A_little_help_ab5769f036.pdf?updated_at=2023-02-27T12:13:16.994Z> accessed 10 April 2023 1, 3.
[164] United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security* (10 March 2021).

stalemate of 2017, but it largely reaffirmed what the 2013 and 2015 UN GGE reports stated, without any clarification on how exactly international law applies to cyber operations.[165]

Interestingly, at the time, all 28 EU MS had voted against the A/RES/73/27, the Resolution establishing the OEWG.[166] This did not mean the EU shied away from actively shaping the outcome of the report. Its contribution to the pre-draft report, however, whilst recognising the applicability of international law, also failed to elaborate further on *how* exactly it would apply.[167] (The limitations of the EU approach to cybersecurity in general will be analysed throughout Chapter III which will analyse how the MS's divergent views have impacted the overall EU approach). The Report of the UN GGE, which was also reassembled (where only 25 states were represented, and for whose establishment all EU MS had voted in favour[168]), went a bit further, "a historical first".[169] It noted that "international humanitarian law applies only in situations of armed conflict" and recalled "the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States."[170] Despite Mačák arguing that the two 2021 reports were important for clarifying the "murky relationship between military cyber operations and international law",[171] neither the UN GGE nor the OEWG elaborated in detail on the longstanding contentious issues of how existing principles applied to cyberspace, which demonstrated that states still could not see eye-to-eye.[172] Such lack of clarity, Lotrionte observed, could lead to misreading the intentions of other states and lead to escalation.[173]

---

[165] Alexandra Kulikova, 'Cyber norms: technical extensions and technological challenges' (2021) 6 Journal of Cyber Policy 340, 342.
[166] United Nations, *Voting on Resolution A/RES/73/27 on Developments in the field of information and telecommunications in the context of international security* (5 December 2018).
[167] Council of the European Union, *Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.* (5 March 2021) para 18.
[168] United Nations, *Voting on Resolution A/RES/73/266 on Advancing responsible State behaviour in cyberspace in the context of international security* (22 December 2018).
[169] Kubo Mačák, 'Unblurring the lines: military cyber operations and international law' (2021) 6 Journal of Cyber Policy 411, 411.
[170] United Nations General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021) para 71 (f).
[171] Mačák 412.
[172] Kulikova 344.
[173] Lotrionte 73.

To sum, the debate is still constantly evolving and states are actively taking advantage of this lack of clarity. This will be further demonstrated in the next section, which will address some of the most public state-on-state cyberattacks since Estonia: there have not been any recent attacks that posed the question whether there has been a violation of article 2(4) of the UN Charter. On the contrary, recent attacks have generally moved below the threshold, and very often, have not even violated international law norms at all. This is a particularly interesting element of state-on-state operations as cyber aggressors should indeed be called out and punished. If, however, an operation cannot be considered an internationally wrongful act, then on what grounds would they be punished? The next section will try to exemplify the peculiarities of cyberattacks that fall below the threshold of *use of force* and those that do not.

2.3. Defining the spectrum of cyberattacks

This section will delve into the different kinds of cyberattacks. Over the course of the last six years, since the development of this thesis first began, scholarship on the topic has advanced: however, whilst one might expect that in 2023 definitions on the different types of cyberattacks would have been fine-tuned and that there would be a coherent classification of what constitutes state-sponsored cybercrime, cyber war, or coercive cyberespionage, the reality is different. As seen, majorly destructive cyberattacks (as predicted in the early years since the Estonia attacks) have not really materialised, meaning that there has been no significant "material" for analysis despite increased awareness among policymakers and cyber security practitioners. Notwithstanding the rise of state-sponsored cyberattacks targeting critical infrastructure sectors in the last few years their impact has rarely been one questioning the applicability of international law to cyberspace the way it did during Phase One. However, whilst they may not have been as harmful as if they had crossed the threshold of *use of force*, they could still be considered "harmful" by the victim state due to their impact. And since the borderlines between non-harmful and harmful interference are imprecise and still subject to a live debate, states and state-sponsored actors have had the possibility to push the boundaries and explore their cyber capabilities. This has posed a challenge to experts trying to fine-tune the definitions and the thresholds. Since these have not been agreed upon, it is important for the overall purpose of this

thesis to adopt a classification and a clear-cut approach on defining the different types of state-sponsored attacks. The taxonomy used is based on already existing sources which will be referenced accordingly. Sections 2.3. through 2.3.4. will thus group cyberattacks into four types - type 1: international cybercrime; type 2: cyberespionage; type 3: cyber *use of force* (violation of UN Charter's article 2(4)); type 4: cyber *armed attack* - and will analyse their development and meaning in detail by providing examples of such incidents. The analysis will be based on two-fold criteria - the *nature* of attack together with the *damage* and the *consequences* it has caused. The focus will not be on the "means" through which an attack has been performed – whether they are DDOS, malware, phishing attacks, spyware, viruses, trojans, exploiting vulnerabilities – as the main aspect that results in their relevance for this thesis, which explores the EU's regulatory approach to state-sponsored cyber incidents, is whether they *are* state-sponsored.

When providing examples of these four types of cyberattacks, analysis in Sections 2.3.1. through 2.3.4. will focus only on those attacks that have been linked to a foreign state. For each type of cyberattack, the chapter provides a list of examples to create a better understanding of the different nuances between the different operations and types of attacks.[174] The focus here will hence not be on the issue of attribution, which will be discussed in Section 2.4.

2.3.1. Type 1. International cybercrime

Before going further with the analysis of this typology, it is important to highlight the difference between "international cybercrime" (sub-type one) and "non-international cybercrime" (sub-type two) in the context of this thesis. This classification will be based only on the *nature* of the attack. By "international cybercrime" is meant a malicious attack performed against a state, by another state or a non-state actor, for instance a DDOS attack, targeting a CI sector, the public administration, or any other public service of any sort that might lead to a disruption of activities vital for the society. As the majority of the Tallinn Manual experts observed, and as agreed by

[174] In the last decade, and especially in the last few years, there has been a surge in cyberattacks against critical sectors, but not all of them have been – or can be - linked to groups operating under a state's orders: many have been performed by independent cybercriminals not linked to a certain state. This is why the subsections providing examples of the different types of cyberattacks might not mention most of the attacks that have become public.

Lotrionte, such attacks would not amount to a violation of the territorial sovereignty of a state.[175] By "non-international cybercrime" is meant low-level and not highly sophisticated attacks against individuals or private companies, such as financial fraud, scam emails, phishing attacks, ransomware (in other words, financial scams from which the perpetrator can gain profit), or illegal interception of communications that – even if damaging for the victim - would not lead to a disruption at state level and would not require a state action, be it recovery or response to the attack. In other words, non-international cybercrime includes those types of attacks that were found in the first ever cyber-related international treaty, the Council of Europe's Budapest Convention on Cybercrime (2001), which addressed "substantive criminal law"-related offences such as illegal access, illegal interception, data and system interference and misuse of devices, "content-related offences" such as child pornography, or offences related to infringements of copyright.[176] Because the Budapest Convention addressed issues that needed to be established "as criminal offences under [the signatory Parties'] domestic law", and as such it did not address states performing such attacks, the act of committing these crimes would not lead to an international cyber conflict. Therefore, despite being an important international treaty on cybersecurity, which demonstrated a significant step towards international cooperation in cyberspace and showed some states' willingness to work and cooperate towards a legal framework, the Budapest Convention falls outside of the scope of this thesis.

Back in 2006 Gordon and Ford claimed that despite being a term that had appeared in academic journals, newspaper articles, movies, etc., what constituted 'cybercrime' was viewed differently by the different sources.[177] Indeed, the Budapest Convention did not provide a clear-cut definition of what the term entails despite providing examples of what crimes it might constitute. Gordon and Ford, therefore, defined cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device",[178] pointing out that no clear definition has major impact also on the prevention and remediation,[179] a statement ever so relevant for all the other types of cyberattacks too. National definitions of cybercrime also varied in this early period of the regulation of cybersecurity. Back in 2013, Italy identified cybercrime as "all malicious

[175] Lotrionte 80.
[176] Council of Europe.
[177] Sarah Gordon and Richard Ford, 'On the definition and classification of cybercrime' (2006) 2 Journal in Computer Virology 13, 13.
[178] Ibid 14.
[179] Ibid 13.

activities with a criminal intent carried out in cyberspace such as swindles or internet fraud, identity theft, stealing of data or of intellectual property".[180] This is a definition that fits more with the Budapest Convention's, but one which does not incorporate the politically motivated dimension of attacks that this study is focusing on. A definition that would fit more with the latter was provided by the US Law of War Manual 2015, who identified these types of crimes as "defacing government webpages; briefly disrupting Internet service in a minor way; briefly disrupting, disabling, or interfering with communications; or disseminating propaganda".[181]

Hence, in terms of their *nature* and the *damage* and *consequences* they have caused, international cybercrime would be considered low-level non-harmful operations that, however, could lead to an international response from the victim state because of the foreign interference. In terms of response, international law has several tools available to states to act even when there is no crossing of the *use of force* threshold. Clearly, the victim state would not be able to invoke the doctrine of "self-defence" launching a counter military operation. Nor would it be able to use countermeasures as clearly these are types of operations that would hardly be in breach of international law. A proportionate response here, lawful under international law, could be retortion.

2.3.1.1. International cybercrime attacks examples

There have been several cyberattacks that fit the definition of "international cybercrime". Most famously, there was the DDOS attacks on Estonia in 2007 – widely considered to be ordered by the Russian government,[182] but never officially attributed to it.[183] The attack targeted banks, media and government institutions which were flooded with spam e-mails that not only caused a complete halt in their work for weeks, but also cost them millions of euro.[184] Some analysts

[180] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *National Strategic Framework for Cybersecurity (Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico)* (December 2013) 12. Translation taken from the English version of the document.
[181] Department of Defense, *Law of War Manual* (June 2015) 1005.
[182] Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia' (*The New York Times*, 29 May 2007) <www.nytimes.com/2007/05/29/technology/29estonia.html> accessed 15 January 2024.
[183] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 289.
[184] Ibid 289.

sought to declare the intervention a "cyber war".[185] From a legal standpoint, however, this label is an overstatement. Had the attack hit the digital infrastructure of electric grids – and maybe causing loss of life and destruction in the physical world - it would have crossed the *use of force* threshold and hence could have been classified as "cyber war" (triggering consequently the rights of self-defence or countermeasures, as seen in the previous section). But no such things happened. The attack caused disruptions in the everyday life of the society, but it did not cause any major consequences such as destruction or death, thereby remaining a low-level cyberattack. Marina Kaljurand, then Estonia ambassador to Russia, observed that in a response to the attacks Estonia blacklisted the attackers and banned them from the Schengen zone. She called it a "primitive" response, but also the first instance of a diplomatic response to a cyber operation.[186] (The topic of diplomatic responses and the EU's approach to cyber diplomacy, developing since 2017, will be discussed in detail Section 3.3.2.).

Other examples from the dawn of contemporary state-sponsored cybercrime attacks include the North Korean attacks on South Korea in 2009 when banks and media websites were targeted.[187] In 2012 Iran-sponsored attack using Shamoon virus targeted employee computers of Saudi Arabia's and world's largest oil producer company Aramco, and set a burning American flag image on the screens.[188] Because the virus required thousands of the oil company's hard drives to be replaces and repaired, the Tallinn Manual 2.0's authors argued that the operations qualified as a violation of the sovereignty principle.[189]

More recent attacks include the 2022 malware targeting Viasat Inc's KA-SAT satellite network which followed the Russian invasion in Ukraine,[190] and attacks on medical institutions during the Covid-19 crisis at the beginning of 2020, particularly the (supposedly Russian) April 2020 attack

[185] See Landler and Markoff;
Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia' (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 22 January 2024.
[186] Cyen, 'Speech by Marina Kaljurand on Sanctions in cyberspace: the EU and the US diplomatic approaches' (27 May 2021) <https://www.youtube.com/watch?v=Ti7AjuUNCfE> accessed 15 January 2023.
[187] John Sudworth, 'New 'cyber attacks' hit S Korea' (*BBC News*, 9 July 2009) <http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm> accessed 21 January 2017.
[188] Nicole Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back' (*The New York Times*, 23 October 2012) <www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html> accessed 21 January 2024.
[189] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 4 para 13.
[190] James A. Lewis, 'Cyber War and Ukraine' [2022] Center for Strategic and International Studies (CSIS).

on a Czech hospital[191] (both addressed in Sections 3.3.2. through 3.5.). In their analysis of attacks on the sector, Mačák *et al* highlighted that "particularly grave cyber attacks against medical facilities could qualify as international crimes, such as war crimes" or qualify as violations of sovereignty.[192] Whilst clearly not the case here, their argument points out the criticality of the health sector and how relatively easy it is to perform a low-level attack that has huge consequences. The International Committee of the Red Cross also advanced a position whereby a new norm of responsible state behaviour was needed -namely that "[s]tates should not conduct or knowingly support ICT activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm".[193] So far this idea has not been taken onboard in any national or international legislation.

Other attacks include the 2019 botnet attack on the US Justice Department, which US authorities attributed to the North Korean government.[194] Already in 2018 the US FBI and DHS had identified two malwares used by the North Korean Government since at least 2009, targeting "multiple victims globally and in the United States—including the media, aerospace, financial, and critical infrastructure sectors".[195]

More recent international cybercrime examples include the WannaCry ransomware (North Korean-sponsored)[196] and the NotPetya attacks (Russian sponsored, targeting Ukraine)[197] of

[191] Samuel Stolton, 'Von der Leyen: Chinese cyberattacks on EU hospitals 'can't be tolerated'' (23 June 2020) <https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/> accessed 22 January 2024.

[192] Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?' (*Just Security*, 27 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 24 January 2023.

[193] International Committee of the Red Cross, 'Norms for responsible State behavior on cyber operations should build on international law' (11 February 2020) <https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law> accessed 15 January 2024.

[194] Office of Public Affairs U.S. Department of Justice, 'Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers' (30 January 2019) <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north> accessed 24 January 2024.

[195] Cybersecurity & Infrastructure Security Agency, 'HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm' (31 May 2018) <https://www.cisa.gov/news-events/alerts/2018/05/29/hidden-cobra-joanap-backdoor-trojan-and-brambul-server-message-block> accessed 24 January 2024.

[196] The UK and the US officially attributed the attack, while the EU stayed silent. Foreign & Commonwealth Office, 'Foreign Office Minister condemns North Korean actor for WannaCry attacks' (19 December 2017) <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks> accessed 24 January 2024.

[197] The UK and the US officially attributed the attack, while the EU once again stayed silent. National Cyber Security Centre, 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' (14 February

2017, which served as examples of how due to the interconnected systems, the attack can spread outside its actual victim's systems and so further evidenced the need for a common approach to cyber incidents at EU level. A seemingly low-level attack (in terms of the *nature*), a ransomware in WannaCry's case, can become a large-scale attacks in terms of the *damage* caused.

What is interesting about these examples is that it is only known what Estonia did in terms of response. All the other attacks have not had an (officially announced) response. For instance, in response to the WannaCry operation, then Foreign Office Minister for Cyber, Lord Ahmad only stated that the UK was "determined to identify, pursue and respond to malicious cyber activity" regardless of the origin, and would impose "costs" on those attacking them in cyberspace.[198] This is a rather generic statement, leading to no (at least officially) concrete steps to use retortion to respond to North Korea. The lack of official information on a potential response in the other cases prompts the question whether states do not (secretly) retaliate in-kind. This would not be an option available to the less mature states in terms of cyber offensive capabilities, but states such as the UK would certainly be among those able of performing such operations. Whether there has been an in-kind response to WannaCry or other attacks by the UK, however, is not currently known.

2.3.2. Type 2. Cyber espionage

As Lindsay puts it, the difference between cybercrime and cyber espionage is that the former "looks to exploit any unguarded host, whereas the latter "targets a particular organization or a person".[199] Performing cyber espionage, he also argues, takes experience and capacity likely to be linked to a state-body rather that a single individual.[200] Indeed, the concept of espionage has been associated with the state and customary international law has never developed any norms against it.[201] On the contrary, intelligence gathering has been considered extremely important for

---

2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 24 January 2024.

[198] Foreign & Commonwealth Office.

[199] Jon R. Lindsay, 'Cyber Espionage' in Paul Cornish (ed), *The Oxford Handbook of Cyber Security* (Oxford Academic, OUP 2021) 226.

[200] Ibid 227.

[201] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 32.

State decision-making process and governments have long been relying on facts obtained by the intelligence agencies when developing their foreign policy strategies.[202] Because espionage would not be considered *threat* or *use of force*, nation states cannot use force as a means of self-defence when responding to espionage.[203] Espionage in itself therefore does not violate international norms; however, the tools and methods to perform it might.[204]

The same rules would be valid also for cyber espionage. And because states do not have to send spies to a foreign state to get sensitive information, cyber espionage has become an "attractive" alternative to traditional espionage.[205] As part of the "new golden age of espionage",[206] cyber intelligence gathering has become a successful strategy for many states, a highly sophisticated foreign policy tool, as valuable and confidential data is stored online in most of the first-world countries and even if encrypted, contemporary ways of gaining remote access and remote surveillance, and decrypting the data are experiencing momentum. Cyber espionage has become the diplomacy tool which "constitutes a customary exception" of the general rule of inviolability of territorial sovereignty.[207]

As with cybercrime, states have so far failed to reach an agreement on a definition of cyberespionage.[208] ENISA, the European Union Agency for Cybersecurity, has further elaborated on the issue, stating that cyber espionage "focuses on driving geopolitics, and on stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields".[209]

Scholars have added their take on the topic, with Buchan summarising it as "the use of cyber operations to copy confidential data that is resident in or transiting through cyberspace, even if it is not read or analysed",[210] underlining that acquiring this data is non-consensual.[211] Similarly,

---

[202] Lung-chu Chen, *An introduction to contemporary international law: a policy-oriented perspective* (2nd edn, New Haven: Yale University Press 2000) 325.
[203] Dominik Herrmann, 'Cyber Espionage and Cyber Defence' in Christian Reuter (ed), *Information technology for peace and security: IT applications and infrastructures in conflict, crises, war and peace*, vol 36 (Routledge 2020) 83, 84.
[204] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 32.
[205] Herrmann 85.
[206] Lindsay 223.
[207] Schmitt and Vihul 1645.
[208] Russell Buchan, *Cyber espionage and international law* (Oxford, UK, Hart Publishing 2018) 13.
[209] ENISA, *Cyber espionage. ENISA Threat Landscape* (From January 2019 to April 2020) 2.
[210] Buchan 17.
[211] Ibid 13.

Kilovaty defined it as "capturing" of confidential information, "meaning interception or observation of the data".[212] But these interpretations are limited in scope – the political dimension of cyber espionage is somewhat lost in them, they do not encompass all the nuances of espionage attacks, and they do not explicitly refer to the difference between economic espionage and politically motivated espionage. Therefore, for the purpose of this thesis, state-sponsored cyber espionage will be defined as a politically motivated operation which, through the use of ICT devices, aims at acquiring remotely located valuable data, stored on an ICT device.

2.3.2.1. Cyber espionage examples

There has been an enormous amount of state-on-state cyber espionage operations and those states who were able to perform them 30 years ago are still those performing them today. Considering this thesis focuses on the EU as a cybersecurity regulator, this subsection will focus on those attacks targeting either its MS or its closest ally – the US. As we will see, Russia and China were identified as the main perpetrators.

Among the first documented state-on-state cyber espionage operations is the 1998 Moonlight Maze operation which targeted confidential information about US military technologies. The attack was successful and resulted in stolen confidential data. Although Russia was the suspected perpetrator,[213] even US attribution capabilities at the time were not advanced enough to attribute the attack with certainty.

In the early 2000s China also made its name as a capable cyber espionage authority. Operation Titan Rain via which unclassified information across many US Government organisations was accessed was labelled among "the most pervasive cyberespionage threats" against the US.[214] In 2011 there was another reportedly Beijing-sponsored attack aimed at accessing data in the Finance Ministry of France. Called "one of the most sophisticated cyberattacks ever launched at

[212] Ido Kilovaty, 'World Wide Web of Exploitations – the Case of Peacetime Cyber Espionage Operations Under International Law:: Towards a Contextual Approach' (2017) 18 Science and Technology Law Review 42, 48.
[213] Hodgson, Shokh and Balk 11.
[214] Ibid 25.

the government", it tried to access G-20 classified documents before its meeting in February of the same year.[215]

More recently, another cyber espionage operation was the DNC hack of 2016, in which a foreign state managed to access classified data of an adversary which was then leaked online.[216] The allegations were denied by President Putin himself, who stated "[t]he hysteria aims only to distract the attention of the American people from the substance of what hackers had put out. And the substance was the manipulation of public opinion."[217] The US Government did not stay silent this time - it sanctioned five Russian entities and four individuals, expelled 35 diplomats suspected of being Russian intelligence operatives, and closed two US-based Russian compounds.[218] The decision to use only retortions received a lot of criticism describing it as inadequate and insufficient,[219] and implied that the Russia-led operations did not break international law – otherwise the US could have used countermeasures, as discussed in Section 2.2.2.1.B) ii). Nonetheless, in his statement, then President Obama added also: "[t]hese actions are not the sum total of our response to Russia's aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized."[220] Such a statement prompts the question whether there was a lack of agreement among government representatives as to whether the operation in reality breached international law, and if yes, which principles exactly.[221] The fact that President Obama did not provide any clear-cut identification of which principles the operation breached fuelled such speculations. None of these actions he avowed, however, ever became public over time - therefore it is again speculative whether there has ever been either an in-kind response, or any other type of response.

---

[215] Peggy Hollinger, 'Cyber attackers target G20 documents' (*Financial Times*, 7 March 2011) <www.ft.com/content/83dc8ce4-48f4-11e0-af8c-00144feab49a> accessed 21 January 2017.

[216] US Intelligence Community Assessment, 'Assessing Russian Activities and Intentions in Recent US Elections' (6 January 2017) <https://s3.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf> accessed 24 January 2024.

[217] Ilya Arkhipov and Anna Andrianova, 'Putin Vents at U.S. for 'Hysteria' Over Hacking Blamed on Russia' (*Bloomberg*, 12 October 2016) <www.bloomberg.com/news/articles/2016-10-12/russia-denies-u-s-allegations-of-hacking-attacks-on-elections> accessed 20 January 2024.

[218] The White House Office of the Press Secretary, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment* (29 December 2016).

[219] Crootof 587.

[220] The White House Office of the Press Secretary, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*.

[221] Ryan Goodman, 'International Law and the US Response to Russian Election Interference' (5 January 2017) <https://www.justsecurity.org/35999/international-law-response-russian-election-interference/> accessed 24 January 2024.

The majority of scholarship seems to agree that the attack constituted a violation of sovereignty because the hack "involved nonconsensual intrusion into cyber systems located in the U.S.".[222] Others, however, have disagreed calling the hack merely routine espionage.[223] These opposing views show how difficult identifying if and how international law's norms can be breached in cyberspace is and further support Schmitt's argument that there are 'grey zones' of international law.

Other 2016 cases include the allegedly Russian hacker-led operation (performed probably by the same group responsible for the DNC hack) which managed to access Italian Air force servers but was unsuccessful in accessing the most classified data regarding F-35 combat aircraft.[224] Another similar case, involving cyberespionage against Italian governmental infrastructure, is the 2014-2015 operation against the Ministry of Defence, aiming at accessing NATO data. No information that would have compromised national security was accessed, but it is not clear whether NATO documents' security was breached.[225] Supposedly Russian groups linked to the state were also named as perpetrators in a number of cyber espionage attacks performed in 2015 in Germany targeting the Parliament and the Christian Democratic Union party.[226]

Other recent cyber espionage attacks include Covid-19-related operations. During the first months of the pandemic, the UK's National Cyber Security Centre (NCSC), together with their Canadian and US counterparts, published a report stating that the group ATP29, "almost certainly" operating as part of the Russian intelligence services, has been trying to access organisations in the UK, Canada and the US dealing with Covid vaccines development and testing.[227] These allegations were denied by Russia.[228] Russia's Foreign Intelligence Service,

---

[222] Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack'.
[223] Ibid.
[224] Giuliano Foschini, 'Russian hackers, blitz against the Air Force in search of F-35's secrets (trs)' (*La Repubblica*, 14 January 2017) <www.repubblica.it/cronaca/2017/01/14/news/hacker_russi_aeronautica-155988414/> accessed 15 January 2024.
[225] Marco Mensurati and Fabio Tonacci, 'Russian hackers in the servers of Italian Ministry of Defence (trs)' *La Repubblica* (17 February 2016) <www.repubblica.it/cronaca/2016/02/17/news/hacker_russi_ministero_difesa_italiano-155988416/> accessed 21 January 2017.
[226] 'Russia 'was behind German parliament hack'' (*BBC News*, 13 May 2016) <www.bbc.co.uk/news/technology-36284447> accessed 21 January 2017.
[227] National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development' (16 July 2020) <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> accessed 24 January 2024.
[228] Chris Fox and Leo Kelion, 'Coronavirus: Russian spies target Covid-19 vaccine research' (16 July 2020) <https://www.bbc.com/news/technology-53429506> accessed 24 January 2024.

SVR was also officially blamed for the 2020-2021 SolarWinds hack.[229] The main victims were in the US and the latter responded once again with retortions.[230] The damage of the attack spread to both the public and the private sector, but the attack spread also worldwide.[231] Six out of fourteen EU institutions, agencies and bodies which used the SolarWinds product also fell victim to the attack,[232] (yet the EU's response seen in Section 3.3.2.1. was underwhelming). According to Ward and Alperovitch, because the operation was "limited in scope, carefully executed, and not designed to destroy, manipulate, or otherwise disrupt data", the US could have considered it "acceptable under existing international norms".[233] Johnson and Schmitt seemed to agree with these views, stating that the SolarWinds hack had "an ambiguous legal character".[234] He also observed that it was not the act of espionage itself that prompted the US to use sanctions – admittedly also the US performs such operations – but there were a number of elements that were considered: the scale of the attack, the attacker's track record, the attack's spread, the nature of the targets (governmental, CI, financial entities), and the ultimate financial cost of remediation.[235] Precisely because of the elements described by Chestney, but considering also the uncertainty of whether international law norms were violated, the US had to respond in an official way. The response measures – at least those officially declared - were retortions: in a statement, the Biden administration declared that it has sanctioned ten Russian individuals, but because it included other issues, e.g. meddling in the 2020 Presidential elections, it was not very clear whether these measures applied strictly to the SolarWinds hack.[236] Nonetheless, it was yet another response to a foreign-sponsored cyber operation. Each response furthers the development

[229] The White House, 'FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government' (15 April 2021) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> accessed 24 January 2024.
[230] Johnson and Schmitt 22.
[231] Brad Smith, 'A moment of reckoning: the need for a strong and global cybersecurity response' (17 December 2020) <https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/> accessed 24 January 2024.
[232] Mr Hahn (on behalf of the European Commission), 'European Parliament Questions to the European Commission: SolarWinds hack' (13 April 2021) <https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.pdf> accessed 24 January 2024.
[233] Dmitri Alperovitch and Ian Ward, 'How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks? ' (*Lawfare*, 12 March 2021) <https://www.lawfaremedia.org/article/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks> accessed 24 January 2024.
[234] Johnson and Schmitt 22.
[235] Robert Chesney, 'Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?' (15 April 2021) <https://www.lawfaremedia.org/article/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross> accessed 25 January 2024.
[236] The White House.

of opinio juris, and helps better define both the types of cyber operations and the appropriate response to them.

2.3.3. Type 3: Crossing the threshold: violating Article 2(4)

Article 2(4) of the UN Charter provides no definition or examples of *use of force*. Historically, there has always been a "practice of relying on vaguely defined grounds justifying *use of force*."[237]The term has seen a substantial development since the Charter was written, especially in the last decades. A relatively restricted (and vague) meaning before, today's legal doctrine has expanded its scope.[238] The rise of terrorist threats, humanitarian interventions to protect human rights in dictatorial states, or helping failed states are among the reasons states have used to justify their *use of force*.[239] The term "anticipatory self-defence" against force has also become relevant to decision-makers[240], as well as the 21st century upgraded version of humanitarian intervention – the responsibility to protect.[241] There is no doubt that the rise of the number of state-sponsored cyberattacks is also one of the reasons for the shift in interpretation of the term. But with regards to what cyber *use of force* could be, it is difficult to define, as legal doctrine – even in previous ICJ cases such as the *Nicaragua case* – still does not offer enough grounds upon which a definition could be based. The following paragraphs will aim at filling this gap.

2.3.3.1. Cyber *threat of force*

Before exploring the possibility of a war waged in cyberspace, it is interesting to examine a neglected aspect of article 2(4) of the UN Charter. Even though the expression *threat of force* is found in the article, which forbids *both threat* and *use of force*, legal scholars have neglected it in

[237] Brownlie 47.
[238] Armstrong, Farrell and Lambert 153.
[239] Wolfrum, *The Max Planck encyclopedia of public international law* 607.
[240] Armstrong, Farrell and Lambert 131.
[241] For more detailed information on the responsibility to protect, view ibid 144.

their discussions.[242] The *threat* has remained in the shadow of the bigger danger – the actual *use* of force, the actual attack. By being disregarded by legal practitioners, doctrine on the matter never really developed. What constitutes *threat of force*, when would it be a violation of article 2(4) and when would it be considered lawful, are among the questions that have never been answered.[243] But in the cyber domain this long overlooked term might find a fruitful soil to grow and develop. Considering how dangerous a cyber *use of force* can be, feeling threatened by the possibility of it occurring would also not be a welcomed turn of events. In the *Legality of the Threat or Use of Nuclear Weapons* ICJ opinion, the Court declared that "[t]he notions of "threat" and "use" of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal – for whatever reason – the threat to use such force will likewise be illegal".[244]

If we were to side with the ICJ's views, it could be argued that some recent cyber operations could fit the description: the cyber operations performed against Ukraine in 2015 and 2016, most likely by Russia,[245] could be a good example. The December 2015 incident left a whole region of the country without electricity for hours, and is considered the first major and successful attack on an electricity grid. Security experts said that the malware was sophisticated enough to only allow the system to be switched back on manually, not remotely.[246] This attack clearly did not amount to *use of force*, because it did not have the main characteristics: violence, destruction and death. But it could be considered "cyber *threat of force*" for a number of reasons.

First, the current political situation between the two states was already critical at the time, and it had been continuously deteriorating since 2014, after Moscow's annexation of Crimea and the subsequent civil conflicts in eastern Ukraine in which Russia supported pro-Russian rebels.[247] Second, the fact that the intruders performed this attack shows that they had learned how to remotely control power grids. This could indicate that they had mastered (or will master) the

[242] Nikolas Stürchler, *The threat of force in international law* (Cambridge: Cambridge University Press 2007) 1.
[243] Ibid 3.
[244] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* International Court of Justice (1996) 96.
[245] Chris Vallance, 'Ukraine cyber-attacks 'could happen to UK'' (*BBC News*, 29 February 2016) <www.bbc.co.uk/news/technology-35686493> accessed 15 January 2024.
[246] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (*Wired*, 3 March 2016) <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> accessed 25 January 2024.
[247] Pavel Polityuk, 'Ukraine to probe suspected Russian cyber attack on grid' (*Reuters*, 31 December 2015) <www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231> accessed 15 January 2024.

ability to also access hospitals or air traffic control servers – an attack on which will definitely fit into the cyber *use of force* definition. Third, many government institutions were repetitively targeted with low-level intrusions in late 2016, with President Poroshenko declaring the number of attacks was around 6,500.[248] Lastly, and most importantly, in December 2016 Ukraine suffered a "suspected" cyberattack on the power grid again, this time in Kiev.[249] Twice is not enough to prove repetitiveness and rise of danger, but it signals that the attacker has the ability to cut the power at their convenience. It is speculative whether the attacks might rise to actual *use of force* or the intrusions, if continued, will be kept (most likely intentionally) right below the threshold. But being in a constant situation of high alert does indicate the feeling of being threatened. Moreover, Poroshenko even declared that "directly or indirectly, Russian cyber teams are "waging a cyber war against" Ukraine.[250] If that is indeed correct, it puts Ukraine in the position of a victim of *threat of force*, as it could never know when and what the next attack will hit. Considering ICJ's *Nuclear Weapons* Opinion on the legality of the *threat of force*, it would seem that, if a state has indeed organised the attacks, it has violated article 2(4).

2.3.3.2. Cyber *use of force*

Cyber warfare is described as "activities and operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance".[251] This definition also has its limits – it does not become clear that for an attack to classify as cyber warfare, it needs to be state – or non-state-actor-sponsored: an individual or a group of individuals' attack, even if politically motivated, would hardly qualify as waging war on a state if not connected to a government or an ideologically motivated group. Thomas Rid has put it more clearly: cyber warfare involves "a potentially lethal, instrumental, and political act of force conducted through

[248] Natalia Zinets, 'Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'' (*Reuters*, 29 December 2016) <www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC> accessed 15 January 2023.
[249] Pavel Polityuk, 'Ukraine investigates suspected cyber attack on Kiev power grid' (*Reuters*, 20 December 2016) <www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF> accessed 15 January 2024.
[250] Zinets.
[251] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *National Strategic Framework for Cyberspace Security* (Presidenza dei Consiglio dei Ministri, Dicembre 2013) 13.

a malicious code".[252] The difference in interpretations once again lies in the political dimension, with Rid's "political act of force" clearly indicating a state or a non-state actor backed attack.

Schmitt pointed out that in cyberspace defining what operations constitute *use of force* is a "dilemma".[253] "A cyber operation constitutes a *use of force* when its scale and effects are comparable to non-cyber operations rising to the level of a *use of force*",[254] and so it "must attain a certain gravity".[255] This means that deaths and destruction, or what McGraw calls a "consequential impact in the physical world",[256] usually associated with a kinetic action, are necessary requirements for meeting the cyber *use of force* threshold. Some international lawyers would also count replacing or physically repairing hardware,[257] and others point out that timing and the context are crucial as well.[258] Infecting the command and control systems of an adversary with malware that allows the perpetrator to take control of a drone attack, for instance, was also considered a possible example of cyber war.[259] Schmitt makes the case for a "not exhaustive" list of seven factors, subsequently incorporated also into the Tallinn Manual, that need to be considered in order to determine if a cyberattack has crossed the *use of force* threshold: severity (involving physical harm), immediacy (of the consequences), directness (examining the chain of causation), invasiveness (targeting secure systems), measurability (quantifiable consequences), presumptive legitimacy (propaganda, espionage or psychological warfare are not considered prohibited by international law), and responsibility (of the state performing the attack).[260] These seven factors are to be considered together as none of them, except from severity, can indicate on its own a cyber operation that has amounted to *use of force*.[261] His analysis gives clear definitions, but these factors would only be applicable if an attack on critical infrastructure is

[252] Rid, 'Cyber War Will Not Take Place' 5.
[253] Schmitt, '"Below the threshold" cyber operations: the countermeasures response option and international law' 719.
[254] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* Rule 11.
[255] Brownlie 366.
[256] McGraw 112.
[257] Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack'.
[258] Ido Kilovaty, 'The Democratic National Committee Hack: Information as Interference' (*Just Security*, 1 August 2016) <www.justsecurity.org/32206/democratic-national-committee-hack-information-interference/> accessed 5 December 2023.
[259] McGraw 112.
[260] Micheal N. Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' (Proceeding of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy) 155.
[261] Schmitt, 'Grey Zones in the International Law of Cyberspace' 14.

proved to have been caused by a cyber intrusion. Evidently, they would not apply to unnoticed, under the radar, long and systematic malware causing harm and destruction in the physical world, simply because the real cause might remain a mystery – which is exactly what happened with the Stuxnet worm. When it was discovered in 2010, experts realised that there had been a more than two-years long and carefully organised on-going state-backed operation that was never detected before.[262]

Lotrionte further developed the nuances in labelling a cyberattack as *use of force*. While she agreed with the *de minimis* standard, whereby the quantity of force matters, she concluded that there was no one-size-fits-all and whether some operations involving minimum *use of force* would violate article 2(4) of the UN Charter would depend on "the specific circumstances of each case".[263]

Given the operational, technical and legal developments in the field whereby measures on cyber resilience of the CI sectors have been put forward across the world, it is unlikely that a cyber intrusion of the level and impact of the Stuxnet worm remained undetected for a long time, yet not completely impossible.

It is also difficult to put cyberattacks that amount to *use of force* on the same spectrum of physical *use of force* attacks that cause immediate death and visible destruction. To be precise, cyberattacks cannot be considered the same as physical intrusions because there is nothing physical in them – technology, e.g. a computer, is required for the malicious code to be build, but nobody blames the machine producing weapons when it comes to kinetic attacks. Therefore, a cyber intrusion cannot be considered the same as a physical intrusion. This, however, does not mean that a cyberattack cannot cause harm, damage and severe destruction and therefore amount to *use of force*. Cyber weapons are simply a different type of weapon that could cause harm in the non-digital realm and even trigger a kinetic (counter)attack. As early as 1963 Ian Brownlie highlighted the importance of deciding "if use of weapons which do not involve any explosive effect with shock waves and heat involves a *use of force*", and in considering bacteriological, biological and chemical weapons, he concluded that they do

[262] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown Publishing Group, Division of Random House Inc 2012) 188.
[263] Lotrionte 85.

constitute *use of force*, because they are "referred to as 'weapons' and as forms of 'warfare'".[264] It is safe to say that cyber weapons, or malware capable of causing severe damage in the physical world, would have made his list had they existed in the 1960s.

But even if cyber *use of force* is different than physical measures, it is indisputable that major harm can be caused by cyber operations. Nonetheless, declaring that an operation has crossed the threshold is a very dangerous thing for states to contemplate. Schmitt maintained in 2010 that decision-makers are still hesitant about which cyber-intrusions could be declared *use of force* because by doing so they might trigger an escalation of the situation.[265] In 2023 this is still the case.

A) Cyber *use of force*: the Stuxnet worm

Arguably the most famous and targeted cyber *use of force* to date is the US-Israeli Stuxnet worm targeting Iranian nuclear plans. The worm was only discovered in 2010, but it was launched sometime in 2008, which meant two years of sustained meddling with the Iranian nuclear plants.[266] The Bush administration was trying to find a way to delay Iran's nuclear programme without physically attacking the country with military intervention.[267] Had Bush decided to attack Iran, the operation would have had major consequences, bearing in mind that was the era of massive US military presence in the Middle East region, already shaken by unpopularity among people protesting against US military involvements around the globe. Therefore, in a way, Bush, and subsequently Obama, managed to keep Iran away from becoming a yet another physical war zone by merely using cyberattacks. "Peace" was preserved. These attacks caused no harm to the population, but they destroyed governmental facilities. The threshold to *use of force* was thereby crossed.[268] Moreover, a state's internal affairs were interfered with by a foreign government, thereby violating both Iran's territorial sovereignty and the non-intervention

[264] Brownlie 362.
[265] Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' 155.
[266] Sanger.
[267] Ibid 188.
[268] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* Rule 10 para 9.

principle. Iran could have acted in self-defence, had they known about the existence of the worm from the very beginning. Yet they did not because at the time no government had a clear idea what an appropriate response justified by international law would be. The attack also demonstrated the advanced cyber capacities the US (and Israel) had years before other states did.

Even though the majority of scholarship has now confirmed that Stuxnet was a violation of article 2(4), not all cyber warfare experts agree. Thomas Rid asserts that none of the widely known cyberattacks could be classified as "war" because they fail to meet the criteria of political motivation, instrumentality and violence.[269] A possible explanation for these conflicting opinions could be the fact that a cyberattack (if caught) does not cause instant consequence for the victim nation: the civilian casualties or damage and destruction generally associated with a kinetic attack, are not observed in the immediate aftermath of a virtual attack. However, downgrading a cyberattack that amounts to *use of force* to cyber espionage could lead to underestimating the actual threat and undermine the attempts to work towards international agreement on the issue.

2.3.4. Type 4. *Armed attack*

The most severe case of a cyber operation would be the one equivalent to an *armed attack* in the non-virtual world.

The UN Charter does not provide a definition on *armed attack.* The IGE agreed that an attack in the virtual world could amount to *armed attack.*[270] They also agreed that ICJ's *Nicaragua judgment*'s "scale and effects"[271] are the relevant factors to be considered to determine if the case is an *armed attack*.[272] They however disagreed upon the statement, put forth by some members, that even if the attack does not cause major destruction or harm, it could still classify as "*armed attack*" under international law. This would happen if the attack brings down the state's economy for instance.

[269] Rid, 'Cyber War Will Not Take Place' 5.
[270] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 54.
[271] According to the Nicaragua Judgement 1986, Merits "195. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its **scale and effects [emphasis added]**, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces."
[272] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 45.

The US DoD Law of War Manual provides some examples of what a cyber *armed attack* could cause:[273] nuclear plants meltdown, damaging a dam in close proximity of many people, interfering with air traffic control in order to cause a plane to crash, or crippling a military logistic system.[274] Based on this list, it could be argued that the Stuxnet worm was actually an *armed attack*.

2.4. Attribution

Back in 2013, the UN GGE's report included a strong appeal to states how to act responsibly in cyberspace: "[s]tates must meet their international obligations regarding internationally wrongful acts attributable to them". The report also added that states should not use "proxies" in conducting such acts and should try to ensure that their territories are not used by non-state actors for conducting malicious cyber operations."[275] Also in 2013, the Tallinn Manual's Rule 6 affirmed the legal responsibility of states in cyberspace: "[a] State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation".[276]

These two statements how that state responsibility and attribution were at the core of the international community's efforts to address state-sponsored malicious cyber operations. Attribution remains a critical issue to address as it lays at the heart of any potential response a victim state might decide to use. But if defining the relevant thresholds of cyber operations is a difficult task for scholars and policymakers alike, attribution is even more difficult to define because of difficulties with identifying the perpetrators accurately.[277] However, whilst identification might be problematic for some states, it appears less so for others. Back in 2016, the US Attorney General John Carlin declared that "the days of perceived anonymity are gone. … No matter where a hacker is located or who he is affiliated with – China or North Korea, ISIL

[273] Historically, in US policy, use of force and armed attack have been put on the same level, while internationally, use of force is considered a milder operation. Milanovic and Schmitt 259.
[274] Department of Defense, *Law of War Manual* 998.
[275] United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security* para 23.
[276] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* Rule 6.
[277] Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?' 317.

or SEA – we can figure who did it, by name and face, we can do so publicly and we can impose consequences."[278] The EU has also demonstrated advanced attribution capabilities when it named eight individuals and four entities for having conducted cyber operations on EU soil in 2020, an issue that will be discussed in detail in Section 3.3.2.1.

This Section will therefore discuss various types of attribution: whilst only state-on-state attacks fall within the scope of this thesis, there are other possibilities in which a state can be involved in a cyber operation, even if it is not directly executed by it. Section 2.4.1. will provide an overview of those state-on-state attacks that have clearly been attributed to state authorities. From a legal perspective, such operations are easier to analyse as the perpetrator is clearly identified. Section 2.4.2. will focus on operations performed by non-state actors affiliated with a state. The analysis will hence address the role of the non-state actors engaging in cyber operations under the orders of, or being financed by, a state. This subsection will offer a more exploratory analysis, as identifying the responsible party in these cases is much more difficult.

2.4.1. Attribution to a state

There has been a huge amount of cyberattacks in the last decade and those that have been made public because of the major damage they have done were mainly state-sponsored attacks. Indeed, very rarely are highly sophisticated cyber-attacks targeting a state not linked to another state.[279]

Some examples of attribution have already been mentioned throughout this Chapter. In the Stuxnet worm case, the intruder was discovered and it was attributed to the US and Israel. In Estonia, it was never officially confirmed that it was Russia, but it is generally believed by the international community that it was them. In 2016 the US attributed the DNC hack to Russia. In 2017, the UK and the US attributed WannaCry and NotPetya to North Korea and Russia respectively, but many other states stayed silent, as did the EU in the immediate aftermath of the

[278] The United States Department of Justice, *Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector* (24 March 2016).
[279] Bela Bonita Chatterjee, 'International law and cyber warfare: an agenda for future research' (*Lancaster: Lancaster University*, 2014) <www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/security-lancaster/tallinn_report_final[1].pdf> accessed 6 December 2016.

attacks. In 2018 the UK was again pointing fingers at Russia, attributing to it the DNC hack,[280] the breach of the World Anti-Doping Agency (Wada) systems, the attack on Ukraine's CI – Kyiv's metro and Odessa's airport of 2017, the cyber operations against a UK TV station in 2015 and the 2018 attacks on the Organisation for the Prohibition of Chemical Weapons (OPCW) computers and networks.[281] In 2021 the Biden administration attributed the SolarWinds hack to Russia.[282] Despite there being victims in the EU as well, including some EU institutions and agencies, the EU is yet to officially attribute that attack (the issue will be further discussed in Section 3.3.2.1.). An EU state attribution, however, followed the satellite KA-SAT network, with the EU "strongly condemn the malicious cyber activity conducted by the Russian Federation against Ukraine".[283] (EU attribution capabilities will be discussed in Sections 3.3.2 through 3.3.2.3.) More recently, in late 2022 Albania attributed a series of cyberattacks targeting the digital infrastructure of the Albanian government, with Albanian Prime Minister Rama stating that the attacks were "orchestrated and sponsored by the Islamic Republic of Iran".[284] In a response to the attacks Albania cut diplomatic relations with Iran – a response that Rama called "fully proportionate to the gravity and risk" of the attacks.[285]

So far, however, attribution to a state has not seem to work as an efficient deterrent. As Eichensehr argues, "[m]easuring the deterrent effect of attributions is difficult".[286] Whilst that might be true, it is always good practice to point the finger to malicious stet-sponsored activity as what is not being perceived as a deterrent in cyberspace today might become such tomorrow.

[280] The purpose of this attribution was more of a political message rather than anything else – the UK was not a victim in the hack.
[281] National Cyber Security Centre, 'Reckless campaign of cyber attacks by Russian military intelligence service exposed' (3 October 2018) <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> accessed 22 December 2023.
[282] The White House.
[283] Council of the EU, *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union* (10 May 2022).
[284] Albanian Government, 'Videomessage of Prime Minister Edi Rama' (7 September 2022) <https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/> accessed 15 January 2024.
[285] Ibid.
[286] Kristen E. Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67 UCLA Law Review 520, 553.

2.4.2. Non-state actors and malicious cyber operations

The possibility of non-state actors performing malicious operations on other states was already implicitly included in the 2013 UN GGE report which stated that states should be proactive in ensuring that their territories are not used by malicious non-state actors.[287] Jensen and Watts advanced the idea of a proxy system whereby if a state has failed to perform its due diligence obligations - meaning that a state needs a "diligent management of territorial cyber infrastructure" – these "nondiligent States" could be the responsible party indirectly, as a proxy.[288] The authors, however, admit that this system is not a panacea as, if applied "aggressively", proxy responses might be counterproductive and cause greater instability.[289] The Tallinn Manual 2.0 nonetheless concluded that the due diligence principle applies to cyber operations: according to Rule 6 "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.".[290] They also added further granularity, clarifying the issue of having a transit state involved in the picture too – where the operation is mounted from the territory of state A, it goes through the territory of state B and strikes state C. In the case of the transit state being aware of its territory being used for malicious cyber activity and having done nothing to terminate it, it is the transit state that bears the due diligence obligation.[291]

The attribution of nominally non-state actors' activity to a particular state, or the apportioning of blame to a state that shelters such individuals, is an area that has not been given enough attention. The topic of where an aggressive cyber operation (that amounts to *use of force*) performed by a non-state actors or terrorist organisations would fit into the spectrum of cyber assaults appears to be even more problematic for scholars as they disagree over recent developments in relevant laws. Even in the case of state-sponsored attacks, the latter might be performed by non-state actors, not necessarily officially affiliated with the government. Hence it

[287] United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security* para 23.
[288] Jensen and Watts 1558.
[289] Ibid 1558.
[290] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 6.
[291] Ibid Rule 6 para 13.

becomes more complex to discuss attribution to a state as the rules of state responsibility apply solely to states.[292]

Former US President Obama addressed the issue stating that there are "non-state actors that can do enormous damage."[293] Identifying these non-state actors is crucial: existing scholarship has underlined the importance of clear division between actions performed by isolated individuals and those of organised groups. According to Schmitt, even if some individuals or "unorganized mobs" are targeting governmental infrastructure, the attack could not amount to "armed conflict" in the sense intended in the Geneva conventions.[294] Although this is true, it is applicable only to a kinetic attack (which was what it was meant by "armed conflict" according to article 2 of the First Geneva Convention of 1949: "armed conflict (…) may arise between two or more of the High Contracting Parties"[295]). But it is not applicable in cyberspace where an individual could easily be physically able to launch a severely destructive operation on critical governmental infrastructure (individual responsibility will be discussed below). The picture changes when an "armed group" is involved – the *armed attack* threshold can potentially be met - if major physical damage or death have occurred.[296] This argument is subject to debate, but *sensu stricto*, since the UN Charter and customary international law apply to states, actions by a non-state actor, if not working for the government, would not be in violation of article 2(4).[297] As stated in the *Max Planck Encyclopaedia of Public International Law*, "[r]ecent State practice (…) confirms that armed force used by non-State actors only becomes relevant with regard to the prohibition of the *use of force* if it can be attributed to a State other than the one affected by it".[298]

Again, it is also disputed what a response against non-state actors or terrorist groups might be. Countermeasures in response to an operation mounted by a non-state actor are prohibited unless

[292] Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?' 319.
[293] The White House Office of the Press Secretary, 'Remarks by the President in Year-End Press Conference'.
[294] Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' 175.
[295] Dietrich Schindler and Jiří Toman (eds), *The laws of armed conflicts. A collection of conventions, resolutions and other documents* (Geneva, Henry Dunant Institute 1973) 298.
[296] Micheal N. Schmitt, 'Five Myths in the Debate about Cyber War' (*Just Security*, 23 September 2013) <www.justsecurity.org/918/myths-debate-cyber-war/> accessed 6 December 2016.
[297] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 43.
[298] Wolfrum, *The Max Planck encyclopedia of public international law* 614.

the operation – the wrongful act - is attributable to a State,[299] which gives a certain "marked asymmetric advantage"[300] to these groups. This fact is important because not all non-state actors necessarily act under the government guidance. However, a State is responsible for all the digital infrastructure located within its territory,[301] hence, it could be argued that countermeasures against a state, even if not directly responsible for the attack, are lawful. In light of these considerations, it is important to add the ICJ's *Congo judgment*, which confirmed the right to self-defence against non-state actors[302] - a view not shared by all scholars.[303] Nevertheless, this judgment is of great significance considering the rise or various ideologically motivated non-state actors over the last few years. It is crucial that the field of international law develops at the same pace as current trends in international crime, especially with regards to cyber operations performed by non-state or terrorist groups.

For the purpose of this thesis, it is essential to differentiate between three types of non-state perpetrators: individual contractors (a single individual or a group of people) with no political or ideological affiliation sponsored by a government, individual contractors with no political or ideological affiliation financed by a government and non-state actors that act as an organised group under the same ideology (cyberterrorists). The difficulties with attributing certain attacks to these three types are, as expected, even more challenging than the difficulties observed in the previous paragraphs. Moreover, they are very different to one another – the main difference is rooted in the reasons behind the involvement of the perpetrator. While a private contractor may only be the executor of the attack and have no personal reasons to do it, a terrorist cyberattack would more likely be based on ideological (therefore personal) ground.

[299] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rules 15 and 17.
[300] Micheal N. Schmitt, 'Normative Voids and Asymmetry in Cyberspace' (*Just Security*, 29 December 2014) <www.justsecurity.org/18685/normative-voids-asymmetry-cyberspace/> accessed 6 December 2016.
[301] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* 13 (f).
[302] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* ICJ Reports 2005.
[303] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 71 para 19.

2.4.2.1. State-sponsored attacks by non-state actors

Non-state actors conducting cyber operations on states has been a challenging topic to address from a legal standpoint. Schmitt has included operations conducted by non-state actors, but linked to a states, as one of the "grey zones" of international law.[304] Suppose the following scenario is considered: a massive cyberattack is conducted (whether it amounts to *use of force* is immaterial for the purposes of this hypothesis) and it is government-organised by State A; the government has hired a group from State B; they perform the attack on state C from the territory of State D (no nationals from state C or D are involved in the group). Who would be the responsible party in this case? If the intrusion amounts to *use of force*, self-defence might be at place. If below the threshold - countermeasures. But against whom could State C act so that its actions are lawful?

UNGA's *Friendly Relations Declaration* specifically addresses the use of non-direct *use of force*, stating that "[e]very State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands including mercenaries, for incursion into the territory of another State".[305] In accordance with this principle, when dealing the issue of government-sponsored non-state actors in the *Nicaragua case*, the judges of the ICJ concluded that "arming and training" these individuals would amount to *use of force* by state A, in this case.[306] However, according to article 2(a) of the Draft Articles on State Responsibility, an "internationally wrongful act" would occur if "is attributable to the State".[307] But if attribution cannot be proven, would the state still be considered as a perpetrator of international law by participating in indirect *use of force*? State C might suspect that state A organised the attack, but if it is not certain, it cannot act in self-defence, or even apply countermeasures, against A, as there would be no legal grounds to do so. Even anticipatory self-defence would not apply, because there would be nothing to "anticipate". According to the *Nicaragua* judgment, for a state to have "legal responsibility", "it would in principle have to be proven that that State had

[304] Schmitt, 'Grey Zones in the International Law of Cyberspace' 9.
[305] United Nations General Assembly, *Declaration on Principles of International Law Concerning Friendly Relations And Co-Operation Among States in Accordance with The Charter Of The United Nations (GAR 2625)* (1970).
[306] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement (1986)* International Court of Justice para 228.
[307] *International Law Commission*International Law Commission.

effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[308] It seems that state A is responsible only if guilt is proven. Therefore, an act of self-defence could be applied only in the case state C is certain that state A ordered the attack and manages to prove it in a timely manner. If attribution does not occur, any act against the territorial sovereignty of state A would be considered violation of international law – even if the act would be in fact be considered "self-defence" by the victim state C. If we consider the proxy theory discussed above, a response against state D could take place as the latter failed with its due diligence, however this option is also not without flaws as it would miss "the mark with respect to [actual] culpability".[309]

Regarding the government-sponsored non-state actors, under article 8 of the Draft Articles on State Responsibility – *conduct directed or controlled by a State* - it seems that even if state A has hired nationals of states B and C, state A would still be the perpetrator of breaches of international legal obligations.[310] Again, however, this is only the case if attribution to A is proven.

With regards to state D from whose territory the hack was performed, it appears from the Tallinn Manual that the IGE could not agree whether if the state did not know about the attack, it violated its responsibility to "use due care in policing cyber activities on its territory".[311]

In sum, if a state-affiliated non-state actors mount an operation that violates article 2(4), the *state* would have violated article 2(4), but can only be held responsible if culpability is proven. This gives an incredible advantage to states investing in cyber offensive operations that are enacted by non-state actors.

[308] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement (1986)* para 115.
[309] Jensen and Watts 1575.
[310] International Law Commission.
[311] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 28.

2.4.2.2. Attribution to a state-financed non-state actors' attack

The *Nicaragua* judgment is extremely interesting with regards to the cyber domain – its considerations of different types of US 'support' of various actors in Nicaragua are directly relevant for considering state sponsorship of non-state actors' cyberattacks. In the judges' opinion, "arming and training" of individuals by a state is a breach of the law, but being funded by this state does not. According to the text of the judgment, "the mere supply of funds (…), while undoubtedly an act of intervention in the internal affairs of Nicaragua (…) does not in itself amount to a use of force".[312] If the scenario from Section 2.4.2.1 is considered again, even where attribution to state A is proven, it would mean that A cannot actually be held responsible for the act of force. It would appear that if a state only financed some individuals that performed the operation crossing the *use of force* threshold, international law would not consider this state as having breached article 2(4). In other words, it seems that a state, by merely financing a group, would get away with *use of force.*

Yet force was used. Who is the responsible party then? The victim state can try to launch countermeasures against state A. But the first thing about countermeasures is asking the state to stop its unlawful activity[313] – in which case state A would simply respond that they merely financed the group who performed the attack (if state A admits to this) and A is not to blame. This group is not part of the armed forces of a state, and therefore are mercenaries under the definition of article 47 of the Additional Protocol 1 to the Geneva Conventions;[314] by being such, they lack "combatant immunity for their actions".[315] According to the interpretation, article 2(4) only refers to a state using force against another state; the UN Charter does not apply to mercenaries.[316] A state-on-state attack would trigger international armed conflict. But non-state actor-on-state would not.[317]

[312] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement (1986)* para 228.
[313] Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack'.
[314] International Commitee of the Red Cross, *Protocol Additional to the Geneva Conventions* (1949).
[315] Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare* 105.
[316] Wolfrum, *The Max Planck encyclopedia of public international law* 612.
[317] Dieter Fleck (ed) *The handbook of international humanitarian law* (2nd edn, OUP 2008) 46.

So how would state C respond if a state cannot act in self-defence against private individuals?[318] If the state cannot be held responsible for the operation, would the non-state actor be the actual perpetrator then? The *Nicaragua* judgment reads that a state's "participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, (…), for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. (…) Such acts could well be committed by members of the contras without the control of the" United States.[319]

Therefore, if law of the armed conflict cannot be applied, the other option is to apply international criminal law.

Until quite recently, no individual could be personally responsible for violating international norms.[320] Doctrine has seen a significant evolution over the last decades regarding the possibility of an individual to be brought to an international court because they committed internationally wrongful acts: the first (and failed) ideas of making people responsible for their international crimes emerged after the end of First World War.[321] These ideas re-emerged again, this time to a successful end, with the establishment of the Nuremberg and Tokyo Tribunals after the end of Second World War, followed by the ad hoc Tribunals for the Former Yugoslavia and Ruanda.[322] But the "major breakthrough in the effective enforcement of international criminal law" came much later, in the 1998, when the International Criminal Court was founded.[323] Article 5 of the Rome Statute enlists war crimes as covered by the Courts prerogatives.[324] Article 8 reads "The Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes".[325]

[318] Wolfrum, *The Max Planck encyclopedia of public international law* 614.
[319] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement (1986)* para 115.
[320] Armstrong, Farrell and Lambert 195.
[321] Antonio Cassese, Paola Gaeta and John R. W. D. Jones (eds), *The Rome statute of the international criminal court: a commentary*, vol 1A (OUP 2002) 4.
[322] Ibid 3.
[323] Ibid 3.
[324] International Criminal Court, *Rome Statute of the International Criminal Court* (1998).
[325] Ibid.

Although cyberattacks do not make the long list of war crimes under the same article, some of the violations, such as "(i) [w]ilful killing" or "(iv) [e]xtensive destruction and appropriation of property", would fit the description of *use of force* in cyberspace[326]. Therefore, a non-state actor – an individual or a group of individuals – by committing a cyber *use of force* after receiving funds from state A, can be held responsible for committing war crimes. All the same, by law, state A that gave them financial support, would be exonerated of legal responsibility.

2.4.3. Cyberterrorism

Cyber terrorism is "ideologically motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organization".[327]

As discussed in Section 2.1., the emergence of global terrorism is one of the reasons the legal term *use of force* has changed and extended its meaning. Back in 2007 Brenner observed that the debate on whether cyber terrorism was "a myth or an inevitability" was ongoing.[328] In fact the UK's Terrorism Act 2000 defines the use or threat of action which "is designed seriously to interfere with or seriously to disrupt an electronic system" as terrorism.[329] The US' Patriot Act, adopted post-9/11, included hacking, cracking, extortion fraud and malware into the definition of "federal crime of terrorism".[330] Cyber terrorism, however, never took off as an international cyber threat. One of the reasons could be that it was never clearly agreed whether *any* "ideologically motivated" act would qualify as a cyber terrorism attack, or whether *any* cyberattack performed by a non-state organisation operating across multiple states would qualify as such. Logically, the latter would make more sense. Whilst major attacks of such type have not

[326] Ibid.
[327] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *National Strategic Framework for Cyberspace Security* 13.
[328] Brenner 714.
[329] UK Terrorism Act 2000 S1 (2) (e).
[330] US Patriot Act Section 233 b.

yet materialised, low-level cyberterrorism has been detected[331] and it was feared that the so-called Islamic State was working on developing sophisticated cyber capabilities back in 2017.[332]

A statement was issued in 2015 when the UN's GGE confirmed the increasing risk of terrorist groups and malicious non-state actors with regards to cyberspace,[333] urging better communication and mutual assistance in order to successfully prosecute the terrorist use of ICTs.[334] Performing a cyberattack does not require massive amounts of money or equipment, no weaponry or an army – therefore it is crucial to decide what a lawful response to a cyberterrorist attack would be before an actual cyberterrorist attack has occurred.

2.5. Conclusion

In cyberspace there is no status quo. This Chapter has demonstrated how in the space of ten-fifteen years, legal doctrine as well as scholarly views on cyber activities have changed profoundly. Yet there has been no unanimous agreement on the applicability of international law principles and as a consequence, no agreement on whether – and if yes – which – principles of international law have been breached by cyber activity.

Another question that remains unanswered is defining the spectrum of cyberattacks. But the lack of definitions, the lack of constraining norms and the ambiguity surrounding cyber operations is only giving technologically developed states the possibility to test their cyber capacities without repercussions.

It is in this reality that the EU has been trying to emerge as an important actor and regulator in cybersecurity. The next Chapter III will explore the way the EU developed its collective cybersecuritisation agenda.

---

[331] 'Warnings over growing IS cyber-threat' (*BBC News*, 3 June 2015) <www.bbc.co.uk/news/technology-32982609> accessed 21 January 2017.
[332] Oliver Wright, 'Isis plotting cyber warfare to kill people in UK, claims George Osborne' (*The Independent*, 17 November 2015) <www.independent.co.uk/news/uk/politics/paris-terror-attack-uk-government-to-invest-2bn-in-cyber-force-to-combat-online-terror-threats-a6737071.html> accessed 21 January 2017.
[333] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* para 7.
[334] Ibid para 13 (d).

Chapter III: The EU *vs* its Member States or the EU *and* its Member States: the challenging road to developing cybersecurity legislation

3.1. Introduction

The European Union's (EU) cybersecurity legal framework has become increasingly important in recent years. As seen in Section 2.1, it was back in the 1990s that information and communication technologies (ICT) first raised concerns for decision-makers and, in the years to follow, EU officials were prompted to potentially consider an EU-level approach to the new threats connected to these technologies. The EU's primary concern at the time was the economic aspect of the threats involved with cyberactivity, to which with time was added the security dimension.[335] Security matters, however, have inherently been considered "at the heart of sovereignty" by the Member States (MS).[336] The concept of sovereignty and how it can be violated in cyberspace has triggered many discussions (Section 2.2.2.1.A)i)). Hence, the EU has tried to take the leadership role in dealing with cyber threats, but its ambitions for *collective* cyber-securitisation, developed in the decades since, have not sat easily with some MS and were not developed without controversy. "[N]ational security remains the sole responsibility of each Member State",[337] as per Article 4(2) of the Treaty on the European Union (TEU), and, as this Chapter will show, some MS have insisted this remains the status quo even as regards cyber*security*.

At present, the EU approach to the broadly encompassing topic of cybersecurity has been developing in three different sub-domains: network and information security (NIS), law enforcement and cyber diplomacy. These coincide to some extent with the three pillars identified in the EU Cybersecurity Strategy of 2013: NIS, law enforcement, and (cyber) defence.[338] The

[335] Carrapico and Farrand, 1115.
[336] Mai'a K. Davis Cross, 'An EU Homeland Security? Sovereignty vs. Supranational Order' (2007) 16:1 79, 80.
[337] Treaty on the European Union Article 4.2 The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, **national security remains the sole responsibility of each Member State** [emphasis added].
[338] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 17.

first two represent the internal cybersecurity dimension, with the NIS framework gaining ever more prominence. The third pillar, which had to develop under the Common Security and Defence Policy (CSDP) and hence represents the external dimension, has remained largely underdeveloped from a legal perspective. The pillar approach was in fact abolished with the new Cybersecurity Strategy 2020 which adopted a more holistic approach and focused on resilience, capacity building and advancing an open cyberspace.[339] Instead of cyber defence, as an alternative, cyber diplomacy has been emerging as an area of rising significance within the broader Common Foreign and Security Policy (CFSP).

This Chapter will briefly discuss securitisation theory in relation to the NIS and cyber diplomacy sub-domains, and will address the needs, benefits and effectiveness of an EU-led legal framework in these areas. It will present the background of the EU's ambitions as a regulator, before delving into the analysis of the different case studies, which will analyse with what level of success the EU has achieved its goal. Since most academic work has not focused on legal measures specifically,[340] leaving underexplored the effects of the contestation of power between the EU and its MS on the former's legislative approaches in these two areas, this Chapter will fill this gap. The focus of the analysis will therefore be on legally binding measures post-2013, with only concise outline of other, non-binding documents, adopted by the EU institutions, as they are more relevant for the development of cybersecurity as a policy area rather than the legal framework. Also, only the most relevant provisions of pre-2013 legislative measures (e.g. related to telecoms security)[341] covering some aspects of the cyber domain will be analysed briefly, as at the time of their development, the EU was not actively pursuing a cyber-strategy.

The analysis will begin in Section 3.2. with a brief overview of the broader topic of collective securitisation, continuing with a discussion on collective EU cybersecurity (Sections 3.2.1 and 3.2.1.1.). This will set up the analytical framework for the discussion that will follow. Academia

[339] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* 5.

[340] Work that have somewhat engaged with the issues include Helena Carrapico and Benjamin Farrand, ''Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers' 67 Crime, Law and Social Change 245;
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.

[341] Directive on a common regulatory framework for electronic communications networks and services (2002) (Framework Directive).

has only recently begun to explore the EU approach: cybersecurity was still viewed as an "emerging policy field" as recently as 2018, with a need for further research analysing its "multiple dimensions" flagged.[342] The body of literature has been growing fast, as this chapter will chart. The aim of this section, however, will not be to discuss conceptual lacunas on collective EU (cyber)securitisation, nor question the role of the EU as a cybersecurity actor. The analytical framework will serve as a backdrop against which the way the EU has been gradually approaching cybersecurity collectively and developing its regulatory agenda, will be evaluated.

Sections 3.3.1. through 3.3.1.3. will then provide the key contribution of this Chapter; the analysis of the vertical (MS-EU) and horizontal (MS-MS) relationships. It needs to be acknowledged that there are limitations to this analysis as very often research could not identify which precisely MS were protagonists in a particular argument, as the common denominator "MS", or the "larger" *vs* the "smaller" MS was used. Taking this into account, the Chapter will apply the theories developed in the previous Section 3.2.1 and will analyse how collective security is actually perceived by the MS in the cyber domain. The focus will be on how the divergent MS's objectives impact the supranational legislative efforts as well as whether the EU's objectives coincide with the MS's. This section will draw comparisons between the securitisation processes in the two areas of NIS and cyber diplomacy, and will illustrate the impact of the (sometimes) tense relationship MS-EU on the overall EU legislative framework.

The Chapter will look into the EU regulatory regime from two points of view: top down and bottom up. The top down approach will allow for the regulatory framework to be analysed as the final result against which the level of preparedness of the case studies will then be compared in Chapters IV to VI. The bottom up instead will look into the role of the MS as being the main drivers in the shaping of the EU regulatory agenda.

The Chapter will thus address the main research question - what has challenged, both internally and externally, the EU approach to cybersecurity, and sub-question a) on how the EU's legal approach to cybersecurity fits and interacts with the international efforts to regulate cyberspace, observed in Chapter II. The aim of the Chapter is to enable an assessment of the EU's

[342] Helena Carrapico and André Barrinha, 'European Union cyber security as an emerging research and policy field' (2018) 19:3 European Politics & Society 299, 300.

harmonisation role, which will then allow for an assessment of the effectiveness of its regulatory regime in Chapters IV to VI, which will delve into the case studies.

3.2. From collective security to collective cybersecurity: a debate

Inherently seen as a responsibility of the state, over the course of the last several decades, the security domain has seen an increased role for various actors, from the private sector to international organisations.[343] At EU level, despite not everybody wanting to admit it, security was beginning to gain prominence in the mid-2000s.[344] This has prompted a growing number of scholars to analyse – some in general terms, others in relation to the EU – the concept and role of collective security. This section will hence delve into the securitisation theory and how it applies to the securitisation process of the cybersecurity field in the EU. As generally used in IR and not in legal research, securitisation theory will not be used as a theoretical framework to answer the main research question and sub-questions and is hence not going to be challenged, tested or used as a basis for the broad comparative research. The theory will merely be discussed in relation to scholarly work on the securitisation process of various fields of EU competence, to provide more context for the development of the collective *cyber*securitisation process, a field where literature is currently scarce.

Securitisation is one of the main ideas upon which the Copenhagen school of security studies was developed.[345] Buzan, Wæver and de Wilde, who are among the main representatives of the School, have associated the concept of "international security" to the "traditional" military-political aspects of security, linking it to surviving an existential threat to a designated referent object.[346] Securitisation, they argued, could be seen as a "more extreme version of

[343] 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, 266.
[344] Cross 80.
[345] Ole Wæver, 'Aberystwyth, Paris, Copenhagen. The Europeanness of new "schools" of security theory in an American field1' in Arlene Tickner and David L. Blaney (eds), *Thinking International Relations Differently* (Taylor & Francis Group 2012).
[346] Barry Buzan, Ole Wæver and Jaap de Wilde, *Security : A New Framework for Analysis* (Lynne Rienner Publishers 1998) 21.

politicization"[347] and hence security could be a negative thing, because the issue could not have been resolved by "normal politics".[348] Webber and Sperling further argued that securitisation is defined by the outcome of shared threat perception and agreement on the response.[349] This existential threat, however, acts as a "securitising move" and does not amount to securitisation in itself: an issue becomes "securitised" when the "audience" endorses it as such.[350] If the audience does not endorse it, the issue remains only a "securitising move" and is not actually securitised.[351] The audience, however, is such if there is a referent object. The referent object could be for instance the state, but not only – the EU can also be viewed as such.[352] In which case, existential threats in the case of the EU (the "referent object"), whose MS would act as the "audience", could be for instance events posing challenges to the integration process,[353] or environmental or religious problems.[354]

Floyd's analysis has challenged the prevalent opinion in security studies that the MS – in this case – need to agree on the threat narrative and the security measures to be adopted, arguing that when no military action is involved, agreement on those two elements is not often reachable.[355] The presence of disagreement over the need for and means of securitisation, however, does not preclude organisations, such as the EU, from pursuing securitisation.[356] The focus then, she suggested, is on the *result* and not on the *debate* and potential disagreements, that might have occurred.[357] Lucarelli further argues that the *success* of securitisation depends on the cohesiveness of the MS ("audience"), as the EU ("collective entity") can only securitise an issue if the "legitimising audience" perceives it as a *collective* issue.[358]

[347] Ibid 23.
[348] Ibid 29.
[349] James Sperling and Mark Webber, 'NATO and the Ukraine crisis: Collective securitization' (2017) 2:1 European Journal of International Security 19, 27.
[350] Ibid 25.
[351] Ibid 25.
[352] Ibid 22.
[353] Ibid 22.
[354] Wæver 53.
[355] Rita Floyd, 'Collective securitisation in the EU: normative dimensions' (2019) 42:2 West European Politics 391, 393.
[356] Ibid 395.
[357] Ibid 396.
[358] Sonia Lucarelli, 'The EU as a securitising agent? Testing the model, advancing the literature' (2019) 42:2 West European Politics 413, 428.

Against this overview of securitisation theory, as will be seen in the next sections of this Chapter, malicious cyber operations could – and will - be considered "existential threats" in the context of this thesis because of their cross-border nature and, evidently, because of their (national and supranational) security-related nature, as they have allowed the EU to work on finding a solution to their rise *collectively* through the adoption of "securitising moves", slowly leading to the "securitisation" of the field.

3.2.1. Collective cybersecurity

Very scarce literature is available on the securitisation of the cybersecurity filed in the EU not only from a legal, but also IR and politics perspective. Christou, for instance, developed the concepts set out in the previous Section 3.2., applying them to cybersecurity, arguing that collective security suggests a "unidirectional model" in which policy implementation appears, following a "securitising move" endorsed by the MS.[359] Examples of such "moves" include the steps the Commission took in the aftermath of the cyberattacks against Estonia in 2007,[360] the 2013 Cybersecurity Strategy, which was the result of cumulative threats to the EU,[361] or the Network and Information Systems Directive (NIS Directive) 2016.[362] He also suggested that when certain "securitising moves" proposed by the Commission were not symmetrically implemented or saw unequal participation by the MS, "imperfect" collective securitisation occurred.[363] And while Sliwinski, in his analysis of the 2013 Strategy, claimed that the EU suffered from a "fundamental lack of collective vision" and it was more cooperation among the MS that was needed, not simply coordination of national cybersecurity strategies,[364] Christou viewed the Strategy as a sign of the rising importance – and identity – of the EU as a cybersecurity actor. While the MS did retain certain prerogatives on the matter, he argued, they

[359] George Christou, 'The collective securitisation of cyberspace in the European Union' (2019) 42:2 West European Politics 278, 295.
[360] Ibid 285.
[361] Ibid 293.
[362] Ibid 291.
[363] Ibid 286.
[364] Krzysztof Feliks Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35:3 Contemporary Security Policy 468, 469.

had clearly attributed the responsibility of collective cybersecurity to the EU.[365] This view is in line with Biscop and Andersson's analysis, according to which without a strategy, an aspiring actor can only be a "reactor".[366]

The existence of a strategy in itself, however, is not sufficient for a "reactor" to become an actor. Two elements need to be added. First, it is the implementation and enforcement of said strategy. Second, the real difference is made by the existence of a legal framework stemming from the strategy. This would add the qualification "regulator" next to "actor". The two roles, although linked, have different relevance. While the latter's direction and goals can change, the former is legally binding upon the MS and it requires more commitment from them. Also, a regulator's objective is to spot and prevent cybersecurity weak links, created by - in the case of the EU - the different levels of legislative preparedness in the MS for example. Only by having addressed those weak links can an actor such as the EU position itself as a leading regulator in cyberspace. In addition, the role of a solid regulator can be further strengthened by a constantly developing legal framework, consisting of "securitising moves": according to Buzan *et al*/Christou's arguments, all EU cybersecurity laws would then qualify as such. Since endorsing a securitising move by the audience would imply the securitisation of an issue, it can be argued that the EU has successfully securitised cybersecurity. Moreover, as per Floyd's analysis, potential disagreements on the need and means of securitisation, which have persistently existed between the MS and the EU itself while developing its cybersecurity legal framework (and will be analysed below), do not preclude that the EU indeed became a cybersecurity regulator. The "result" she focuses on is manifested in the legislative framework, which is the outcome of the negotiations between the members and the supranational body. Hence, the collective security narrative can apply not only to military aspects, but also to economic and societal activities that might be affected by malicious cyber operations (the "existential threat"). Also, collective cybersecurity can be based on resilience and diplomacy – not defence – which are the two elements at the core of the existing EU's body of law. The EU has therefore achieved its goal of becoming a collective security actor and *regulator*, even though the military aspect is not central to its legislative framework.

[365] Christou 294.
[366] Sven Biscop and Jan Joel Andersson, 'Introduction' in *The EU and the European security strategy: Forging a global Europe* (Routledge 2008) 4.

This work will therefore analyse whether the internal MS-EU dynamics and debates have led to a legal framework that stands as a manifestation of a solid and effective collective cyber-securitisation.

3.2.1.1. Collective cybersecurity: the legal framework

Initially linked to the economic prosperity, the concept of the abuse of ICT was included in various EU official documents in the early 90s.[367] The years to follow saw the realisation that ICT crimes have become a threat with broader than economic impact,[368] resulting in a "hybrid economic/security discourse".[369] These developments mirrored what was happening at international level, as observed in Sections 1.1.1. and 2.1., where the 1990s saw a raise in cyberattacks, leading to some states such as the US, Canada, the UK, Italy, Germany amending their legal frameworks to address these new types of attacks. Through a "layering process",[370] which saw the adoption of several important documents over the years,[371] the EU was also slowly, but consistently preparing the ground for developing its strategic and legal approaches to cyber threats. Yet, back in 2012, the EU Parliament's Committee on Foreign Affairs (AFET) noted that "clear and harmonised definitions" of cybersecurity and cyber defence were lacking at EU level.[372]

[367] View European Commission, *Proposal for a Council Decision in the Field of Information Security* .
European Commission, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century: White Paper* 107.
[368] Dublin European Council, *Presidency Conclusions* (13-14 December 1996) Chapter V Justic and Home Affairs para 2.;
Council of the EU, *Action Plan to Combat Organised Crime (97/C 251/01)* (15 August 1997) 1.
[369] Carrapico and Farrand 1115.
[370] Ibid 1116.
[371] E.g. European Commission, *Communication on Network and Information Security: Proposal for A European Policy Approach COM(2001)298 final*;
European Commission, *Communication on A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" {SEC(2006) 656}* ;
Council of the EU, *European Security Strategy. A secure Europe in a better world* (2009);
European Commission, *Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673 final)*;
European Commission, *A Digital Agenda for Europe* (19 May 2010);
Council of the EU, *Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"* (27 May 2011).
[372] European Parliament Committee on Foreign Affairs, *Report on Cyber Security and Defence* (17 October 2012), para G.

Thus, as a sole-standing pillar of security, *collective cybersecurity* gained prominence only in 2013 with the first EU Cybersecurity Strategy. The Strategy is regarded as "particularly representative" of the many steps the EU took towards becoming a coherent cybersecurity actor.[373] It encompassed the network and information system (NIS) pillar (the well-functioning of the internal market, e.g. an attack against a critical infrastructure (CI) sector in a member state that could potentially affect other MS too), defence (under the CSDP), and law enforcement (for online crimes).[374] It also provided definitions of 'cybersecurity' and 'cybercrime',[375] signaling that, against an international environment struggling to fine-tune definitions (seen in Sections 2.3. through 2.3.4.), the EU was beginning to take small, but decisive steps to address cyberspace's challenges.

The 2013 Strategy further acknowledged the "increase of economic espionage and state-sponsored activities",[376] and suggested that state-sponsored cyberattacks could trigger (cyber)defence mechanisms.[377] Although it also acknowledged that threats are "multifaceted" and therefore "synergies between civilian and military approaches in protecting critical cyber assets should be enhanced",[378] the proposed legislation – the NIS Directive, decoupled cyber defence and (state-sponsored) attacks against CI sectors, and linked the latter solely to their impact on economic and societal activities. This is why its legal basis is Article 114 TFEU,[379]

[373] Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55:6 JCMS 1254, 1260.

[374] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 17.

[375] Ibid 3. Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.
Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

[376] Ibid 3.

[377] Ibid 19.

[378] Ibid 11.

[379] Treaty on the Functioning of the EU Article 114 1. Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of the objectives set out in Article 26. The European Parliament and the Council shall (…) adopt the measures for the **approximation of the provisions** laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market. (…) [emphasis added].

and not Article 83(1) TFEU[380] (which is the legal basis of, for instance, the Directive on Attacks against Information Systems 2013, tackling the criminalisation of illegal system and data interference, illegal interception and illegal access to information systems), and has the well-functioning of the internal market at its core. The NIS Directive thus has a rather different aim from security and defence, which is interesting, as when the proposal came out, the international environment was still largely focusing the possibility of cyber war (as seen in Section 2.2.2.1.). The NIS Directive, adopted in 2016, became not only the first ever EU law regulating cybersecurity for the CI sectors, but because it was legally-binding, it became a "securitising move" even more important than the Strategy, as it was the first step towards the EU becoming a cybersecurity regulator.[381] It also signaled that the EU was focusing on developing a regulatory approach to cyberattacks fit for its own unique case, rather than following what was happening at the international level.

Since 2016, the cybersecurity strategic and legal frameworks put some flesh on the bones, adding more "securitising moves". These include the Cybersecurity Act 2019 (a Regulation), the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) 2021, the Cybersecurity Strategy 2020, the NIS2 Directive 2022, the upcoming Cyber Resilience Act. The EU has therefore become the only supranational organisation in the world that has approached the vulnerability of CI sectors with a legislative, rather than a voluntary approach, further consolidating its ambitions for pursuing collective cybersecurity. There are other sectorial pieces of legislation also shaping the EU legal approach to cybersecurity, such as the General Data Protection Regulation (GDPR) 2016, the European Electronic Communications Code (EECC) 2018, the upcoming Artificial Intelligence

[380] Ibid Article 83 1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension (…)
These areas of crime are the following: (…) **computer crime** and organised crime. (…) [emphasis added]

[381] There are pre-2013 legislative steps in the domain, which will not be analysed in detail as their relevance is not central to this paper, but deserve mentioning as they would later become the very grounds upon which the post-2013 legal framework was built. These include the Framework Directive on electronic communications networks and services 2002, the Council Framework Decision 2005 on attacks against information systems and the Regulation establishing the European Network and Information Security Agency (ENISA) 2004. The former is important, as it provides the very definition of "electronic communications networks" (Article 2 *Definitions*) which is one of the types of "network and information systems" identified in the NIS Directive. The latter, instead, established and defined the initial tasks (Article 3 *Tasks*) of what would later become known as the "EU Cybersecurity Agency". At the time of adoption, "citizens, consumers, enterprises and public sector organisations of the European Union" (Article 1.1) were within the scope of the Regulation, and not specifically – of exclusively - CI sectors.

(AI) Act, and the Delegated Regulation of the Radio Equipment Directive 2022, among others, which will not be analysed in detail, as their relevance is not central to this thesis. All these "securitising moves", however, have been developing under the NIS pillar and therefore relate to the "internal" dimension of the EU cybersecurity regulatory regime.

The "external" dimension has been developing as a separate framework: as part of the foreign policy domain, the EU has also been developing its cyber diplomacy approach, through the adoption of the Cybersecurity Diplomacy Toolbox in 2017 via Draft Council Conclusions, another potential "securitising move" of significant importance, shaping the EU's regulatory agenda for cybersecurity. Despite its ambitious beginning, however, cyber diplomacy has not grown substantially in the last few years. Its analysis, however, is still of key importance, as it provides the full picture of tools available to the EU in case of state-sponsored attacks on EU soil.

Against this background, the following section will discuss how the MS have perceived the EU-led regulatory approach to cybersecurity and what the EU's road to becoming a cybersecurity regulator has been.

3.3. The EU *vs* its MS or the EU *and* its MS: a cybersecurity dilemma

Analysing the benefits of an EU-led approach on the topic, research has not focused enough on the impact the divergent security objectives of the single MS (including their representatives in the Council and the European Parliament, as well as the national cyber agencies) have had on the development of the EU legal framework, leaving the issue of the different MS's roles underexplored. Scholarly work in the field, explored below, has identified the difficult relationship between the MS and the EU, but the angle of research has mostly been on the political and policy side, with the impact of this relationship on the legislative framework remaining under-investigated. Further, literature on individual MS[382] has focused mainly on their

[382] E.g. Scott Romaniuk and Mary Manjikian, *Routledge Companion to Global Cyber-Security Strategy* (2020); Sergei Boeke, 'National cyber crisis management: Different European approaches' (2017) 31 Governance 449.

internal dynamics and developments of national regulatory and policy approaches and not so much on their role in shaping the EU's framework.

Scholarship has argued that the emergence of the EU as a security actor as a solution to the malicious cross-border cyber activity, with it challenging the MS's reign over the security domain, is logical and effective;[383] some have argued that the EU can be much more than "a cipher for member state preferences".[384] If not addressed properly, cybercrime would "severely hinder" the EU's economic growth plans.[385] But while the Commission has been pushing for more integration in the cybersecurity legislative field, the emergence as a strong security regulator for the EU has been challenged by some of its own MS and their respective representatives (alongside the major state actors in the field such as China, the US and Russia).[386] Despite only thirteen out of 28 MS had a cybersecurity strategy back in 2013 when the first EU Strategy came out,[387] MS did not initially see the need for an EU-level intervention and have persistently resisted an EU having "a more stringent control over their cyber activities", limiting thereby its "coherence in the field".[388] Bendiek *et al* in fact warned that larger MS could potentially complicate the development of an EU-led approach because of national interests and solutions,[389] and therefore MS-level efforts ought to be abandoned.[390] They further argued that "all stakeholders" should embrace more EU legislation strengthening cyber resilience.[391]

In addition, back in 2015, Christou identified the MS's preparedness levels as "perhaps the most important dimension of the cybersecurity ecosystem", with at least some minimum standards needing to be met. Failing to do so could hinder "achieving an effective EU cybersecurity

[383] Carrapico and Barrinha 299.
[384] James Sperling and Mark Webber, 'The European Union: security governance and collective securitisation' (2019) 42:2 West European Politics 228, 253.
[385] George Christou, 'The challenges of cybercrime governance in the European Union' [Routledge] 19 European Politics and Society 355, 355.
[386] Carrapico and Barrinha 301.
[387] European Parliament, *Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (12 September 2013) para G.
[388] Carrapico and Barrinha 1268.
[389] Annegret Bendiek, Raphael Bossong and Matthias Schulze, 'The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges' (2017, November) Stiftung Wissenschaft und Politik (SWP) - German Institute for International and Security Affairs 1, 3.
[390] Ibid 1.
[391] Ibid 4.

strategy".[392] It would also hinder the development of an effective body of law, which certainly would have affected the EU more than if only the strategic approach was weakened; indeed, MS's roles, objectives, preparedness, and actions as regards cybersecurity and cyberattacks are at the core of developing the supranational-level approach. Those elements, as Chapters IV through VI will demonstrate, have varied significantly across the MS – not only because of different security interests, but also socio-cultural and political differences. If, then, collective cybersecurity can only be achieved in practice if endorsed and implemented by *all* MS, as per Buzan *et al*'s theory, the difficulties in achieving it are inevitable.

Thus, as Section 3.3.1. will show, the need for EU-wide cyber laws has always been met with caution – and even pushed back against at times - by some MS. An EU legal framework would have affected better prepared states disproportionately as it would have led to conceding some powers to the EU, an avenue that would have hardly been their chosen one to explore. Consequently, some MS's sovereignty and national security concerns led to disagreements with the EU and its desire to achieve autonomous action in the field. As Barrinha and Renard observed, cooperation in cyberspace is a "choice, not a given".[393] And the choice of MS cooperating in cyberspace has never come easy to some of them.

The following Sections 3.3.1.2. through 3.3.1.3. will therefore analyse the most contentious issues amongst the MS – which include information sharing, the scope of the framework, the actual powers given to the EU and the European Union Agency for Cybersecurity (ENISA)[394], among others – which arose during the development of the EU's legal framework. Most of these issues date back to the process surrounding the adoption of the NIS Directive, which caused the most – and longest – discussions, precisely due to divergent perceptions of how cybersecurity should be addressed at EU level and what powers the EU should have. Since then, other pieces of legislation such as the Cybersecurity Act and the NIS2 Directive, while raising some disagreements, have generally seen more approval and a more streamlined process of adoption from the MS, demonstrating that the EU is gaining a clearer and more accepted role as a

[392] George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* (Palgrave Macmillan 2016) 62.
[393] André Barrinha and Thomas Renard, 'Cyber-diplomacy: the making of an international society in the digital age' (2017) 3:4-5 Global Affairs 353, 357.
[394] As seen in footnote 382, ENISA stands for European Network and Information Security Agency. The acronym was never officially changed, but the Agency is now commonly known as "the EU Cybersecurity Agency".

regulator by its MS. This does not mean, however, that the different views between the EU and the MS have been fully overcome; it merely signals an improvement as regards to EU leadership in the field of cybersecurity regulation.

3.3.1. The rise of the NIS legal framework

3.3.1.1. The NIS legislative measures

This section will be divided into two main parts, the first providing an overview of the NIS framework's main legislative steppingstones. This is needed to provide context for the second part, which will backtrack a bit and will analyse the key moments that have led to the shaping of said measures. Sections 3.3.1.1. A) to C) will thus address the general direction of the NIS regulatory regime and will look into it top down: what EU measures were adopted and what was expected from the MS to be implemented afterwards. Sections 3.3.1.2. through 3.3.1.3. will use a bottom up analysis, namely how the MS shaped said key legislative measures.

A) The NIS Directive 2016

Labelled "a true game changer for cybersecurity resilience and cooperation in Europe",[395] the NIS Directive aimed at achieving a high common level of cybersecurity across the MS, to fill the gaps and harmonise existent legislative approaches. The transposition deadline was 9 May 2018.[396] Out of the three case studies, only the UK transposed it on time: the NIS Regulations 2018 came into force on the 10 May 2018, the Italian Legislative decree 65/2018 – on 24 June 2018 and the Bulgarian Cybersecurity Act – on 7 November 2018 (these will be discussed in detail in Sections 4.2.4. through 4.2.5., Sections 5.4. through 5.4.3., and Sections 6.3. through

[395] European Commission, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union* (13 September 2017) 2.
[396] Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive 2016) Article 25 (1).

6.3.4. respectively). This already gave the first signals of the levels of preparedness (which will be addressed in Chapters IV through VI).

Before delving into the cybersecurity-related requirements of the NIS Directive, it is essential to provide some definitions. 'Network and information systems' have been identified as "an electronic communications network within the meaning of point (a) of Article 2" of the Framework Directive on a common regulatory framework for electronic communications networks and services (Framework Directive) of 2002.[397] The later has defined 'electronic communications network' as:

> transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

This makes the Framework Directive 2002 of crucial importance for the development of cybersecurity legislation as regulating the telecoms sector has provided the basis upon which the regulation of the CI sectors in the NIS Directive's scope has been built.

The Directive aimed at achieving the high common level of cybersecurity (or security of network and information systems, as per the Directive's official text) in the MS through a number of key targets: each member state should have had the "minimum capabilities and a strategy ensuring a high level of security"[398] of the network and information systems, as well as a well-functioning computer security incident response teams (CSIRTs).[399] A CSIRT Network was also created with the aim of developing "confidence and trust" between the MS.[400] Each member state should have designated a national competent authority (NCA) to monitor the application of the Directive,[401] and a single point of contact (SPOC) to ensure the cross-border cooperation

[397] Ibid Article 2 (1) (a).
[398] Ibid Recital (4) and Article 7.
[399] Ibid Article 9.
[400] Ibid Article 12 1.
[401] Ibid Article 8 1. and 2.

between the MS's authorities.[402] A cooperation group was set up "to support and facilitate strategic cooperation and exchange of information".[403] MS had to also identify the "operators of essential services"[404] (OES) – public or private companies operating in their respective territories and proving services to the critical infrastructure (CI) sectors (energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure)",[405] and "digital service providers" (DSP) (online marketplaces, online search engines and cloud computing services).[406] (It is to be noted that the telecoms sector was excluded from the scope despite its obvious relevance. This is simply because it was already regulated by the Framework Directive 2002). OES and DSP had to adopt the "appropriate and proportionate technical and organisational" risk management measures[407] and to ensure a notification "without undue delay" of incidents, having a significant impact on their services.[408] To avoid repetition, these requirements will be unpacked in detail in Chapters IV to VI to compare and demonstrate how the EU measures were interpreted and implemented in the three MS, and how they interacted with already existing measures in the MS.

B) The Cybersecurity Act 2019

The Cybersecurity Act, a Regulation, was the second very important step in the EU NIS framework. It gave a permanent mandate to ENISA[409] and established the framework for European cybersecurity certification schemes for ICT products, services and processes.[410] As regards ENISA, from a support agency it became an operational body with technical capabilities: its new tasks included facilitating operational cooperation among the MS, providing support to the MS which request assistance with the assessment of cyber incidents, providing technical

[402] Ibid Article 8 3. and 4.
[403] Ibid Article 11.
[404] Ibid Article 5.
[405] Ibid Annex II.
[406] Ibid Annex III.
[407] Ibid Articles 14 1. for OES and 16 1. for DSP.
[408] Ibid Articles 14 3. for OES and 16 3. For DSP.
[409] Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (2019) (Cybersecurity Act) Article 1 a) and Title II.
[410] Ibid Article 1 b).

handling of the incidents, supporting information sharing and technical solutions - on a voluntary basis – between the MS, and supporting the cooperative response to large-scale cross-border cyberattacks and crises.[411] As regards the certification framework, the latter aimed at supporting businesses in the EU with having to certify their ICT products, processes and services only once and see their certificates recognised across the EU.[412]

The Cybersecurity Act also adopted a much more streamlined definition of cybersecurity compared to the one found in the 2013 Cybersecurity Strategy (see Section 3.2.1.). Cybersecurity was thus defined as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".[413] Whilst the two definitions are similar in content, they reflect the different perceptions of dealing with cybersecurity in 2013 and 2019. The 2013 definition focuses on protection in the "civilian and military fields" thereby reflecting the general attitude towards interpreting cybersecurity as the fifth domain of war at the time (addressed in detail in Section 2.2.2.1.). The 2019 definition instead has omitted the reference to the military field, thereby reflecting the changes in the focus of the regulatory debates (away from the imminent arrival of cyber war and what laws apply to it, as seen in Section 2.2.2.2.).

C) The NIS2 Directive 2022

The NIS2 Directive was adopted in 2022. It built upon NIS1, but it also significantly expanded its scope. The terminology developed in the 2016 version, namely OES and DSP was abolished and instead two categories of entities were introduced – essential and important[414] – operating in the 'sectors of high criticality' and 'other critical sectors' respectively.[415] The expanded scope therefore included space, ICT services management, public administrations and waste water as

[411] Ibid Articles 5, 6 and 7.
[412] Ibid Title III.
[413] Ibid Article 2 1.
[414] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) Article 3.
[415] Ibid Annex I Sectors of high criticality and Annex II Other Critical Sectors.

'sectors of high criticality',[416] and research, food, chemicals, manufacturing, waste management and postal services as 'other critical sectors'.[417]

The NIS2 Directive officially established also the European cyber crisis liaison organisation network (EU-CyCLONe) for the "coordinated management of large-scale cybersecurity incidents and crises at operational level".[418] It also created a European vulnerability database, to be developed and maintained by ENISA,[419] and encouraged MS to introduce new rules for tackling supply chain attacks in their respective Cybersecurity Strategies.[420]

In terms of incident reporting, NIS2 was much clearer in terms of the timelines, giving entities 72 timeframe to report incidents (as will be seen in Chapters IV through VI there were huge discrepancies between the MS and how they identified the "without undue delay" under the NIS Directive 2016).

3.3.1.2. The NIS legal framework – the back story

A) Hard law *vs* voluntary approach

i) NIS Directive 2016

Even though, according to the Impact Assessment of the NIS Directive, uneven capabilities preparedness among the MS and lack of information sharing on incidents, risks and threats were identified as "drivers of the problem",[421] with the "problem" being "insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market",[422] in their very first reaction to the document, after the debate in the Council, the MS invited the Commission to provide further justification why these "drivers" were addressed with a hard law, rather than a voluntary

[416] Ibid Annex I.
[417] Ibid Annex II.
[418] Ibid Article 16 1.
[419] Ibid Article 12.
[420] Ibid Article 7 2 (a).
[421] European Commission, *Staff Working Document; Impact Assessment on the NIS Directive {COM(2013) 48 final} {SWD(2013) 32 final}* (February 2013) 3.
[422] Ibid 2.

approach.[423] The Council position was indicative as to how much some MS did not view an EU-led approach on cybersecurity the same way the EU did itself. It also presented the prevailing sentiments and revealed a potential tension between the MS and the EU, as the former were clearly questioning the latter's legal advancements in this security domain.

Follow-up discussions led to the first diverse views among the MS: some pushed for a flexible approach, while others insisted on a fully binding approach for all sectors (public administrations or market operators[424]), in line with the Commission proposal.[425] Striking a balance between these different views was seen as the "main challenge" for achieving a similar level of preparedness among the then 28 MS.[426] Here one member state stands out as leading the opposition: the UK was among those states pushing for a "hands-off" approach, as opposed to the Commission's "hands-on" approach, in a push for demonstrating its "leadership in cybersecurity within the EU".[427] The UK feared that the EU was advancing in an area historically seen as a national concern. Having the UK "lead" the EU cybersecurity approach would have entailed the MS assuming a dominant position in terms of policy setting, with the *support* of the EU, and not *vice versa*. Therefore, the EU's first tentative securitising move – the 2013 Strategy – clearly had not convinced some of the MS of the benefits of collective cybersecurity. These countervailing pressures meant that although the process of collective EU cyber-securitisation had begun taking shape in 2013, its first tangible result came only in 2016, when the NIS Directive was adopted.

[423] European Parliament Legislative Observatory, 'High common level of network and information security across the Union. NIS Directive 2013/0027(COD) (Summary of debate in Council)' (6 June 2013) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1274749&t=e&l=en> accessed 28 December 2023.

[424] NIS Directive Proposal Article 3 (8) "market operator" means:
(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;
(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.

[425] European Parliament Legislative Observatory, 'High common level of network and information security across the Union. NIS Directive 2013/0027(COD) (Summary of debate in Council)' (*Legislative Observatory*, 5 December 2013) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1327607&t=e&l=en> accessed 28 December 2023.

[426] Ibid.

[427] Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* 80.

B) Sensitive information sharing: building trust

i) NIS Directive 2016

While forming the legislative framework, and especially while shaping the first concrete legislative steps, contentious issues included sharing sensitive information about security breaches in the CI sectors, the assessment of risks, threat intelligence and coordinating response to attacks.[428] Also here contrasting views were multilayered: tackling those issues in an efficient manner in order to achieve a good law saw disagreements not only between national delegations, but also between the EU and the MS.

It was acknowledged already in 2013 in the NIS proposal that "trust among peers […] is a prerequisite for […] information sharing", but at the time, there was "cooperation only among a minority of Member States" with advanced capabilities,[429] which were "less willing" to share information with the smaller ones.[430] Reporting and sharing information was not a natural process for all MS.[431] For instance, signalling a rift from the Commission's approach, the Czech Republic expressed concern with the "rather extensive" powers given to the Commission in the NIS proposal,[432] as regards the criteria to be met by the MS in order to be "authorized to participate to the secure information-sharing system".[433] Further, British MEPs expressed "concern", linking mandatory reporting of incidents and information-sharing to a "tick-box approach"[434] and highlighted the need for a "change of culture" in the MS if trust issues were to be overcome.[435] French MEPs further called out the "dogmatic" approach taken in relation to coordinating responses to incidents, in contrast with Bulgarian representatives, who argued that

[428] Catherine Stupp, 'Commission wants member states to trust each other more on cybersecurity' (*EURACTIV*, 26 April 2016) <https://www.euractiv.com/section/digital/news/commission-wants-member-states-to-trust-each-other-more-on-cybersecurity/> accessed 23 December 2023.
[429] NIS Directive Proposal Explanatory Memorandum 3.
[430] Stupp.
[431] Carrapico and Barrinha 1264.
[432] The Senate of the Parliament of the Czech Republic, *Resolution of the Senate on the Proposal for NIS Directive* (16 May 2013) Para 4.
[433] NIS Directive Proposal Article 9 2. and 3.
[434] European Parliament, 'Speech by Vicky Ford on High common level of network and information security (debate)' (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 6 January 2024.
[435] European Parliament, 'Speeches by Vicky Ford and Malcolm Harbour on High common level of network and information security (debate)' (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 6 January 2024.

"high coordination" is the "key for fostering a secure, innovative and tech-savvy Europe".[436] As Christou summarises, it was the states with high level of preparedness that pushed for a voluntary approach on critical issues such as information sharing and the less advanced – for a mandatory one.[437] Supposedly though, if no state apparatus in the smaller states was in place to receive, handle or use sensitive information, sharing it would have likely caused more damage. The case studies analysed in the Chapters IV through VI will demonstrate that differing security capabilities – as well as different political preferences – were a significant cause of incompatible MS priorities.[438] This, in itself, highlights the need for the EU to regulate in areas of cross-border security relevance where weak links were evident. Also, the reality of not sharing information, or sharing it on a voluntary basis, meant consolidating the lack of trust among the MS, reinforcing the cracks in their preparedness, resulting in deepening the fragmented strategic and legislative approaches. This explains why the Commission's proposal advanced the concept of "Secure information-sharing system" in the NIS proposal – an attempt to iron out differences that was (unsurprisingly) shot down by the MS.

The final version of the NIS Directive hence saw the practice of exchanging incidents information and providing support in cross-border incidents to be done on a voluntary basis,[439] despite being deemed insufficient in addressing the growing vulnerability of the CI sectors.[440] The Commission echoed scholarly views, stating that the adopted version of the Directive was "a lot weaker" than the proposal.[441]

[436] European Parliament, 'Speeches by Mylène Troszczynski and Eva Paunova on High common level of security of network and information systems across the Union (debate)' (5 July 2016) <https://www.europarl.europa.eu/doceo/document/CRE-8-2016-07-05-ITM-013_EN.html> accessed 6 January 2024.
[437] Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* 183.
[438] Barrinha and Renard 1265.
[439] NIS Directive 2016 Articles 12. 3. (c) and (e).
[440] Bendiek, Bossong and Schulze 2.
[441] Stupp.

ii) NIS2 Directive 2022

As it was insufficient to fully tackle the cross-border nature of cyberattacks, with trust issues continuing to be seen as an obstacle to better integration,[442] the EU soon proposed addressing the shortcomings in the NIS Directive by adopting a new "securitising move" – the NIS2 Directive proposal. Commission officials admitted that among the big withstanding issues post-NIS Directive were incident reporting and threat intelligence sharing, and acknowledged that trust was still lacking eight years after the first NIS proposal came to light, eight years being an "eternity" in cybersecurity.[443] This was further reflected in the NIS2 Directive Impact Assessment, which stated that although, tendentiously, there was more trust, information sharing was still limited and MS did not do it "systematically".[444] ENISA's executive director Lepassar further stated that MS's unwillingness to share information – for example in 2021 no cross-border incidents were reported – hindered ENISA's ability to improve the level of the EU's cybersecurity.[445] Nonetheless, the EU position was once again pushed back against by MS representatives, with Dutch MEP Groothuis arguing that reporting of both potential incident and potential cyber threats should not be mandatory because it would be burdensome and ineffective.[446] Generally speaking, however, debates[447] were much more streamlined as it took two years from the proposal stage to the final product (as opposed to more than 3 years for NIS1) and their focus was not to question the role of the EU. One of the reasons, arguably, was that the UK – one of the main challengers of the EU being the cybersecurity locomotive – had left the EU in 2020. Another could be that, despite some persisting issues as abovementioned, MS had come into terms with the EU leadership position.

---

[442] European Commission, *Staff Working Document; Impact Assessment on the NIS2 Directive {COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final} Part 1/3* (16 December 2020) 15.
[443] 'Cybersecurity – the Heart of the EU Security. Interview with Despina Spanou' 7:1 European Cybersecurity Journal 12.
[444] European Commission, *Staff Working Document; Impact Assessment on the NIS2 Directive {COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final} Part 1/3* 15.
[445] Laura Kabelka, 'EU's cyber incident reporting mechanism does not work, agency chief warns' (*EURACTIV*, 27 April 2022) <https://www.euractiv.com/section/cybersecurity/news/eus-cyber-incident-reporting-mechanism-does-not-work-agency-chief-warns/> accessed 28 December 2023.
[446] European Parliament Committee on Industry Research and Energy, *Draft Report on the Proposal for NIS2 Directive* (3 May 2021) 57.
[447] European Parliament, *Report on the 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* (4 November 2021).

C) Scope of the laws: national *vs* EU-level cybersecurity

i) NIS Directive 2016

Another critical issue that saw a power battle between the national and EU officials was the scope of the various pieces of cybersecurity legislation.[448] Also on this matter, the bigger states pushed for a weaker EU approach that would not have interfered majorly with their own national approaches. On the topic, Bendiek *et al* labeled "wishful thinking" the potential Commission attempts to integrate in its approach advanced national approaches.[449]

This issue again experienced the UK as leading the opposition: it successfully argued against the inclusion of providers of information society services[450] in the NIS Directive.[451] Germany, on the other hand, successfully achieved the exclusion of public administrations of the scope,[452] even though Bulgarian MEP Kalfin argued against such a step.[453] The Commission also expressed views that excluding these two sectors was risky and it was very important to get the scope of the Directive right.[454] Having a broader scope, however, proved to be impossible to achieve: as Italian MEP Danti pointed out in 2016, the "selfishness and reluctance" of many MS to cede powers to the EU has meant a less ambitious legal text.[455]

[448] European Parliament Legislative Observatory, 'High common level of network and information security across the Union. NIS Directive 2013/0027(COD) (Summary of debate in Council)'.
[449] Bendiek, Bossong and Schulze 4.
[450] NIS Directive Proposal Annex II List of market operators: 1. e-commerce platforms; 2. Internet payment gateways; 3. Social networks; 4. Search engines; 5. Cloud computing services; 6. Application stores.
The final version of the NIS Directive, Annex III, Types of digital services, includes: 1. Online marketplace; 2. Online search engine; 3. Cloud computing service.
[451] Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* 80.
[452] Ibid 133.
[453] European Parliament, 'Speech by Ivailo Kalfin on High common level of network and information security (debate)' (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-INT-3-904-000_EN.html?redirect> accessed 15 January 2024.
[454] European Parliament, 'Speech by Neelie Kroes on High common level of network and information security (debate)' (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 15 January 2024.
[455]European Parliament, 'Speech by Nicola Danti on High common level of security of network and information systems across the Union (debate)' (5 July 2016) <https://www.europarl.europa.eu/doceo/document/CRE-8-2016-07-05-ITM-013_EN.html> accessed 15 January 2024.

ii) The Cybersecurity Act 2019

The scope of the EU's proposals was again seen as problematic when the Commission proposed the Cybersecurity Act 2019 (see Section 3.3.1.1.B)), especially the first part on the role and powers of ENISA: here, the protagonists were Germany and France. The UK was already negotiating its way out of the EU, but had there been no Brexit, the UK would have likely been among those MS challenging the EU again.[456] Even though the Commission representatives stated that "there is definitely an overwhelming support both from MS and the private sector for actually a strong ENISA (…) to grow",[457] France and Germany's information systems security agencies' (ANSSI and BSI respectively) bosses, Guillaume Poupard and Arne Schönbohm, strongly argued against taking the backseat in ENISA-overseen cybersecurity certification schemes for ICT products, stating that they were forced to take a "step back into the past".[458] Even though the certification schemes were introduced as voluntary in the proposal (and remained such after the adoption of the law), this was another example of how the institutional EU-led approach was challenged by the reality of individual MS which wanted to lead the way, rather than EU institutions like ENISA (in that particular case). Comparing BSI and ANSSI with the EU Cybersecurity Agency, Poupard argued the latter had no manpower or experience to perform its new tasks.[459] This is true as, at the time of discussions – spring of 2018 - it was revealed that, prior to its enlargement, ENISA had around 80 people staff, compared with around 600 in ANSSI and around 900 in BSI.[460] Schönbohm further stated that the Cybersecurity Act proposal was inefficient and that "the European Commission is not a spaceship that can do what it likes to do".[461] These MS, hence, kept insisting the role and powers of ENISA to be downplayed. Opposition again came from a representative of a smaller MS – Bulgarian MEP

[456] Back in 2004, after ENISA Regulation was adopted, the UK appealed to the EU Court of Justice (Case C-217/04 United Kingdom vs. European Parliament and Council [2005] I-10553) claiming that ex article 95 EC (now article 114 TFEU) does not provide the right legal basis for the Regulation, arguing that the power to harmoise national laws does not mean the power to establish new Community bodies hence the ENISA Regulation provisions fall outside the scope of the article. The Grand Chamber dismissed the action and upheld the legal basis.
[457] QED, 'Speech by Jakub Boratynski at the 5th Annual QED Conference on Cybersecurity' (22 June 2017) <https://www.youtube.com/watch?v=Ayc8Jef_Rds> accessed 15 January 2024.
[458] Catherine Stupp, 'French cybersecurity chief warns against 'step back into the past'' (*EURACTIV*, 25 April 2018) <https://www.euractiv.com/section/cybersecurity/news/french-cybersecurity-chief-warns-against-step-back-into-the-past/> accessed 15 January 2024.
[459] Ibid.
[460] European Parliament, 'Speech by Peter Kouroumbashev on cybersecurity - debates in ITRE Committee' (22 March 2018) <https://www.youtube.com/watch?v=3265VcpSI14&t=3s> accessed 15 January 2024.
[461] Stupp, 'Commission should 'walk the walk' on cybersecurity, German chief says'.

Kouroumbashev – who kept calling out bigger states for their "selfishness" precisely because their national interests which seemed to be prevailing over the EU's.[462] In the end, as seen in Section 3.3.1.1.B), there was a small victory for the smaller MS as ENISA was given more operational role and attributed technical capabilities to contribute to a cooperative response to large-scale cross-border cyber incidents.

iii) The NIS2 Directive 2022

As observed in Section 3.3.1.2B)ii) during NIS2 Directive's debates MS proved to be in much more harmony compared to the NIS1 debates. In fact, as regards the scope, which caused extensive debates when NIS1 was drafted, it was acknowledged that NIS2 "**justly** widens the scope significantly" [emphasis added],[463] demonstrating that the almost ten years difference between the first and the second Directive have raised the maturity level and understanding of the cyber threats, and the importance of regulating all critical elements of the economy at EU level.

In terms of incident reporting, as seen in Section 3.3.1.1.C), the NIS2 gave a 72 timeframe to report incidents. This went against the initial Commission proposal, but not because of divergent views between the MS and the EU. It was because the initially proposed 24 hours were "unreasonable".[464] The Rapporteur pointed out that when targeted by a cyberattack first priority is to mitigate it, meaning that reporting would come only as a secondary priority.[465] Considering the NIS2 again is a Directive, thereby giving ample scope to the MS to adapt their national transposition laws to their specific views and needs, it is not a given that all MS will adhere to the 72-hours timeframe. As MS are still developing their respective transposition laws (as of summer 2023), it cannot be stated with certainty discrepancies between the MS on this issue would persist.

[462] European Parliament, 'Speech by Peter Kouroumbashev on cybersecurity - debates in ITRE Committee'.
[463] European Parliament, *Report on the 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* 126.
[464] Ibid 127.
[465] Ibid 127.

3.3.1.3. Summary

To sum, these sub-sections demonstrated empirically Buzan *et al*'s theory which differentiates between securitising moves and actual securitisation: the "moves" – legislative proposals - introduced by the Commission have seen endorsement by the MS only after they had a saying in the drafting of the legal texts. It is then the final outcome of negotiations to be considered a "securitising move" if we were to argue that the EU has achieved collective cyber-securitisation. This section has also evidenced with examples Christou's views on an imperfect collective securitisation due to asymmetrical implementation and different participation of the MS. However, the fact that there clearly is imperfect collective cyber-securitisation does not stop the EU from also claiming a clear regulator's role: the more laws ("securitising moves") the EU adopts with the green light of its MS, the stronger this role becomes.

3.3.2. The rise of the cyber diplomacy framework

As opposed to the NIS pillar body of law, cyber diplomacy has been developing within the CFSP area. Due to the nature of the area – the development of strategic foreign policy concepts does not follow the ordinary legislative procedure - research has not identified detailed sources on the divergent MS objectives as in the NIS area, but rather a more generic ones, where single MS names do not stand out.

Some 20 years ago, Hill claimed that EU external policy is "unsatisfactory and even dangerous", with a major gap between its capabilities and its unrealistic expectations in the area.[466] More recently, despite the time gap, other experts have largely echoed his words, stating that the EU foreign policy as "controversial", "largely paralyzed" and practically non-existent, with "lack of legitimacy granted" by the MS because of carefully guarded sovereignty, with national interests prevailing over a potential European one, resulting in a leadership paradox where the MS engage in informal practices allowing them to bypass the High Representative on foreign policy

[466] Christopher Hill, 'The Capability-Expectations Gap, or Conceptualizing Europe's International Role' (1993) 31:3 JCMS 305, 326.

issues.[467] The cyber diplomacy approach therefore bears the burden of the shortcomings of both of the EU foreign policy in general *and* the most developed pillar of the general cybersecurity approach – the NIS framework - as they are both rooted in the divergent MS's national interests. Some MS's unwillingness to cooperate both with the EU and with the other MS, as seen above, indicated that also developing a foreign policy and sanctions regime on cyberattacks would be a challenge.

Back in 2017, Barrinha and Renard identified cyber diplomacy as a "relatively new concept".[468] They also argued that "cyber-diplomacy is to cyberspace what diplomacy is to IR: a fundamental pillar of international society".[469] Therefore developing this area at EU level was not only important, but necessary: if the EU wanted to advance further its security actorness in cyberspace, if it wanted to be a recognised and respected factor, actor and *regulator*, having a common cyber foreign policy was essential. The latter was, however, initially seen as a "well-meant declaration of intent".[470] This view persisted, as academia did not see the EU as a major player in this cyber sub-domain even in 2018,[471] even after the adoption of the Cyber Diplomacy Toolbox in 2017, analysed below.

Hence, this sub-section will explore how the cyber-securitisation process in the foreign policy domain has developed, what the limitations of the framework are and what challenges lie ahead of it. The subsequent sections will thus refer back to the discussions in Chapter II specifically the one related to sovereignty (Section 2.2.1. and Section 2.2.2.1.i.) and attribution (Section 2.4.). By adding another element to the broader EU cybersecurity regulatory puzzle, this discussion will help draw conclusions on the overall effectiveness of the securitisation process in the cyber domain and hence the potential status of the EU of a strong cybersecurity *regulator* when considering its ambitions and legislative efforts.

---

[467] View Sliwinski 471;
Nathalie Tocci, 'On foreign policy, EU has to speak up — even if it's not with one voice' (1 October 2020) <https://www.politico.eu/article/eu-foreign-policy-vision-belarus-sanctions/> accessed 8 January 2024.
Lisbeth Aggestam and Markus Johansson, 'The Leadership Paradox in EU Foreign Policy' (2017) 55:6 JCMS 1203, 1217.
[468] Barrinha and Renard 356.
[469] Ibid 361.
[470] Annegret Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy: From Trans-formation to Resilience' (October 2017) SWP Research Paper 1, 20.
[471] Carrapico and Barrinha 301.

3.3.2.1. The EU Cyber Diplomacy Toolbox: the power of attributing cyberattacks

Before delving into the EU's cyber diplomacy approach and the first concrete step – the Cyber Diplomacy Toolbox, it is interesting to give an overview of what happened in Estonia in the aftermath of the 2007 attacks – where it *all* began - and how what happened then influenced and shaped the EU's diplomatic approach to malicious foreign-sponsored cyber operations.

The cyberattacks against Estonia played an important role in shifting the international narrative, as observed throughout Chapter II, but here they will be seen from a different angle. Estonia fell victim to state-sponsored cyberattacks and its response was diplomatic: according to the then Estonian ambassador in Moscow Marina Kaljurand, Estonia was the first country in the world to use diplomatic tools in response to cyber operations, and while attribution was "primitive" – Estonia put the Russian nationals who declared to have committed the attack into the Schengen black list – she argued that this was a "really strong diplomatic move".[472] However, it acted bilaterally, not via the EU, and "attribution is strong if done collectively".[473] At the time, however, the EU did not have a general strategic approach to cybersecurity or cyberattacks at all. The attack and Estonia's response, hence, evidenced precisely this gap in legal and strategic preparedness that an organisation such as the EU, developing its foreign and security policy, and advancing its collective security agenda, should have had.

In 2017, ten years after the Estonia attacks, the first tangible outcome in the field, the Cyber Diplomacy Toolbox, was adopted via Draft Council Conclusions.[474] The Toolbox became one of the steppingstones upon which the EU's overall cybersecurity strategic approach has been developing and has progressively become an important political instrument. In fact, the political, as opposed to military, measures that were put forward, signalled that the EU was developing its agenda in this sub-domain as a "force for peace".[475] What makes the Cyber Diplomacy Toolbox a very important political and strategic diplomatic document, however, is the power of

[472] Cyen.
[473] Ibid.
[474] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities 2017 ("Cyber Diplomacy Toolbox").
[475] Annegret Bendiek, 'The European Union's Foreign Policy Toolbox in International Cyber Diplomacy' (December 2018) 2:3 Cyber, Intelligence, and Security 57, 71.

attributing cyberattacks to states and non-state actors (the legal considerations of which at international level have been addressed in Section 2.4.).

Although important - attribution is what makes the Toolbox have "teeth" – it is also the element that undermines its very effectiveness and evidences the current limitations of the EU cyber diplomacy approach. Two interlinked issues arise here. First, according to article 24 TEU, foreign policy decisions shall be "defined and implemented by the European Council and the Council acting unanimously". Being part of the CFSP, the same rules should apply to cyber diplomacy too and so should the abovementioned shortcomings in the CFSP decision-making process where national interests regularly prevail over the EU's. Even though the benefits of changing the current voting system to qualified majority for cyber sanctions have been discussed,[476] so far nothing has changed. Hence, unanimity in cyber foreign policy, while not impossible, would be hard to achieve.

Second, attribution to a state or a non-state actor is a "sovereign political decision based on all-source intelligence",[477] something that was acknowledged also by the reviewed Cybersecurity Strategy in 2017.[478] As seen in Section 2.4.1., there have been many cases of state-level attribution to another state, also by single MS such as the UK. This section, however, highlights the shortcomings of the EU cyber diplomacy regime as regards attribution, which, once again are rooted in the MS's capabilities and preparedness. As Bendiek and Kettemann highlighted, MS have "different methods and procedures to establish a degree of certainty on attributing a malicious cyber activity" and currently there are no common standards for identifying the perpetrator of an attack.[479] Despite the reviewed 2017 Cybersecurity Strategy arguing that to facilitate attribution, "forensics capabilities need to be reinforced",[480] this has not yet been addressed, at least not officially. This means that in the case where one member state could potentially identify a cyberattack as worthy of an EU-level response, it is not improbable that other MS do not. Moreover, the EEAS's Intelligence and Analysis Centre relies on intelligence

[476] Annegret Bendiek and Matthias Schulze, 'Attribution: A Major Challenge for EU Cyber Sanctions An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW' SWP Research Paper 11 37.
[477] Cyber Diplomacy Toolbox 2017 para 4.
[478] European Commission, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (13 September 2017) 16.
[479] Annegret Bendiek and Matthias C. Kettemann, 'Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy' (February 2021) SWP 1, 4.
[480] Commission, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* 14.

gathered from the MS, and does not possess independent intelligence gathering capabilities,[481] making therefore an EU-level attribution even more dependent on the MS's resources. Since, as seen in Section 3.3.1.2.B)ii), the lack of trust in handling sensitive information among the MS persists, hurdles could also persist, leading to potential gaps in attribution at MS level. Exacerbated by the need for unanimity, this, consequently, could lead to a missed opportunity of an EU-level attribution. Because, in fact, for an EU response to be triggered, a "shared situational awareness **agreed** among the Member States" [emphasis added] is needed.[482] This could potentially indicate that should there be no shared situational awareness among the MS - an essential component of attribution[483] - an autonomous EU-level response would be unlikely even though collective measures have much more significant political impact than a single Member State one. This leads the discussion back to Sections 3.3.1.2. through 3.3.1.2.B)ii), on the lack of trust among the MS when it comes to sensitive information sharing, highlighting the similarities in the flaws of both the NIS legislative framework and the cyber diplomacy framework.

Despite these major hurdles in the decision-making process, the sanctions regime under the Toolbox was in fact used twice - in July and October 2020 respectively - issuing restrictive measures against eight foreign individuals and four foreign entities in total for having performed attacks in 2015 and 2017 such as the attack against the German Bundestag, the WannaCry ransomware and NotPetya attack[484] (whose attribution was addressed also in Section 2.4.1.). The sanctions acknowledged that those individuals were working for the Russian and North Korean governments respectively, but despite having named individuals, not the actual *state* (a joint EU diplomatic response does not require attribution to a state[485]), the attacks could not be considered "state-sponsored attacks by non-state actors", as per analysis in Sections 2.4.2. through 2.4.2.2.

---

[481] EU Intelligence Analysis Centre (EU INTCEN), 'Fact Sheet' (19 April 2012) <https://www.asktheeu.org/en/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf> accessed 30 January 2024.

[482] Cyber Diplomacy Toolbox 2017 para 5.

[483] European Parliamentary Research Service, *Understanding the EU's approach to cyber diplomacy and cyber defence* (May 2020) 9.

[484] Council of the EU, *EU imposes the first ever sanctions against cyber-attacks* (30 July 2020);
Council of the EU, *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack* (22 October 2020).

[485] Cyber Diplomacy Toolbox 2017 para 4.

In the more recent example of the SolarWinds breach (addressed also in Sections 2.3.2.1. and 2.4.1.), six out of fourteen EU institutions, agencies and bodies which use the SolarWinds product fell victim to the attack.[486] This time, however, the EU remained silent on possible attribution. It only issued a press release "expressing solidarity" with the US and stating that the "United States assesses" that the operation "has been conducted by the Russian Federation".[487] This was a missed opportunity to further advance the EU's attribution capabilities.

Here experts' views on whether attribution could act as a deterrent vary: some believe that blacklisting and banning individuals to enter the EU sends a strong political message, others believe that measuring attribution's effectiveness on deterring cyber operations is difficult.[488] Soesanto, in particular, argued that the 2020 sanctions failed to achieve their strategic aims.[489] Nonetheless, possessing the capabilities for (correctly) attributing cyberattacks is still better than not possessing them, especially at EU level – attribution might not be a deterrent today, but in cyberspace there is no status quo and things can change rapidly, leaving the unprepared behind. And while attribution might not fully discourage malicious actors to perform harmful operations, silence is more damaging, as it signals there is no unified EU voice, caused, potentially, by the shortcomings of the decision-making process (seen in Section 3.3.2.), in combination with the different capabilities of the MS that will be examined in the Chapters IV through VI.

A) Attribution: Ukraine 2022

Another attribution dilemma within the Diplomacy Toolbox could be illustrated by the ongoing Russian cyber operations on Ukrainian soil.[490] According to the Council Decisions 2019, via which the Toolbox was officially adopted, the latter could be applied even in the case of a third country being targeted by a malicious cyber operation – it does not necessarily have to be a

[486] Mr Hahn (on behalf of the European Commission).
[487] Council of the EU, *Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation* (15 April 2021).
[488] Eichensehr, 553.
[489] Stefan Soesanto, 'After a Year of Silence, Are EU Cyber Sanctions Dead?' (26 October 2021) <https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead> accessed 15 January 2024.
[490] For more details view Lewis.

member state or the EU itself that is the target and/or the victim.[491] Hence, the EU could issue restrictive measures against Russia on the basis of having targeted Ukraine. The package of sanctions adopted by the EU so far has not seen any individuals being sanctioned for having performed attacks against Ukrainian infrastructure, similarly to those sanctions adopted in July and October 2020. The EU has, however, indeed applied the Toolbox as regards state operations against Ukraine: in May 2022 it attributed the malware attacks against the satellite KA-SAT network to Russia,[492] signalling that at least when it came to Russian-led malicious operations against Ukraine, MS had less differences and the decision-making process under the CFSP did not prove an obstacle.

3.3.2.2. Summary

To sum, the adoption of the Cyber Diplomacy Toolbox was an important political move. However, the analysis shows that it is not its adoption that should be considered a "securitising move", but rather the adopted sanctions. While so far there have been just these two cases of cyber sanctions to individuals and one to a state, prompting experts to ask whether the EU sanctions regime is "dead",[493] their relevance for the development of the legal framework should not be underestimated. In the cyber diplomacy domain, it is not the existence of the framework what makes it effective and what makes the EU a regulator-leader in further defining what constitutes responsible state behaviour in cyberspace, but the use of said framework: when and how it is applied. A relatively new area with a potential to be developed further, the EU should not miss the opportunity to add more "securitising moves" if it wants to solidify its role as a cybersecurity *regulator*.

[491] Council of the EU, *(CFSP) Decision on restrictive measures against cyber-attacks threatening the Union or its Member States* (17 May 2019) Recital (7): "(…) Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, this Decision also allows for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations."
[492] Council of the EU, *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*.
[493] Soesanto.

3.4. Cyber defence – moving towards a renaissance?

As mentioned in Section 3.1., the EU approach to cyber defence never gained enough prominence after the publication of the EU Cybersecurity Strategy 2013. Because defence is traditionally linked to state-security, the likelihood of MS's security objective differing also in this domain is significant. In fact, in the *defence* domain, even more so. This was acknowledged already in 2015 with the European Parliament report on *Threats and Policy Responses*.[494] The report observed that "[t]raditional approaches to pan-European defence policy may be unsuitable given the boundless character of cybersecurity threats"[495] and that attempts to develop EU cyberdefence capabilities might result in "greater resistance in terms of harmonisation and coordination".[496] The same report also observed that "[t]he observation that cybersecurity means different things to different people is not without its consequences. How the issue is framed influences what constitutes a threat as well as what counter-measures are needed and justified."[497] But, as seen in Sections 2.3. through 2.3.4., regardless of whether a state-sponsored cyber operation crosses the *use of force* threshold, the defence systems of a state can be triggered and a proper lawful response under international law is available and needs to be considered. *But*, as will be seen in the case studies Chapters (Sections 4.2.1. and 4.2.4.1. for the UK, Sections 5.3.1.1. and 5.4.1. for Italy, and Sections 6.2.4. and 6.3.1. for Bulgaria), MS have defined the different types of cyberattacks differently, which leads the discussion again to what was observed in Section 3.3.2.1. – namely, that it is possible that one member state identifies a cyberattack as worthy of an EU-level response, but other MS do not. That said, it is important that this Chapter analyses it, as, if well-developed in the future, cyber defence could become an element of significant importance in the EU regulatory puzzle as regards state-sponsored attacks.

After 2013, there have been a number of policy-related documents on the topic, among which the 2014 EU Cyber Defence Policy Framework (CDPF)[498] and its update in 2018.[499] Whilst their importance is obvious for political scientists or IR experts, these are not as important for this

[494] European Parliament Directorate General for Internal Policies, *Cybersecurity in the European Union and Beyond Exploring the Threats and Policy Responses* (2015) 47.
[495] Ibid 47.
[496] Ibid 55.
[497] Ibid 13.
[498] Council of the EU, *EU Cyber Defence Policy Framework* (18 November 2014).
[499] Council of the EU, *EU Cyber Defence Policy Framework (2018 update)*

study. As they are not as relevant as a law or a particularly important strategy, they cannot qualify as "securitising moves" shaping the EU regulatory agenda.

The Cybersecurity Strategy of 2020 tried to mitigate this by putting cyber defence on the table again. An update of the CDPF was envisaged, with the idea to "enhance further coordination and cooperation" between the MS as well as EU agencies with defence responsibilities like the EEAS, or the EDA.[500] The most important policy document – the Communication on EU Policy on Cyber Defence came out in 2022 and it sow the seeds of what would later become the proposal for an EU Cyber Solidarity Act. The latter was adopted in April 2023 and, although it does not explicitly reference cyber defence, it aims "to detect, prepare for and respond to cybersecurity threats and incidents".[501] Despite, however, the initiative for a legally binding measure in the cyber defence area, it appears that, once again, and as expected, the MS are challenging the EU's views on the matter.[502] As of late summer 2023, the Cyber Solidarity Act is still under negotiations and therefore its role in the regulatory puzzle cannot be assessed as yet. Moreover, "response" here has not been identified as the potential answer by a member state or by the EU in terms of what is available under international law, but as "action in the event of a significant or large-scale cybersecurity incident, or during or after such an incident, to address its immediate and short-term adverse consequences".[503] This means that, as of late summer 2023, there is still a lack of an EU-level guideline on the appropriate response to a state-sponsored cyberattack against a MS such as countermeasure, self-defence, retortions (as described in Chapter II). Nonetheless, despite this obvious shortcoming of the EU cyber defence regime, if the Cyber Solidarity Act lives up to the expectation – and if MS find a way forward without watering down the legal text too much – this might be the first significant "securitising move" in the cyber defence field.

[500] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* 18.
[501] Proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents 2023 (EU Cyber Solidatity Act) Article 1.
[502] Alina Clasen, 'EU countries' reservations persist on Cyber Solidarity Act' (*EURACTIV*, 24 November 2023) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-reservations-persist-on-cyber-solidarity-act/> accessed 15 January 2023.
[503] Proposal for EU Cyber Solidatity Act Article 2 (10).

3.4.1. The Solidarity and Mutual defence clauses

The applicability of the Mutual defence and Solidarity clauses (Article 42.7 TEU and Article 222 TFEU respectively)[504] to cyberattacks is another important issue to be discussed that has so far remained ambiguous. Bendiek implied that there is no doubt as regards the applicability of at least the Solidarity clause: she argued that cyber incidents fall within the "man-made disasters" the clause lists, therefore its applicability is clear.[505] While logical as an argument, official EU documents present less certainty in the use of the clauses, falling short from clearly defining the red lines to be crossed for the two clauses to be applied. Back in 2012, a European Parliament Resolution suggested that cyber incidents threatening national security could trigger the Solidarity and/or the Mutual Defence Clauses.[506] This was the first time the EU had addressed in an explicit way the possibility of using these two clauses for cyber operations. The 2013 Cybersecurity Strategy further consolidated this, by stating that "[a] particularly serious incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause".[507] Yet, according to the 2020 Strategy "the EU should reflect upon the interaction between the cyber diplomacy toolbox and the possible use of Article 42.7 TEU and Article 222 TFEU".[508] This not only fails to build upon previous strategic efforts, it is vaguer and actually backtracks from the 2013 Strategy. While this could simply be a change of strategic approach, considering how serious and targeted most of the major recent attacks on CI sectors have been (addressed in Sections 2.4. through 2.4.2.1. and further in Sections 3.3.2.1. and 3.3.2.1.A)), a seven-year gap between the two Strategies should have led to a stronger strategic approach and the applicability of the two clauses - further explored and reinforced.

---

[504] Treaty on the European Union Article 42(7): If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, (…);
Treaty on the Functioning of the EU Article 222: The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to: (…)
(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

[505] Bendiek 68.

[506] European Parliament Committee on Foreign Affairs para 3.

[507] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 19.

[508] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* 17.

3.5. Testing the legal framework: the COVID pandemic as a case study

When analysing strategic and legislative approaches, having words on paper directing policy and legal requirements is not sufficient: it all comes down to their enforcement. This became evident in the cybersecurity domain with the COVID-19 pandemic, which was the first large-scale cybersecurity-resilience challenge some MS had to encounter. The correct implementation and enforcement of the NIS Directive (observed in detail in the three case studies in Chapters IV through VI) was tested. While health institutions across various (current and former) MS were targeted,[509] the March and April 2020 attacks in the Czech Republic provide an illustrative case study of the broader EU picture.

The March 2020 attack targeted a hospital in Brno,[510] the second largest city in the Czech Republic. It reportedly brought IT systems to a complete halt. Daily work was thus affected, new patients had to be re-routed to different hospitals and operations postponed. At the time of the attack, the hospital was also performing COVID-19 testing. While there is no certainty that this hospital was identified as an OES under the NIS Directive, it certainly meets the criteria. In which case, Czech officials failed to correctly implement and enforce the security requirements for OES as described in Section 3.3.1.1.A). A month later, the health sector in the Czech Republic suffered another series of attacks. While "unsuccessful", and although Czech officials never officially attributed the attack to a foreign state, it was reported Russia might be behind them.[511] The allegations were officially labelled "fake news" by Russian officials.[512] However, if foreign interference indeed took place, this would have additional legal implications as it might

[509] Walter Rocchi, 'Cybersecurity in the healthcare sector, medical equipment and confidential data at risk: the scenario (Cyber security nel settore sanitario, a rischio apparecchiature mediche e dati riservati: lo scenario)' (*Network Digital 360*, 5 Maggio 2020) <https://www.cybersecurity360.it/nuove-minacce/cyber-security-nel-settore-sanitario-a-rischio-apparecchiature-mediche-e-dati-riservati-lo-scenario/> accessed 15 January 2024;
'Coronavirus: Cyber-attacks hit hospital construction companies' (*BBC News*, 13 May 2020) <https://www.bbc.com/news/technology-52646808> accessed 15 January 2024;
Helene Fouquet, 'Paris Hospitals Target of Failed Cyber-Attack, Authority Says' (*Bloomberg*, 23 March 2020) <https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says> accessed 15 January 2024.

[510] Catalin Cimpanu, 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak' (*ZDNET*, 13 March 2020) <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> accessed 15 January 2024.

[511] Stolton.

[512] Russian Embassy in the Czech Republic, 'Embassy Comment on the accusation that Russia has performed cyberattacks on the territory of the Czech Republic' (20 April 2020) <https://www.facebook.com/AmbRusCz/posts/2440514632835902> accessed 22 January 2023.

have constituted wrongful act under international law such as violation of sovereignty in cyberspace for example (as defined in Section 2.2.2.1.i)). To reiterate also what was observed in Section 2.2.1., "[s]tate activity in cyberspace is thus limited by the traditional rules on sovereignty and territorial integrity".[513] Neither Czech, nor EU officials, however, ever discussed the possibility of violation of sovereignty or another bedrock principle of international law, at least not publicly. The EU's reaction was in fact very vague and weak. The High Representative Borell referenced cyberattacks on the health sector, stating that the EU and its Member States condemned "malicious behaviour in cyberspace".[514] In June, Commission's President von der Leyen seemingly pointed a finger at China, stating attacks on hospitals "cannot be tolerated".[515] But neither statement referenced the Czech attacks specifically, nor did they mention the possibility of a foreign interference within the territory of an EU MS. No reference was made regarding an EU-level response in support of the victim MS despite the Cyber Diplomacy Toolbox offering the necessary tools to respond. And while the EU has remained silent, the US Secretary of State Pompeo explicitly referenced the Czech attacks, declaring that anybody engaging in such activities against allies should "expect consequences", implicitly undermining the EU's authority and making it seem unprepared to respond.[516]

The COVID attacks thus were a missed opportunity as the EU could have advanced further the discussions on the key topic of state-on-state attribution (addressed in Section 2.4.). It could have also used these cases to develop its views on how international law principles such as sovereignty (as analysed in Sections 2.2.2.1.A)i) and 2.2.2.1.i)-) can be violated in cyberspace as, as observed in Section 2.2.2.2., the EU still has not done so.

[513] Wolfrum 989.
[514] Council of the EU, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic' (30 April 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/> accessed 15 January 2023.
[515] Stolton.
[516] U.S. Embassy in the Czech Republic, 'The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector' (17 April 2020) <https://cz.usembassy.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/> accessed 15 January 2024.

3.6. Conclusion

This Chapter analysed the decade-long road the EU has walked to pursue a better integration in the cybersecurity field and become a collective cybersecurity regulator in the two sub-domains of NIS and cyber diplomacy. The EU has had an ambitious agenda, trying to regulate in an area that, as presented in Chapter II, regulatory measures and applicability of existing laws are still subject to lively debates both at the experts' and at the decision-makers' tables. In the jungle of diverging opinions and views at international level, the EU has tried to become less insecure in cyberspace. However, despite significant achievements, such as the adoption of key cybersecurity laws (or "securitising moves") – the NIS Directive 2016, the Cybersecurity Act 2019, the NIS2 Directive 2022 – and the adoption of the Cyber Diplomacy Toolbox in 2017, among others, both the NIS and the CFSP legal regimes still present some significant gaps. In the NIS area, the debates between the MS and the Commission, at times exacerbated by disagreements and tension, have ultimately helped shape the framework that might seem imperfect because of asymmetrical implementation and different roles of the MS, but it is a framework that best fits the EU's nature and is adapted to its security objectives. In an area of such relevance to national security, where technical and operational capabilities are key, it is not surprising that some MS sometimes would want to act independently from the EU and from other MS. The reality is that different levels of preparedness still exist among the MS (as will be observed in Chapter IV through VI), but that does not disqualify the EU as an (imperfect) cybersecurity regulator and should not imply the need for circumventing the EU legislation to pursue MS-level response to cyberattacks on the CI sectors.

The securitisation process of the foreign policy area, however, differs from the NIS pillar, with the two securitisation processes moving at different paces and, as appears, in different directions. While the NIS body of law demonstrates the EU's consolidating position as a cybersecurity regulator, the EU foreign policy posture remains underdeveloped and still does not amount to a regulatory stage: the process of securitisation of this particular field is in its infancy. Divergent security (and not only) objectives see the MS unable to compromise, making the adoption of new "securitising moves" – sanctions – largely unattainable. As evidenced in Section 2.4. some MS such as the UK (when still a member state) never shied away from actively pursuing their own security objectives in state attribution, and the fact that the EU experienced difficulties in

addressing foreign policy issues collectively (Sections 3.3.2. through 3.5.) was never a deterrent for the MS with high level of preparedness.

To conclude, also in view of the international developments seen in Chapter II, the EU's legal approach to cybersecurity has indeed interacted – and in general terms reflected the international developments in the field. It has grabbed the opportunity to advance a regulatory approach where the international community remained undecided. Yet, the credibility and effectiveness of its own regulatory framework depends on its MS. The manifestation of the strengths of the regulatory regime is in fact seen through the actual implementation and enforcement process of the laws across the MS, but the different levels of preparedness among them persists, despite almost ten years of strategic and legal approaches' evolution. The aim of the next three Chapters is therefore to address how the EU acted to address the impact of the different levels of preparedness on its regulatory regime and how it filled the gaps left by the different levels of preparedness of the MS in order to achieve its ambitious cybersecurity regulatory agenda.

The next three Chapters will address three case studies – the UK, Italy and Bulgaria. Each of these Chapters will illustrate in more detail how the MS operate their different approaches to cybersecurity, which has resulted in the limitations of the EU's advancements as a regulator. Chapters IV through VI will also explore to what extent the EU's regulatory achievements have actually worked in practice, by considering how they were implemented in MS that found themselves at three very different levels of preparedness when the NIS Directive came into force. The UK represents those states with high level of preparedness, Italy – those with medium level, and Bulgaria – those with low level. Ultimately, the analysis of the case studies will aim at presenting a conclusive analysis on the effectiveness of the EU regulatory approach to cybersecurity (comprising of all relevant sub-fields) and how the later fits with the broader regulatory developments in the field of cybersecurity at international level.

Chapter IV: Member States' legal cybersecurity frameworks: the UK

4.1. Introduction

This Chapter will focus on the UK, now a former EU MS, but one that had a key role in shaping the EU cybersecurity regulatory framework. It will represent the MS with high level of cybersecurity preparedness.

The Chapter will be divided into two main sections: pre- and post-Brexit, reflecting the development of the national legal framework as a member state and as a non-member state. The analysis will address the legal preparedness the UK had while an EU MS, by comparison to the other MS analysed, and will further discuss the effects Brexit has had on the development of the EU ambitions to become a cybersecurity regulator. Thus, the Chapter will analyse the main research question, and more specifically - how the UK has influenced the development of the EU regulatory framework and what its overall preparedness pre- and post-NIS Directive tells about the EU legal preparedness. The Chapter will begin by evaluating the UK legal framework before the adoption of the NIS Directive. It will address how the UK defined malicious foreign-sponsored cyber operations and what the institutional architecture was. Even though cyberattacks have been considered a Tier One threat to national security since 2010, no legislation on the matter addressed cybersecurity of the critical infrastructure (CI) sectors specifically before the adoption of the NIS Regulations 2018, the transposing instrument of the NIS Directive. Yet the UK has been considered a "global cyber leader" in cyber security.[517] This is because over the course of more than three decades, the UK has been gradually addressing various aspects of cybersecurity, such as device misuse (today known as cybercrime, as defined in Section 2.3.1.), with the Computer Misuse Act (CMA) 1990; the security of the telecoms sector (as addressed in Section 3.3.1.1.A)), with the Communications Act 2003, transposing the EU Framework Directive 2002; the role of the intelligence agencies in preemptively conducting equipment interference (also known as hacking, or offensive cyber) with the Intelligence Services Act 1994 and more recently, the Investigatory Powers Act 2016. This Chapter will give a brief account of only those pieces of legislation contributing significantly to the development of the cybersecurity

[517] Templeton and Dewar.

legal framework. Related issues, such as the Snowden revelations of mass surveillance and hacking perpetrated by the UK intelligence agencies, and the subsequent privacy-related lawsuits against the GCHQ, will be mentioned but not analysed in detail. In this respect, this Chapter will be different from the other case studies, as Italy and Bulgaria have not, as yet, become offensive cyber powers and their respective intelligence agencies have not yet been subjected to lawsuits challenging their intrusive powers in cyberspace.

Section 4.2.4. will then detail how the UK transposed the NIS Directive: despite the imminent withdrawal from the EU, the UK was among the first MS to transpose it, on 10 May 2018, via the NIS Regulations. This demonstrated that the UK considered the EU Directive – and the overall topic of cybersecurity of the CI sectors – as very important. As of August 2023, the NIS Regulations remain the only legally binding cybersecurity measures applicable to CI sectors adopted in the UK.

In the post-Brexit part of the Chapter, Section 4.3., the focus will be on the UK's legal developments as a non-EU member state, with the aim to access the EU regulatory powers and its ability to export its framework outside its own MS. The EU-UK relationship will also be investigated, as the role the UK played as a member state shaping the EU's legislative framework was crucial (as seen in Sections 3.3.1.2. through 3.3.1.3.). This analysis is not going to consider in detail the law enforcement pillar of cybersecurity, therefore it will not deal with Justice and Home Affairs, the role of Europol and the European Cybercrime Center and how Brexit affected, for example, online crime related to data sharing between the UK and the EU as it falls outside the scope of this thesis. The Chapter will instead focus on the impact of Brexit in terms of the EU's role as a cybersecurity regulator and will assess, in light of one of its key leaders leaving the decision-making table, whether the EU is able to meet the challenging international environment in cyberspace where capabilities and intelligence information are key.

4.2. Pre-Brexit

This introductory sub-section sets out a brief overview of how the UK's strategic approach on cybersecurity more generally, and foreign-sponsored cyberattacks more specifically, developed

since the very first cybersecurity strategy was adopted in 2009. The discussion will serve as the basis for the analysis of the legal framework that has been developing simultaneously, discussing how the different types of attacks seen in Chapter II have been conceptualised by British laws.

Cybersecurity and foreign-sponsored cyber threats were first acknowledged in the UK in the 2008 National Security Strategy.[518] Guitton argued that while the UK's cyber strategy fitted the threats identified in the Strategy, the resources allocated were excessive as no major cyberattacks had occurred on UK soil at the time.[519] But cybersecurity was progressively gaining more political and strategic importance. Cyberspace was hence identified as "the most important new domain in national security of recent years" by the updated version of the Strategy, published in 2009,[520] which also announced the adoption of the very first UK cybersecurity strategy.[521] Interestingly, the latter did not define cybersecurity in technical terms – which was the case with the EU (Section 3.2.1.), Italy (Sections 5.3.1.1. and 5.3.1.2.) and Bulgaria (Sections 6.2.4. through 6.2.4.2.) - but as a politico-strategic domain, embracing "both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers".[522] The latter also acknowledged that "the most sophisticated threat" in cyberspace came from states,[523] which reflects the international developments at that time, where the applicability of international law to state-on-state cyber operations was still causing contentious debates (as seen Sections 2.2.2. and 2.2.2.1.). In terms of cyber warfare, the term was not defined but only referenced by acknowledging that there was still an ongoing debate as to what the term may entail,[524] reflecting international developments in the field, at the time exacerbated by the 2007 Estonia attacks and the possibility of war being waged in cyberspace that dominated experts' and decisionmakers' debates (as seen in Sections 2.2.2. through 2.2.2.2.).

[518] Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world* (March 2008) 16.
[519] Clement Guitton, 'Cyber insecurity as a national threat: overreaction from Germany, France and the UK?' (2013) 22:1 European Security 21, 22.
[520] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009. Security for the Next Generation* (June 2009) 13.
[521] Ibid 4.
[522] Cabinet Office, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space* (June 2009) 9.
[523] Ibid 13.
[524] Ibid 14.

Despite this first attempt at approaching the topic from a politico-strategic standpoint, in the 2010 National Security Strategy, the Government admitted having "a defence and security structure that is woefully unsuitable for the world we live in today".[525] The Strategy identified "[h]ostile attacks upon UK cyber space by other states and large scale cyber crime" as a Tier One threat to national security.[526] In their analysis of the Strategy, Neville-Jones and Phillips pointed out the challenges surrounding the acknowledgement that cybersecurity was not "a traditional defence or security issue" to be dealt with only by the Defence Ministries or the intelligence agencies.[527] Indeed, at the time, cybersecurity was a more complex field, a largely uncharted territory from a legal and strategic perspective for many EU states, in which civilian and military issues intersected. In the early 2010s only thirteen out of 28 EU MS, among which the UK, had a cybersecurity strategy (Section 3.3.). The UK was beginning to emerge as a state with high level of strategic and legal preparedness on the topic.

The 2011 Cyber Strategy further revealed a persistent trend as regards state-sponsored attacks: it changed the language slightly, listing states as "some of the most sophisticated threats".[528] Unlike the 2009 version, this Strategy also discussed the UK critical infrastructure sectors' position of being mostly privately owned,[529] but no connection between the vulnerability of these sectors and the rise of state-sponsored attacks was made. The 2016-2021 Strategy showed a different viewpoint, claiming that "only a handful" of states had the technical knowledge and sophistication to become a serious threat,[530] thereby signalling that the UK was beginning to single out particular states as potential cyber powers. No link appeared again between these states and potential attacks on CI sectors; however, the 2016 Strategy introduced a new concept in relation to the protection of the latter: active cyber defence (ACD), meaning that the UK had begun addressing cyber threats more proactively, rather than simply acknowledging that they exist. Defining ACD as "the principle of implementing security measures to strengthen a network or system to make it more robust against attack",[531] one of its objectives was to

[525] H M Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (2010) 5.
[526] Ibid 27.
[527] Pauline Neville-Jones and Mark Phillips, 'Where Next for UK Cyber-Security?' (December 2012) 157 RUSI JOURNAL 32, 32.
[528] HM Goverment, *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world* (November 2011) 15.
[529] Ibid 28.
[530] HM Government, *National Cyber Security Strategy 2016 - 2021* (November 2016) 18.
[531] Ibid 33.

strengthen the CI sectors against threats.[532] Furthermore, when addressing the possibility of a cyberattack against the UK, the text of the document revealed that the UK already had offensive cyber capabilities[533] (something Italy and Bulgaria have not had yet). Under the strategy's text, the UK could use them should they "chose to do so"[534] and cyberattacks which were treated as an "equivalent conventional attack" would trigger such a response.[535]

The most recent Strategy to date, published in 2022, was the first one adopted in a post-Brexit reality and has a significantly different approach to state-sponsored operations. It does not mention such operations in the generic way the previous ones did, but it concretely attributed cyberattacks to Russia and China, such as the SolarWinds hack and the attacks on the Microsoft Exchange servers.[536] As seen in Section 2.4. this puts the UK's name among a very short list of states that have attributed attacks to other states, consolidating the UK's proactiveness, top intelligence capabilities and, consequently, attribution capabilities. Whilst speculative, the fact that the UK was so explicit in the first Strategy post-Brexit and has never been before could be also linked to its newly gained sovereignty and unchained-from-the-EU status. As Section 3.3.2.1. observed, the EU's attribution decision-making process and issuing sanctions took years, potentially also limiting the MS's attribution powers despite the EU framework allowing for sovereign actions as regards attribution.

Against this strategic background, the following sub-sections will analyse the operative legal framework. The analysis will backtrack a bit to provide the basis upon which the cybersecurity-related legislation was built, starting from the first regulatory developments which in all three case studies manifested in the realisation that the rise of potential misuse of devices needs to be addressed by criminal law. Section 4.2.1. will hence review how the devices' use and misuse-related laws in the UK were conceptualised, creating the ground for the development of the cybersecurity legislation of today with its focus on the cyber resilience of the CI sectors, state-sponsored cyberattacks and cyber offensive and defensive capabilities.

[532] Ibid 34.
[533] Ibid 9.
[534] Ibid 9.
[535] Ibid 25.
[536] HM Government, *National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK* (December 2022) 27.

4.2.1. The UK legal framework pre-NIS transposition law

In the UK (and in Italy and Bulgaria), cybersecurity legislation's ground lies upon various building blocks which represent different devices misuse-related laws evolving through a layering process. In the UK a completely new law was adopted to deal with these new criminal phenomena – the Computer Misuse Act 1990 (CMA 1990), analysed in detail in Section 4.2.1.1. (as opposed to Italy and Bulgaria which amended their respective Penal Codes, as will be seen in Sections 5.2.1. and 6.2.1.). After the adoption of the CMA 1990 some twenty years would pass before these crimes came to be considered a potential threat to national security and, with cybersecurity strategic approaches gaining a momentum of their own, as observed in Section 4.2., another few years of threat landscape and legislation development had to pass. Sections 4.2.1.1. through 4.2.2. will therefore provide an overview of how – what we would today call – cybersecurity legislation has developed, using a thematic approach rather than a chronological one. These Sections will hence discuss the topics of computer misuse, the telecommunications sector's securitisation, and equipment interference and interception capabilities (or cyber defence and offence, as per the UK's own perception of the applicability of these capabilities, seen in Sections 4.2.1.3. through 4.2.1.3.i)), and how they have been addressed in the British legal system.[537]

4.2.1.1. Unauthorised access to computer systems

Even though some computer misuse-related crimes were already tackled by existing criminal law such as the Criminal Damage Act 1971 or the Forgery and Counterfeiting Act 1981,[538] in 1988, the UK Law Commission issued a Working Paper on Computer Misuse with the purpose to "examine the applicability and effectiveness of the existing law of England and Wales in dealing

[537] The UK does not have one overarching legal system, it has three separate jurisdictions. But legislation concerning national security issues extends across all the jurisdictions.

[538] For more detailed account, view Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70:5 The Journal of Criminal Law 424, 425 - 429. Fafinski includes a list and analysis of existing pieces of legislation such as the Criminal Damage Act 1971, which has been relied upon in *R v Talboys*, *Cox v Riley*, and the Forgery and Counterfeiting Act 1981, relied upon *R v Gold & Schifreen*.

with instances of computer misuse" and the potential need for a reform of the criminal law.[539] The following year the same Commission published its *Computer Misuse* report, recommending for three new offences of computer misuse to be created: unauthorised access to a computer, unauthorised access to a computer with intent to commit or facilitate the commission of a serious crime and unauthorised modification of computer material.[540] This pressure, together with the warning-flag case of *R v Gold & Schifreen* – in which the defendants managed to enter the British Telecom Prestel computer network – in 1988, finally led to the adoption of the Computer Misuse Act 1990 (CMA 1990),[541] which included the Law Commission's recommended offences.[542] Drafted "with the laudable intention of providing flexibility to adapt to a rapidly evolving field of criminal behaviour",[543] the CMA 1990 failed to deliver precisely on this: for instance, DDoS attacks, which rose to popularity in the late 1990s,[544] were not included in the scope of the law. Macewan argued that among the reasons the CMA was revealed to have flaws so soon after its adoption, lay the work of the Law Commission, which was "hampered by a dearth of reliable information", and was heavily influenced by stakeholders' views, delivered confidentially.[545] Hence, to reflect also changes in the threat landscape, the CMA had to be amended on multiple occasions to widen its scope. The adoption of the Police and Justice Act 2006 (sections 35-38),[546] for example, extended the offences to "encompass all" DDoS attacks.[547] Thereafter the Serious Crime Act 2015 (sections 41-44)[548] added provisions to comply

[539] The Law Commission, *Working Paper No. 110 on Computer Misuse* (1988) para 1.2.
[540] The Law Commission No.186, *Criminal Law. Computer Misuse* (1989) para 5.2.
[541] Stefan Fafinski, 'The UK legislative position on cybercrime: a 20-year retrospective' (2009) 13:4 Journal of Internet Law 3, 4.
[542] The wording of the offences differs slightly form the Law Commission's recommendations: the CMA 1990 lists unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised modification of computer material.
For a more detailed account of the law, including case law stemming from it, view Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change'.
[543] Ibid 442.
[544] Charalampos Patrikakis, Michalis Masikos and Olga Zouraraki, 'Distributed Denial of Service Attacks' (December 2004) <https://web.archive.org/web/20190826143507/https:/www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html> accessed 20 December 2023.
[545] Neil Macewan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (December 2008) Criminal Law Review 955, 960.
[546] The Police and Justice Act 2006 (sections 35 - 38) tackle various computer misuse issues such as unauthorised access to computer material, unauthorised acts with intent to impair operation of computer and making, supplying or obtaining articles for use in computer misuse offences.
[547] Oriola Sallavaci, 'Combating Cyber Dependent Crimes: The Legal Framework in the UK' (2017) Communications in Computer and Information Science 53, 59.

with the EU Directive on attacks against information systems 2013.[549] Even though, as Sallavaci observed, and despite these amendments, the CMA's effectiveness in combating device-related crime is "questionable" because of low prosecution rates,[550] the CMA 1990 remains the UK's leading law on cybercrime to date.[551]

Some ten years later, the Terrorism Act 2000 was passed, and it named seriously interfering or seriously disrupting an electronic system to political ends as an act of terrorism.[552] What type of electronic systems was not specified. Clearly, any such operation would not fit the definition of cyberterrorism as defined in Section 2.4.3. Moreover, whilst important to be mentioned in the overall analysis of cyber threats, cyberterrorism largely falls out of scope of this thesis which focuses on state-on-state malicious cyber operations. Still, it is important to mention Section 1 of the Terrorism Act as it was among the first provisions in the UK to address disruption of electronic systems.[553] No similar provisions were observed in Italy and Bulgaria.

4.2.1.2. Securitisation in the telecommunications sector[554]

The topic of telecommunications' security has evolved significantly, especially since the emergence of electronic communications as potential threat-enablers. In the UK there are several laws that have progressively addressed the topic, the most relevant of which, analysed below, are the Communications Act 2003 and the Telecommunication (Security) Act 2021. Despite its

[548] The Serious Crime Act 2015 included an important section regarding culpability of an individual causing damage to "human welfare in any place", "economy of any country" and "national security of any country" - Serious Crime Act 41 (2)(2)(a), (c), (d). It also introduced much tougher punishments in case of damage to the national security or loss of human life, illness or injury. If convicted on indictment, the person will be imprisoned for life - ibid 41 (2)(1)(7).
[549] Sallavaci 61.
[550] Ibid 64.
[551] For a more detailed account of the CMA 1990, the Police and Justice Act 2006 and the Serious Crime Act 2015, including case law stemming from them, view ibid.
[552] UK Terrorism Act 2000 Section 1 (2) (e).
[553] For more details on the Terrorism Act 2000 Section 1 view Keiran Hardy and George Williams, 'What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism' in Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism Understanding, Assessment, and Response* (Springer 2014).
[554] It is to be mentioned that the 'securitisation in the telecommunications sector' meant in this study refers only to a few security-related articles in the EU Frameworks Directive 2002. It does not imply that the objective of the Directives was to introduce only security measures to the sector. This study is adopting this simplified terminology to demonstrate in a clearer way the steps national governments have taken to address the gradual incorporation of security measures in the different national legislation.

seeming relevance to this topic, the Telecommunications Act 1984 will not be discussed in this section, but in the following one, as it is important for the development of capabilities performed by the Security and Intelligence Agencies (SIAs) rather than the telecommunications sector.

The Communications Act 2003's relevance is manifested, like in the other case studies (Sections 5.2.2. and 6.2.2.), in the fact that it introduces the definitions of "electronic communications", as found in Article 4 of the NIS Directive (as seen in Section 3.3.1.1.A)). The definition derives from EU legislation, namely, the Framework Directive 2002[555] and the UK Communications Act 2003 was its transposing instrument.

The law was subsequently amended with the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020 (transposing the European Electronic Communications Code 2018 into UK law), and more recently, with the Telecommunications (Security) Act 2021, to bring security measures up to date and to remove references to EU instruments no longer applicable in the UK post-Brexit. More recently, the Product Security and Telecommunications Infrastructure Act, delivering security provisions for connected products, was adopted.[556] The law is similar to the EU Cyber Resilience Act, currently under development as of summer 2023, which requires that products with digital elements available on the EU market need to meet specific essential cybersecurity requirements through their life cycle, including design and development phases.[557] In the telecoms field therefore, the UK and the EU seem to be moving in the same direction post-Brexit.

[555] Framework Directive 2002 Article 2 (a).
[556] Culture Department for Digital and Media & Sport, 'Telecoms security: proposal for new regulations and code of practice' (August 2022) <https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice> accessed 20 December 2023.
[557] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act).

4.2.1.3. Cyber offence and cyber defence: equipment interference, interception and collection of communications data: developing offensive and defensive cyber capabilities

This subsection analyses the UK legal concepts of equipment interference (EI), interception, and acquisition of communications data, and will walk the reader through the various pieces of legislation, relied upon when conducting cyber operations overseas. As opposed to the other two case studies, the concepts of cyber offence and defence come up higher than the other two because the UK has had powers to engage in such operations for almost 30 years and the capabilities that will be addressed below have been an integral part of the shaping of the UK as a cybersecurity leader. The focus will be on techniques used to conduct politically motivated defensive and offensive cyber operations, and relevant laws here are the Intelligence Services Act 1994 (ISA 1994) and the Investigatory Powers Act 2016 (IPA 2016) as regards EI, and the Regulation of Investigatory Powers Act 2000 (RIPA 2000) and again the IPA 2016 as regards interception. The Telecommunications Act 1984 (Telecoms Act 1984) will also be discussed in this sub-section, as the first law (chronologically, among those listed) that regulated bulk collection of electronic communications data. Considering the vast and different scope of these laws - they were not specifically drafted with cyber operations in mind - this section will follow the evolution in applicability of only those provisions applicable to cyber activities and capabilities. EI, interception and acquisition of communications data operations for, for example, counter-terrorism purposes, and locating criminal activity in the dark web such as weaponry smuggling, financial fraud, child pornography, can potentially be authorised under the same laws – but these operations fall out of scope of this thesis.

The three capabilities in question have been practiced in the UK for more than two decades, unbeknownst to the public. The practice of collecting data in bulk became public with Snowden's revelations in 2013 when he released enormous amounts of documentation proving that the UK agencies, together with their U.S. counterparts, have practiced mass surveillance and hacking.[558] In the aftermath of the scandal, over the course of the next few years, the UK Government was forced to admit that they have, in fact, practised bulk collection of data, specifically bulk interception (BI), under RIPA 2000's section 8(4),[559] bulk acquisition of

[558] 'Snowden Revelations' (*Lawfare*) <www.lawfareblog.com/snowden-revelations> accessed 10 March 2017.
[559] Regulation of Investigatory Powers Act 2000, s.8 (1) An interception warrant must name or describe either—

communications data under section 94 of the Telecoms Act 1984,[560] and EI under section 5 and 7 of the ISA 1994.[561] The Government was swift to claim that BI had developed because of the rise of new threats[562] and both EI (but not bulk EI) and BI were identified as having had a vital role in detecting cyber threats to the UK.[563]

A few years after the Snowden scandal, the IPA 2016 was adopted[564] with the aim of collecting in one piece of legislation many already existing provisions.[565] It includes a wide range of powers, including for bulk acquisition (BA), bulk personal datasets (BPD), BI and BEI. Bulk powers will be the main focus here as they are foreign-focused, aiming at acquiring, accessing or manipulating data overseas,[566] whereas targeted powers, also covered by the IPA, are not.[567]

(a) one person as the interception subject; or
(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.
(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.
(…)
(4) Subsections (1) and (2) shall not apply to an interception warrant if—
(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and
(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying—
(i) the descriptions of intercepted material the examination of which he considers necessary; and
(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

[560] Gordon Corera, 'How and why MI5 kept phone data spy programme secret' (*BBC News*, 5 November 2015) <https://www.bbc.com/news/uk-politics-34731735> accessed 21 December 2023.

[561] Home Office, *Equipment Interference Code of Practice* (January 2016) para 1.1-1.5.

[562] HC Deb 12 April 2016, vol 608, col 129.

[563] David Anderson Q.C., *Report of The Bulk Powers Review* (August 2016) para 2.54 (d) (for bulk EI) and para 5.54 (for bulk interception).

[564] Before the IPA was adopted, there was the short-lived (because of a sunset clause) Data Retention and Investigatory Powers Act 2014 (DRIPA 2014), which was adopted "in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data; to amend the grounds for issuing interception warrants, or granting or giving certain authorisations or notices, under Part 1 of the Regulation of Investigatory Powers Act 2000" DRIPA Introduction. This Chapter will not focus on the DRIPA as more recent laws such as the IPA 2016 have covered the topics addressed in it.

[565] HC Deb 21 April 2016, vol 608, col 441.

[566] "Bulk interception warrants allow for the collection of communications of persons who are outside the UK in order to discover threats that could not otherwise be identified." Home Office, *Investigatory Powers Bill Factsheet - Bulk Interception* (October 2015) 1 and David Anderson Q.C. para 2.7-2.8.
"'[B]ulk equipment interference warrants are foreign focused and are aimed at identifying communications and other information relating to individuals and entities outside the British Islands." Home Office, *DRAFT Equipment Interference Code of Practice* (February 2017) para 2.7.

[567] The main difference between, for example, targeted and bulk EI powers lies in the safeguards: targeted EI warrants can be conducted not only by the SIAs, need no link to national security or for them to be foreign-focused.

Even though these powers were heavily scrutinised by the UK Parliament,[568] Ben Wallace, then minister of State for Security, asserted that the IPA did not introduce new powers to the agencies.[569] This is somewhat misleading, as the previous legislation listed above, regulating SIAs work, did not address bulk capabilities *sensu stricto* and these powers were never debated or voted on in the House of Commons.[570] Therefore, these powers were not new indeed, but they were made legal *explicitly* for the first time with the IPA 2016.

A) Collection of communications data

Now repealed by the IPA 2016,[571] over the course of three decades, the Telecoms Act 1984 was the legal basis for bulk collection of electronic communications data.[572] The Act is important not because of its overall purpose,[573] but because of one particular clause - Section 94 *Directions in the interests of national security*.[574] The existence of the capability of collecting data stemming

---

Bulk EI warrants are more "tightly controlled", can only be sought out by the SIAs, need to be in the interest of national security and have to be foreign-focused. At the same time, targeted thematic warrants can be "very broad in their scope" and used "at scale" – yet, subject to fewer safeguards. David Anderson Q.C. para 2.51-2.57.

[568] The possibility of abuses of privacy due to the increasing use of computers were discussed in the UK already in 1975. A White Paper on Computers and Privacy was published in December 1975 which envisaged bringing forward legislation drafted by the Data Protection Committee. HC Deb 03 March 1977, vol 927, col 589.
The Committee on Data Protection was appointed in July 1976 with the task to ensure "that all existing and future computer systems holding personal information, in both the private and public sectors, were operated with appropriate safeguards for privacy" and to consider legislation permanently establishing such safeguards. Data Protection Committee 1976-1978, *Data Protection Committee: Evidence and Papers* (The National Archives 1975-1979).
The Data Protection Act was adopted in 1984 to "regulate the use of automatically processed information to individuals and the provision of services in respect of such information". The Data Protection Act 1984.

[569] HC Deb 23 February 2017, vol 621, col 38WS.

[570] HC Deb 15 March 2016, vol 607, col 890.

[571] Investigatory Powers Act 2016 c.25, s. 272(1), Sch. 10 para 99.

[572] Interception of Communications Commissioner's Office (IOCCO), *Report of the Interception of Communications Commissioner. Annual Report for 2016* (2017), 25.

[573] The Telecoms Act 1984 was adopted with the purpose of abolishing British Telecommunications "exclusive privilege with respect to telecommunications", amending other legislation e.g. the Wireless Telegraphy Act 1949 and 1967, appointing and listing the functions of a Director General of Telecommunications, among other things. Telecoms Act Introduction.

[574] The Telecoms Act 1984 Section 94 Directions in the interests of national security etc. [emphasis added]
(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such **directions of a general character** as appear to the Secretary of State to be **requisite or expedient in the interests of national security or relations with the government of a country or territory outside the United Kingdom.**
(2) If it appears to the Secretary of State to be requisite or expedient to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with

from section 94 was an "extremely tightly-controlled secret",[575] not officially acknowledged until November 2015,[576] but practiced by the GCHQ at least since 2001.[577] The provision was problematic because the text did not specify a timeframe for when a "direction" for data collection issued under it would automatically expire,[578] making it very controversial.[579] As this

---

a person to whom this section applies, **give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction**.
(3) A person to whom this section applies shall give effect to **any direction** given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under this Act.
(4) The **Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom**, or the commercial interests of any person.
(5) A **person shall not disclose**, or be required by virtue of any enactment or otherwise to disclose, **anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom**, or the commercial interests of some other person.
(6) ...
(7) ...
(8) **This section applies to the Director and to any person who is a public telecommunications operator or approved contractor** (whether in his capacity as such or otherwise); and in this subsection " approved contractor " means a person approved under section 20 above [emphasis added].
[575] David Anderson Q.C. para 2.29.
[576] Ibid para 1.25 d).
[577] Ibid para 2.35.
[578] This, in itself, means that the clause was in direct violation of article 5 (1), *Confidentiality of communications,* of the EU ePrivacy Directive 2002: 1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
Article 15(1) then proceeds to state [emphasis added]
Member States may adopt legislative measures **to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security** (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, **adopt legislative measures providing for the retention of data for a limited period** justified on the grounds laid down in this paragraph. (…)
[579] The fact that the clause was not repealed or amended with the RIPA 2000, adopted considering the developments in technology and communications (Burkhard Schafer, 'Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill' (Wiesbaden) 40 Datenschutz und Datensicherheit - DuD 592, 592), demonstrates its importance for the security agencies and the lack of willingness on their side for it to be amended. The UK's regime has, therefore, been in violation of EU law for fifteen years. This was officially confirmed by the CJEU in 2020 Case C-623/17, according to which "[a]rticle 15(1) of Directive 2002/58, (…) must be interpreted **as precluding national legislation** enabling a State authority to require providers of electronic communications services to **carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security**." Consequently, also the UK Investigatory Powers Tribunal, in its 2021 Case No PT/15/110/CH, para 28, stated that "[i]n the light of the

thesis does not look into bulk collection of communications or other personal data specifically, pinpointing this particular section legalising this particular capability is seen not from the angle of violation of privacy and abuse of power, but as a proof of how early the UK started developing legislation that empowers technical capabilities to access data. This legislation would evolve and consolidate operations such as communications' interception and EI capabilities on overseas devices, which can already be identified as straightforward offensive cyber operations. The UK was therefore gradually developing legislation supporting cyber capabilities that was very advanced compared to Italy and Bulgaria, which, as will be seen in Chapters V and VI, have never got to the same level of preparedness.

B) Interception

BI is regulated today by Part 6 Chapter 1 of the IPA 2016. Before the IPA, as mentioned, the provision regulating these powers was found in the RIPA 2000, specifically section 8(4).[580] The main purpose of BI is to intercept large quantities of overseas-related communications in order to collect intelligence on possible threats.[581] BI can be used for both extraction of communications data or for interception of actual content.[582] The GCHQ maintained that when it comes to cyber defence, the need for BI was "constant"[583] and "vital" and that it had prevented a large number of cyberattacks.[584] According to Home Office, BI powers were essential for detecting the vast majority of cyberattacks against people, businesses and government networks in the UK.[585] The use of interception techniques, however, has been progressively hampered by encryption, making EI the only option available to obtain the necessary information.[586]

---

judgment of the CJEU, which is binding on this Tribunal, it is now clear that **section 94 of the 1984 Act was incompatible with EU law**". [all emphases added]. This, however, is a topic not discussed in detail further.

[580] David Anderson Q.C. 21.

[581] Home Office, *Investigatory Powers Act 2016. Consultation: Codes of Practice* (February 2017) 7.

[582] Lorna Woods, 'United Kingdom: Draft Investigatory Powers Bill' 2:1 (2016) European Data Protection Law Review 103, 105.

[583] David Anderson Q.C. 81.

[584] Ibid 91.

[585] Home Office, *Operational Case for Bulk Powers* (March 2016) para 4.15, 16.

[586] David Anderson Q.C. para 2.47.

C) Equipment interference

BEI,[587] on the other hand, is regulated by Part 6 Chapter 3 of the IPA 2016. Known in the past as computer network exploitation (CNE), today EI is commonly known as hacking, or any other sort of intrusion into a technical device.[588] Labelled "the most powerful and intrusive capability GCHQ possesses",[589] the purpose of EI is to "obtain communications, equipment data or other information",[590] or, in more general terms, prevent cyberattacks targeting the UK.[591]

Before the IPA, the provision regulating EI was the ISA 1994's section 5 for both inside and outside the UK, and section 7[592] for outside the UK.[593] This became known only in 2015 with the publishing of the *Draft Equipment Interference Code of Practice*.[594] The Government was forced to publish it because of a case, *Privacy International* v *Foreign Secretary (Privacy/GreenNet),*[595] during whose proceedings GCHQ's practice of relying on the ISA 1994 for conducting EI became known.[596] It should be stressed that the GCHQ could *legally* rely on section 7 of the ISA 1994 only since 2001, as per amendment made to the law by section 116 of the Anti-terrorism, Crime and Security Act 2001.[597] Prior to that only MI6 could rely on the 1994 Act. Therefore, while EI might not have been new, the power of conducting it was significantly expanded with

[587] For a very detailed analysis on the use of EI from a privacy perspective, and its compatibility with the European Convention on Human Rights, under both the ISA 1994 and the IPA 2016, view Paul F. Scott, 'General warrants, thematic warrants, bulk warrants: property interference for national security purposes' 68:2 (2017) Northern Ireland Legal Quarterly 99.
[588] David Anderson Q.C. 34.
[589] *Privacy International and Greennet & Others v.s (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters [2016]* Investigatory Powers Tribunal, Witness statement of Eric King, 5 October 2015, 5.
[590] Home Office, *Investigatory Powers Act 2016. Consultation: Codes of Practice* 7.
[591] David Anderson Q.C. 37.
[592] Intelligence Services Act 1994 Article 5(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.
(3) A warrant authorising the taking of action in support of the prevention or detection of serious crime may not relate to property in the British Islands.
Article 7(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.
[593] David Anderson Q.C. para 2.48.
[594] Ibid para 2.50.
[595] *Privacy International and Greennet & Others v.s (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters [2016]*.
[596] Scott 105.
[597] Anti-terrorism, Crime and Security Act 2001 Section 166 (1) In section 7 of the Intelligence Services Act 1994 (c. 13) (authorisation of acts outside the British Islands), in subsection (3) —
(a)in paragraphs (a) and (b)(i), after "the Intelligence Service" insert, in each case, " or GCHQ " (…)

the IPA 2016,[598] with the 1994 regime not repealed by the IPA.[599] While Scott has claimed that the 1994 law "lacks safeguards in relation to confidential material"[600] and identified the use of EI warrants under such regime as "particularly concerning" as it included no requirement that the "information thus acquired be examined only according to a requirement of necessity",[601] he also asserted that 1994 law will continue to be relied upon for EI operations different from simply acquiring data (for which the IPA 2016 would be used), such as EI with the purpose of destroying or manipulating the functioning of an electronic system.[602]

Hence, protecting GCHQ's EI capabilities (in lawsuits) was seen as essential, especially "from judges in Luxembourg and Strasbourg" whose perception of conducting espionage operations is seen from the perspective of totalitarianism practices in Europe rather than "the British tradition of royal prerogative and empire".[603] This observation leads back to Section 3.3.1.2. which followed the UK's constant push for the MS to remain the sovereigns of cybersecurity as opposed to the EU leading the way and developing its own legislative approach. It also highlights the profoundly different perception the UK had as regards offensive cyber operations. Feeling entitled to pursue its own security interests in cyberspace, the UK kept challenging the EU, thereby demonstrating that one of the "deterrents" in the development of the EU legal regime were actually its own MS (as per the main research question posed in Section 1.2.).

i) Equipment interference in use

While David Anderson's Bulk Powers report "unsurprisingly" emphasises the counter-terrorism agenda where bulk powers are concerned,[604] their use, and specifically the use of EI for cyber operations, is somewhat downplayed both in the report and other accompanying the IP Bill documents. It can be speculated why that is – perhaps because the SIAs would not want that

[598] Scott 100.
[599] Ibid 119.
[600] Ibid 114.
[601] Ibid 107.
[602] Ibid 120.
[603] 'The snoopers' charter of warrants and watchers' *The Economist* (23 January 2016) 23, 23.
[604] Tom Sorell, 'Privacy, bulk collection and "operational utility"' in *National Security Intelligence and Ethics* (1 edn, Routledge 2021) 142.

attention was put on performing politically-backed hacking operations abroad for instance or because these were indeed not central to the scope and aims of the Bill – but it is clearly *not* because EI is not commonly used for such operations. It is true that section 7 of the ISA 1994 and particularly after being amended in 2001 had made hacking on overseas devices legal long before the first *UK Cyber Security Strategy 2009* was adopted and long before state-led attacks were considered a Tier One threat to national security. However, as Donohue observed, what constitutes a national security issue "can be moulded to fit the moment."[605] Hence, despite cyber operations on foreign actors not being the main purpose of the 1994 law upon its adoption, such operations, if conducted today, could be conducted using this legal basis. While it is difficult to imagine the GCHQ hacking into a foreign government's confidential documentation for espionage purposes in the early 2000s (so a straightforward state-on-state offensive espionage operation), and much easier to imagine the GCHQ hacking into the electronic devices of an overseas-based private individual, suspected of being a terrorist threat to the British state (so a counter-terrorism defensive operation), clearly, the ISA 1994 provides the legal basis for both operations. Although no such official information exists – but nor does any information that disproves it - it could be speculated that the UK indeed performed cyber espionage on foreign states in the early 2000s. Research has not managed to identify when the UK first started relying on section 7 of the ISA 1994 for offensive cyber operations on foreign states, but in late 2013, the then defence secretary Philip Hammond admitted that the UK was "developing a full spectrum military cyber capability, including a strike capability", the first time any country admitted to having offensive cyber capabilities publicly.[606] Considering that it was precisely in 2013 that the first EU Cybersecurity Strategy came out, observing the gaps in the capabilities of some of the MS,[607] the fact that the UK was publicly acknowledging its very advanced cyber offensive capabilities at the exact same time was an indication of the role the UK would play in shaping the EU regulatory agenda (as seen in Sections 3.3.1.2. through 3.3.1.2.C)i)).

More recently, with the establishment of the National Cyber Force (NCF) in 2020, it was revealed that the UK was a "world-leader on offensive cyber operations, with GCHQ pioneering

[605] Donohue Laura K, 'Criminal Law: Anglo-American Privacy And Surveillance' 96 Journal of Criminal Law and Criminology 1059, 1155.
[606] UK Ministry of Defence, 'New cyber reserve unit created' (*GOV.UK*, 29 September 2013) <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit> accessed 31 January 2024.
[607] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 5.

the use and development of these cyber techniques".[608] Under the IPA 2016's section 229, it is the Investigatory Powers Commissioner that is responsible for the key statutory powers for performing offensive cyber operations.[609] The official institutionalisation of the National Cyber Force eradicates any doubts as regards the technical and legal capabilities of the UK to perform offensive cyber operations. As will be seen in Chapters V and VI, Italy and Bulgaria's have not taken any similar steps and it will be a long time before either puts forward the idea of developing and offensive cyber capabilities center. With this, the UK has once again proven not only its advanced capabilities, but also that it has clearly applied for a leadership role in cybersecurity internationally as one of few states with such a body. On this particular issue, it is clear that the EU was crippled in a way by Brexit, addressed in Section 4.3. as it meant that it lost access to these vital UK capabilities.

4.2.2. WannaCry UK?

Even though devices-related legislation might have been developing well, a gap remained in the UK legal system covering the vulnerabilities of the CI sectors from cyberattacks. In their Written Evidence in 2016, Google, Microsoft, Yahoo, Twitter and Facebook argued that the draft IP Bill failed to provide statutory provisions on "the importance of network integrity and cyber security".[610] The major consequences of the lack of legislation covering network integrity and cyber security was evidenced by the WannaCry ransomware attack of May 13th 2017 which hit an enormous amount of computers around the world, causing unprecedented consequences.[611] It was also the first major cyberattack on a CI sector – the NHS – that went public in the UK. The virus hit devices using Windows XP – an outdated and unsupported version of Microsoft software, highly vulnerable to attacks - a fact of which the NHS was aware.[612] Not patching

[608]GCHQ, 'National Cyber Force transforms country's cyber capabilities to protect the UK' (19 November 2020) <https://www.gchq.gov.uk/news/national-cyber-force> accessed 31 January 2024.
[609] HC Deb, 19 May 2021, cW.
[610] UK Parliament Public Bill Committee, *Investigatory Powers Bill. Written evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc and Yahoo Inc (IPB 21)* (Session 2015-16) para 31.
[611] 'Massive ransomware infection hits computers in 99 countries' (*BBC News*, 13 May 2017) <https://www.bbc.com/news/technology-39901382> accessed 21 December 2023.
[612] 'NHS was repeatedly warned of cyber-attack, says Fallon' (*BBC News*, 14 May 2017) <https://www.bbc.com/news/uk-39912825> accessed 21 December 2023.

systems was the reason why the NHS fell victim of the attack and one of the reasons why all 200 audited NHS trusts post-WannaCry failed the NHS Digital's cybersecurity assessment.[613] Medical records were affected and could not be accessed. No information if patients' lives were in danger because of the system failure was made public but considering that medical emergencies are not a rare occurrence, it is safe to assume a certain level of damage did occur. It is important to add that the issue with hacking medical records is far from new. It was already subject of discussion in the UK back in 1991 when the "unpleasant aspects of these new systems of technology" were acknowledged in relation to hacking into hospital computers.[614] Yet, 26 years later the WannaCry attack caused major disturbances and a halt to the work of the NHS. This attack further validated Google & co.'s warning and confirmed the need for a NIS Directive-like law also in the UK: even though the UK's framework was advanced to the point of regulating offensive cyber capabilities, regulating the cyber resilience of the CI sectors was inexistent, which highlights the role the EU had for the development of the UK regulatory regime to cybersecurity. It is also a clear indication that the EU had the potential to lead in an area where the international community (as seen in Chapter II), where also the single MS are represented, struggled to advance a regulatory approach to malicious cyber operations on the CI sectors.

4.2.3. The institutional infrastructure pre-NIS

Whilst much of the information in this sub-section has already been touched upon elsewhere in this Chapter, it is necessary to summarise it here for clarity and comparability with the Italy and Bulgaria in Chapters V and VI. As opposed to those states, in the UK the institutional infrastructure of cybersecurity has not been laid in a legislative measure, but rather in the strategies. Prior to the transposition of the NIS Directive the institutional infrastructure was very simplistic. The Centre for the Protection of National Infrastructure (CPNI) (now closed), accountable to the Director of MI5, provided advice on reducing the vulnerability of

[613] House of Commons Committee of Public Accounts, *Cyber-attack on the NHS. Thirty-Second Report of Session 2017–19* (28 March 2018) 10.
[614] *HL Deb 04 June 1991 vol 529 col 535*.

organisations operating in the CI sectors.[615] In 2016, the National Cyber Security Center (NCSC) was established within the GCHQ, and has since led the protection of these sectors' IT networks.[616] A potential overlapping of the NCSC and the CPNI frameworks was raised as an issue, but never addressed substantially.[617] The GCHQ continues to have a crucial role for conducting cyber defensive and offensive operations as the body responsible for performing EI operations since (at least) 2001. When the NCF was established in 2020, it took over offensive responsibilities. However, the NCF *is* part of GCHQ, as well as MI6, the Ministry of Defence and the Defence Science and Technology Laboratory, making it a joint intelligence and defence partnership.[618] Compared to the other case studies, this institutional infrastructure looks simplistic, yet it is effective and not unnecessarily burdensome in terms of who does what - which is what was observed in Italy and Bulgaria prior to the implementation of the NIS Directive (as will be seen in Sections 5.3.1.3. through 5.3.2.1. for Italy and 6.2.5. for Bulgaria) – another matter on which the EU's regulatory role was needed to polish institutional discrepancies.

4.2.4. Transposing the NIS Directive into national law

The transposition of the NIS Directive was seen as an important and welcomed step towards securing the CI sectors in the UK. It was introduced in the UK legal system with NIS Regulations 2018, a statutory instrument made under Section 2(2) of the European Communities Act 1972.[619]

---

[615] 'National Protective Security Authority Official Website' <https://www.npsa.gov.uk/about-npsa> accessed 15 January 2024.

[616] National Cyber Security Centre, 'Official website' <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> accessed 28 august 2023.

[617] Meha Shukla, Shane D. Johnson and Peter Jones, 'Does the NIS implementation strategy effectively address cyber security risks in the UK?' (2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)) 1, 6.

[618] 'Official NCF website' <https://www.gov.uk/government/organisations/national-cyber-force> accessed 21 December 2023.

[619] European Communities Act 1972 section 2 (2) Subject to Schedule 2 to this Act, at any time after its passing Her Majesty may by Order in Council, and any designated Minister or department may by regulations, make provision—(a)for the purpose of implementing any Community obligation of the United Kingdom, or enabling any such obligation to be implemented, or of enabling any rights enjoyed or to be enjoyed by the United Kingdom under or by virtue of the Treaties to be exercised ; or

The National Security Secretariat, which "provides coordination on security and intelligence issues of strategic importance across government",[620] acknowledged that the CI sectors' regulatory landscape was "mixed",[621] and that the NIS Regulations would "introduce an effective cyber security regulatory regime", a consistent approach and levelled-up standards.[622] The UK Parliament had an overall positive opinion on the role the NIS Regulations would play in the UK system.[623] Their added value manifested in the "more robust regulatory framework" for many CI sectors, specifically with the mandatory incident reporting for operators, and the "higher benchmark for cyber risk management" they would set for the designated sectors.[624] This proves that despite constantly challenging the need of an EU regulatory approach, the UK considered the NIS Regulations as a vital element in its cybersecurity legal framework. It also underscores the role of the EU as a cybersecurity regulator capable of guiding its MS on how to tackle cyber threats more efficiently.

The NIS Regulations list only five out of the seven sectors – Energy, Transport, Health, Drinking water supply and distribution, and Digital infrastructure. Banking and Financial market infrastructures are not included.[625] At the same time, other CI sectors identified in the UK prior to the adoption of the NIS Directive – chemicals, civil nuclear, communications, defence, emergency services, food, government, space – were not included in the scope of the Regulations, prompting the Parliamentary Joint Committee on the National Security Strategy to admit that the NIS Regulations are not a "silver bullet" because of their limited scope, lack of expertise to "provide credible assurance of operator's efforts" with regard to some of the designated national competent authorities and fragmented responsibilities distributed to

---

(b)for the purpose of dealing with matters arising out of or related to any such obligation or rights or the coming into force, or the operation from time to time, of subsection (1) above ; and in the exercise of any statutory power or duty, including any power to give directions or to legislate by means of orders, rules, regulations or other subordinate instrument, the person entrusted with the power or duty may have regard to the objects of the Communities and to any such obligation or rights as aforesaid. (…)

620 'Official National Security Secretariat website' <https://www.gov.uk/government/organisations/national-security/about> accessed 21 December 2023.

621 Cabinet Office National Security Secretariat, *Cyber Security: Critical National Infrastructure inquiry, Written evidence for the Joint Committee on the National Security Strategy* (17 January 2018) para 39.

622 Ibid para 40.

623 The Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure Contents* (19 November 2018) Conclusions and Recommendations para 10.

624 Ibid Conclusions and Recommendations para 10.

625 NIS Regulations 2018, Schedule 1, Designated Competent Authorities.

government, administrations and regulators.[626] The Joint Committee also expressed doubts that the Regulations would be sufficient to achieve cyber resilience in all CI sectors.[627] That said, the May 2020 Post-Implementation Review of the Regulations had an overall positive view of their effectiveness as progress has been made and the necessary action had materialised in a reduction of risks.[628]

The following Sections 4.2.4.1. to 4.2.5. will provide a brief overview of the technical details in the NIS Regulations, following the structure of the other case studies.

4.2.4.1. Definitions

Although key concepts such as cyber security, cybercrime, computer network exploitation, active cyber defence, cyber threat were identified only with the 2016-2021 Cybersecurity Strategy,[629] other terms such as cyber espionage, cyber terrorism or cyber warfare have not been unpacked to provide the British understanding of them. The NIS Regulations also did not offer such definitions. In this, the law is very different from the Bulgarian transposition law, the Bulgarian Cybersecurity Act 2018, which did incorporate definitions of key terms (Section 6.3.1.). There is also difference with the Italian way of drafting the transposition law, as, even though the latter did not include these terms either, prior strategies had done so (see Sections 5.3.1.1. and 5.3.1.2.) – whereas in the UK, as observed in Section 4.2. above, this was not the case. The NIS Regulations hence did not fill a gap, which, however, might have been intentional. An unclear interpretation of key operations such as state-led cyber espionage or cybercrime for instance is less restrictive when in the position of the performer of such operations. As seen in Section 4.2.1.3C)i), the UK has been an offensive power for decades.

[626] The Joint Committee on the National Security Strategy, Conclusions and Recommendations, paragraph 11.
[627] Ibid, Conclusions and Recommendations, paragraph 11.
[628] Secretary of State for Digital Culture Media and Sport, *Post-Implementation Review of the Network and Information Systems Regulations 2018* (May 2020) 5.
[629] HM Government, *National Cyber Security Strategy 2016 - 2021* 74.

4.2.4.2. The new institutional infrastructure

A) National competent authorities (NCA) and single point of contact (SPOC)

Like Bulgaria and Italy, the UK also preferred a sector-by-sector and decentralised approach for identifying the NCA (see Section 3.3.1.1.A).[630] Further fragmentation, however, was observed due to the different powers England, Wales, Scotland and Northern Ireland have in the UK. The department of Finance of Northern Ireland for instance, was chosen for the Energy sub-sectors of Electricity, Oil and Gas, the Rail and Road Transport sub-sectors, the Health sector and the Drinking water supply sector. The last two observed even further decentralisation as England, Scotland and Wales all attributed different NCA in the face of the respective sectorial Ministers. The Water and Air Transport sub-sectors, as well as the Digital Infrastructure sector were the only ones where the NCA was picked at UK-level, with the Transport Secretary of State and the Office of Communications chosen as the respective NCA. Soon after choosing these entities, it was revealed that some of them did not have the necessary experience to conduct cybersecurity regulatory tasks and there were even cases when they were not willing to accept regulatory responsibilities.[631] Inconsistency in the decision-making process on appropriate security measures of the NCAs was also an issue, especially in the case of cross-sector services,[632] and so was their different levels of preparedness and cyber capability know-how.[633]

In terms of incident reporting to the NCA, the UK's approach was different from the EU's. The latter's "without undue delay" (as seen is Section 3.3.1.1.A)) became "without undue delay and in any event no later than 72 hours" in the UK NIS Regulations.[634] Interestingly, the 72 hours timeframe was required by the GDPR 2016's Article 33, *Notification of a personal data breach to the supervisory authority*.[635] This alignment of legislative measures is not accidental as the UK Parliament probably saw into the possibility of a cyberattack against an OES that could also lead to a leak of personal data – for example a hospital handling medical records. Aligning two

[630] NIS Regulations 2018, Column 3, Schedule 1.
[631] Shukla, Johnson and Jones 1, 4.]
[632] Ibid 4.
[633] Ibid 7.
[634] Legislative decree 65/2018 Reg. 11 (3) (b) (i).
[635] General Data Protection Regulation 2016 Article 33 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55 (…).

or more pieces of legislation that could potentially be triggered by a cyberattack could smooth out the notification process removing ambiguity in interpreting which law should be abided by and when exactly the reporting of an incident should occur. By including the 72 hours therefore, the UK once again demonstrated its high level of preparedness, as opposed to the Italy and Bulgaria which have taken completely different approaches (as will be seen in Sections 5.4.2.1. and 6.3.2.4. respectively). The timeframe represented also an EU-level gap that was filled by the NIS2 Directive 2022, which included the same timeframe for incident reporting like in the UK (see Section 3.3.1.1.C)).[636]

As regards the appointment of the single point of contact (SPOC) the Regulations listed the GCHQ as the responsible body.[637]

B) Operators of essential services (OES)

The UK identified 470 OES, positioning itself at second place compared to Bulgaria's 185 and Italy's 553.[638] These numbers were expected to be different as, because of the nature of the EU law in question – the NIS *Directive*, each MS could decide which sectors to include in the scope and how to identify OES.

C) CSIRT

The GCHQ was also listed as Computer Security Incident Response Team (CSIRT).[639] Effectively, however, it is the NCSC performing these functions, as the latter is the UK's cybersecurity agency, institutionalised under the GCHQ umbrella. As opposed to Italy and Bulgaria, which have chosen their respective CSIRTs as the bodies to be notified in case of incidents (Sections 5.4.2.3.A) and 6.3.2.4. respectively), this was not the case in the UK. The CSIRT would in fact have to be contacted by the NCA when an OES or DSP has notified them

[636] NIS2 Directive 2022 Article 23 4. (b).
[637] NIS Regulations 2018 Reg. 4 for SPOC.
[638] European Commission, *Report on assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems* (28 October 2019) 27.
[639] NIS Regulations 2018 Reg. 5 for CSIRT.

about an incident,[640] providing therefore for a two-step approach to incident handling. A similar approach was observed also in Italy, and the related hurdles will be seen in Section 5.4.2.3.A).

4.2.5. Summary

Sections 4.2. through 4.2.5. discussed the evolution of the UK's regulatory approach to device-related use and misuse. Even though the framework was developed enough to tackle concepts such as DDoS attacks, or the performance of computer network exploitation/EI and interception operations on foreign-based targets – and to an extent that leaves way behind the other two case studies - the introduction of the NIS Regulations filled a major gap as none of the already existing pieces of legislation had addressed the importance of cybersecurity in the CI sectors, thereby demonstrating both the importance of the EU regulating in an area of crucial relevance for cross-border *security*, as well as evidencing why having an EU legal approach to the topic outweighed a single MS-based one. On this, in fact, it was the UK that lagged behind Italy, as the later adopted its first cybersecurity of the CI sectors-related legal measure back in 2013. Despite Brexit, the NIS Regulations were adopted and were followed through with implementation and continuous work towards their update. The following section will discuss their evolution post-Brexit, as well as the overall relationship EU-UK since 2020 to access the role Brexit has had on the development of the EU cybersecurity regulatory regime.

4.3. Brexit

This sub-section will analyse the impact Brexit has had on the development of the UK cybersecurity regulatory regime. As a non-member state, "freed" from the institutional law-making at EU level requiring the input of 27 other MS, the UK will now have to adapt to the reality of being a single state trying to regulate the many different aspects of cyberspace. This sub-section will briefly discuss the status of EU law in the UK since the UK left the EU, scholarly analysis on what Brexit could mean *in practice* for said partnership, and the relevant bi-lateral documents signed by the UK and the EU parties and what they mean for the future

[640] Ibid Reg. 5 (2) (c).

partnership as regards cybersecurity. The final sub-sections will discuss the effect Brexit has had on the development of the NIS Regulations regime as well as the UK's international posture in terms of the applicability of international law to cyber operations. The UK's attribution capabilities will finalise the analysis, putting the last piece in the UK cybersecurity regulatory puzzle into place.

Section 4.3.5. then concludes by considering what Brexit has meant for the development of the EU cybersecurity regulatory regime considering it lost a MS with a high level of legal preparedness and technical and operational knowhow, and indeed one of the key MS that helped shaped the basis of the EU regulatory agenda as we know it today (as observed in Sections 3.3.1.2. through 3.3.1.3.).

4.3.1. EU law in the UK post-Brexit

Before delving into the important documents regulating the post-Brexit UK-EU's relations, it is important to provide a short overview of the status of the EU law in the UK legal system post-Brexit. The European Union (Withdrawal) Act 2018 states that EU laws already adopted by the UK will remain in the latter's legal system as "retained EU law".[641] As de Mars observed that "scrapping" retained EU law would lead to "unimaginable holes in the UK legal framework" and undermine the principles of legal certainty and legitimate expectations".[642] Regardless, the status quo is that the NIS Regulations continue to be enforced despite Brexit.

4.3.2. UK-EU relations: the reality

Scholarly work has agreed that a continuous cooperation between the UK and the EU, post-Brexit, is mutually beneficial.[643] Many have argued that on different security fronts, such as

[641] European Union (Withdrawal) Act 2018 Article 7.
[642] Sylvia de Mars, *EU law in the UK* (OUP 2020) 119.
[643] Ian Walden and Johan Michels, 'Going it alone? UK cybersecurity regulation post-Brexit' 2 International Cybersecurity Law Review 1, 24.

defence-industrial projects,[644] joint research initiatives,[645] defining security norms,[646] even important informal networking within the EU cyber-experts' world,[647] both the EU and the UK will suffer because of Brexit. Scholarship, however, is divided on who has lost more. Wall argued that Brexit would make the UK more vulnerable to attacks against its critical infrastructure.[648] Lavorgna pointed out that the UK will be in the "more isolated position" compared to its neighbours and will lose influence over and access to a "transnational cooperation".[649] Brexit, she argued, will likely lead to a decrease in international influence and soft power which might have negative effects on the prevention, investigation and prosecution of cyberattacks.[650] Sweeney and Winn went further and stated that in all aspects of internal and external security the UK is at a greater risk.[651] On the other side, according to Carrapico *et al*'s views, Brexit will have a more negative impact on the European internal security in relation to cyber issues, as the UK's influence and contribution to the development of the EU's general cyber-related policies will be lost.[652] Wall also pointed out that the UK has been "a leader in defining security norms".[653] Brexit, Porcedda further argued, will come at the expense of the EU because the latter will lose its advanced cyber capabilities.[654]

Security practitioners also weighed in on the matter: Andrew Parker, then head of MI5, stated in 2018 – without specifically naming cyber operations – that cooperation between the UK and "European intelligence services" was "more operationally vital than ever before".[655] This comes

[644] Simon Sweeney and Neil Winn, 'Do or die? The UK, the EU, and internal/external security cooperation after Brexit' European Political Science 237, 242.
[645] Ibid 246.
[646] David S. Wall, 'Policing Cybercrime in the EU: Shall I Stay Or Shall I Go?' [2016] 78 British Society of Criminology Newsletter 1, 3.
[647] Templeton and Dewar.
[648] Wall 5.
[649] Anita Lavorgna, 'Brexit and Cyberspace: Implications for Cybersecurity' in Carrapico Niehuss and Berthélémy (ed), *Brexit and Internal Security Political and Legal Concerns in the Context of the Future UK-EU Relationship* (Palgrave Macmillan 2019) 114.
[650] Ibid 116.
[651] Sweeney and Winn 247.
[652] Helena Carrapico, Antonia Niehuss and Chloé Berthélémy (eds), *Brexit and Internal Security: Political and Legal Concerns on the Future UK-EU Relationship* (Palgrave MacMillan 2019) 29.
[653] Wall3.
[654] Maria Grazia Porcedda, 'Brexit, Cybercrime and Cyber security: From 'Block Opt-Out' to 'Creative Opt-Ins' in the AFSJ and the Internal Market?' in Carrapico Niehuss and Berthélémy (ed), *Brexit and Internal Security Political and Legal Concerns in the Context of the Future UK-EU Relationship* (Palgrave Macmillan 2019) 108.
[655] Ewen MacAskill, 'MI5 chief: UK and EU intelligence sharing 'never more important'' (*The Guardian*, 13 May 2018) <https://www.theguardian.com/uk-news/2018/may/13/uk-and-european-intelligence-more-vital-than-ever-warns-m15-head> accessed 24 December 2023.

with the caveat that the intelligence capabilities of no EU MS, nor the EU itself, equal those of the UK,[656] and the UK has never relied on the EU for its cybersecurity objectives.[657] Even so, in 2019, Ciaran Martin, then NCSC CEO, said with confidence that post-Brexit cooperation with the "European partners" would continue.[658] He, however, had also previously stated that Brexit will "not have an impact" on the bilateral cooperation because "very little" of what NCSC did depended on EU law and EU competences. He insisted "productive" relationships with other EU countries such as France have not suffered at all because of Brexit.[659] While that might be true, bilateral relations are different from sharing a platform where intelligence was shared by 28 members, 28 intelligence agencies, 28 cybersecurity authorities, as while still a MS, the UK shared and had access to a large volume of classified threat intelligence information with both EEAS's INTCEN and the other MS.[660]

To sum, clearly, cooperation was - and is - considered vital for the UK. Focusing on who has lost more is arguable, and, as evidenced, depends on the specific issues scholars and practitioners analysed – capabilities, policies, legal frameworks, politics. For instance, Carrapico *et al*'s argument might be true for more generic cyber issues such as cross-border cybercrime, bank ransomwares, fraudulent online operations, which fall within the domain of Europol's European Cybercrime Centre, but it is not entirely true for the internal market-related issues. As seen in Sections 3.3.1.2. through 3.3.1.2. C)i) – the UK has been firmly against more integration and a more cyber-powerful EU, specifically as it came to the development of the body of law, namely the NIS Directive. Mr Martin's statement also deserves attention as it demonstrates and confirms two things seen in the abovementioned Sections from Chapter III – one, that the UK has always preferred to work bilaterally with the other EU countries with advanced capabilities, and two – that strengthening the EU-level response has never been a priority. Post-Brexit, however, as seen throughout Chapter III, there has generally been more agreement among the MS and the EU NIS

[656] Ioannis L. Konstantopoulos and John M. Nomikos, 'Brexit and intelligence: connecting the dots' 16 Journal of Intelligence History 100, 104.
[657] Tim Stevens and Kevin O'Brien, 'Brexit and Cyber Security' 164 The RUSI Journal 22, 29.
[658] Warwick Ashford, 'UK committed to working with EU cyber security partners' (21 February 2019) <https://www.computerweekly.com/news/252458102/UK-committed-to-working-with-EU-cyber-security-partners> accessed 15 January 2024.
[659] Vivienne Clarke, 'Brexit 'will not impact' UK-EU co-operation on cybersecurity' *The Irish Times* <https://www.irishtimes.com/business/technology/brexit-will-not-impact-uk-eu-co-operation-on-cybersecurity-1.3682697> accessed 31 July 2022 .
[660] HM Government, *The future relationship between the United Kingdom and the European Union* (July 2018) para 102.

body of law has been consistently growing. At the same time, the update of the NIS Regulations in the UK is still ongoing, potentially signalling a stronger EU post-Brexit, whose leadership in cybersecurity has been endorsed by its MS.

4.3.3. UK-EU relations: important documents

Although UK and EU cooperation in cyberspace has not been among the major topics in the Brexit discussions, neither diplomatically, nor publicly,[661] regulating cybersecurity found its place in the (not legally binding) Political declaration setting out the framework for the future relationship between the EU and the UK, and the (legally binding) Trade Cooperation Agreement (TCA). A rather technical overview of the articles on cybersecurity found in these documents will be provided: this is needed both to better understand the legal obligations agreed by the two parties, and to better analyse the Brexit effects on cybersecurity cooperation and future relations between the EU and the UK.

The Political declaration set very clearly that "a broad, comprehensive and balanced security partnership" should be established on various topics including cyberattacks.[662] The two parties also agreed that they "should exchange intelligence on a timely and voluntary basis" on cyber threats, with such information to contribute towards a "shared understanding" of the security environment in Europe.[663] This timely and voluntary exchange should also be "reciprocal" and includes incidents, techniques, origin of the perpetrators, best practices and threat analysis.[664] This is particularly important as, as seen in Section 3.3.1.2.B)i), sharing sensitive information among the EU MS when drafting the NIS Directive was among the contentious issues and the UK took a very cautious position on it. As the NIS Directive created a network of cross-border information sharing, coordination and response to malicious cyber operations, Brexit meant the end of the UK's participation in those.[665] This meant a *de facto* end of membership in ENISA,

[661] Stevens and O'Brien, 22.
[662] Political declaration setting out the framework for the future relationship between the EU and the UK (November 2019) para 78.
[663] Ibid para 103.
[664] Ibid para 108.
[665] Walden and Michels 22.

the CSIRTs network and the Cooperation Group. Hence, the Political Declaration established the possibility of participation in certain activities of the NIS Cooperation Group and ENISA, as well as a cooperation with CERT-EU.[666] The document, however, did not mention cooperation with the CSIRTs network, responsible for the development of confidence and trust between the MS, for promoting swift and effective operational cooperation and for providing support in addressing cross-border incidents – something the May Government's July 2018 report on the *Future Relationship between the United Kingdom and the European Union* did: it made clear that it is the UK that proposes to go further with a "close cooperation" with the NIS Cooperation Group, ENISA *and* the CSIRTs network.[667]

Further details as to how these bilateral relationships with the EU cyber authorities would work were provided in the TCA, Part Four, Title II, which regulates the relationship of the two parties as regards cybersecurity and it largely replicates what appears in the Political declaration.

Article 705 regulates the "voluntary, timely and reciprocal basis to exchange information on tools and methods, such as techniques, tactics, procedures and best practices, and on general threats and vulnerabilities" between the national UK computer emergency response team, so the NCSC, and CERT-EU. This does not mean, as Walden and Michels have claimed, that the NCSC and CERT-EU would cooperate in case of a cross-border incident,[668] as Article 705 implies no such thing. However, it is still questionable what the purpose of the article was meant to be, as CERT-EU is responsible for the "security of the ICT infrastructure of all Union institutions, bodies and agencies".[669] It is not, therefore, a body responsible for critical infrastructure protection, nor is the body to be contacted by private ICT companies responsible for providing services to a CI sector, nor is a cybersecurity agency, nor is the body coordinating cross-border incident response. Here it seems that what was agreed on paper proves the scholarly views which argued that the UK will be in the losing position: the agreement on information exchange put the UK in a much weaker position than when it was a MS and having free access to all this pool of data at any time.

[666] Political declaration setting out the framework for the future relationship between the EU and the UK (November 2019) para 109.
[667] HM Government, *The future relationship between the United Kingdom and the European Union* para 103.
[668] Walden and Michels 24.
[669] Interinstitutional Agreement on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) (January 2018) Article 1 2.

The TCA further confirmed that the UK could participate in activities of the Cooperation Group in relation to, among others, exchanging information on risk and incidents,[670] only if invited by the Chair of the Cooperation Group, or having requested such participation.[671] The UK Parliament's Joint Committee on the National Security Strategy had explicitly recommended that the UK maintained access at least to - what the report wrongly referred to as the "NIS Coordination Group" instead of - the NIS Cooperation Group, in order to "facilitate continued information-sharing and collaboration" with the EU MS as cyber threats know no borders.[672] Cooperation with ENISA, again only via invitation or by a UK request, was limited to participation in capacity building, knowledge and information and awareness raising and education.[673] The CSIRTs network, however, remained left out also from the TCA: a potential cooperation in case of a cross-border incident would have to be decided on an ad-hoc basis. This is important as agreeing to cooperate on everything *but* support for incident response signals mistrust between the two parties. It translates into, on one hand, the EU not being able to outright rely on the UK's NCSC's capacities and know-how when handling a cross-border incident on the critical infrastructure, and on the other, the UK not being able to outright rely on any of the MS's CSIRTs cooperation, forced to handle response to such incidents on its own.[674]

In sum, the two texts seem to confirm experts' views that the future bilateral relations between the EU and the UK will hardly find a winning party: both have lost a lot and the agreements provide for a rather weak cooperation strategy, not exemplary for two parties that used to share the same pool of sensitive data and were part of the same institutions and agencies for almost 50 years. While the UK might have always preferred to work on a one-to-one basis with the other MS, there has always been the possibility of accessing EU-level information, if needed. The one-to-one partnership with the other MS might persist now, but it cannot morph into a fast-track to

[670] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (April 2021) Article 706 1. (c).
[671] Ibid Article 706.
[672] The Joint Committee on the National Security Strategy Conclusions and Recommendations paragraph 14.
[673] Trade and Cooperation Agreement Article 707.
[674] It is important to mention that the UK continues to benefit from the second largest national group of liaison officers posted at Europol, and continues to be part of J-CAT, Europol's Joint Cybercrime Action Taskforce, and has access to data via SIENA, Europol's Secure Information Exchange Network Application. However, the information shared through these channels falls out of scope of this thesis, as both these groups' work is Europol-led and they deal with the law enforcement side of tackling cybercrime (e.g. counterterrorism in the case of SIENA and generic cybercrime in the case of J-CAT), and not cyberattacks against the critical infrastructure that might potentially have a cross-border effect, which is what the CSIRT network was created for.

EU information access. Most importantly, being left out of cybersecurity incident response support – when the EU legislation was drafted precisely because of the cross-border nature of cyberattacks on the critical infrastructure sectors and the crucial importance of EU-level cooperation when these occur – means an isolated UK having to request cooperation with the EU on an ad-hoc basis.

4.3.4. Brexit's effect on the NIS Directive

Post-Brexit, evidently, the NIS Regulations had to be amended to be compliant with the new UK regulatory framework (which could no longer cross-reference EU law that was not binding in the UK). The NIS (Amendment etc.) (EU Exit) Regulations 2019 came into force on the twentieth day after the Brexit date.[675] Similarly to the EU, which introduced its NIS2 Directive proposal in late December 2020, the UK saw the importance of updating the NIS regime to face the new threats and announced in late 2022 that it would again update its NIS Regulations.[676] Changes will comprise a broader scope to include managed service providers and other organisations that entities already covered depend on, strengthen existing incident reporting duties, and a two-tier supervisory regime for all digital service providers (DSP) – a new proactive tier "for the most critical providers" and the existing reactive supervision for all other DSP.[677] While these measures will indeed mean a better level of cybersecurity preparedness across the CI sectors, they are far from being as wide and robust as the new measures set out in the NIS2 Directive seen in Section 3.3.1.1.C). Because of Brexit, the UK will also not be able to take part in the European cyber crisis liaison organisation network (EU-CyCLONe) (as described in Section 3.3.1.1.C)), which supports the "coordinated management of large-scale cybersecurity incidents and crises at operational level".[678]

While the text of the revised NIS Regulations is still unpublished as of August 2023, its new rules will almost certainly fall short from having the same impact as the EU measures. This is

[675] The NIS (Amendment etc.) (EU Exit) Regulations 2019 Article 1 (2).
[676] NIS Regulations 2018.
[677] Department for Digital/Culture/Media/Sport, *Proposal for legislation to improve the UK's cyber resilience* (Updated 30 November 2022).
[678] NIS2 Directive 2022 Article 16 (1).

also a potential factor in the development of the UK's international cybersecurity regulatory posture – if the EU's cybersecurity framework is constantly evolving, improving, and expanding its areas of influence, how would the UK be able to challenge that and promote its own position when so obviously weaker than the EU's?

So far, it appears Brexit has had a rather negative effect on the development of the UK's cybersecurity legislative framework. Also, because the UK lost its seat at the EU negotiation table, it could no longer influence the NIS2 Directive. Considering its history and its overall approach to have the MS lead the cybersecurity field with the support of the EU and not vice-versa (seen in Sections 3.3.1.2. through 3.3.1.3.), it could be speculated that the UK would have objected some of the new provisions, for example those on the European vulnerability database. Having an EU executive agency with the manpower of 120 people staff handling such sensitive information, rather than each MS's CSIRT or national Cybersecurity Agency, would have unlikely sat well with the British delegation.

That said, it is to be seen what will happen with the NIS Regulations 2.0 in view of the Government's plan to scrap all EU retained law.

4.3.5. Brexit effect on the EU as a cybersecurity actor

4.3.5.1. Attribution

Attribution is a key element of a national cybersecurity strategy and having the capabilities of correctly attributing attacks is an immense advantage over both allies and adversaries in terms of international influence and soft power. Being the third most targeted country for the period July 2020-June 2021,[679] the UK has never been among the countries shying away from publicly attributing cyberattacks (Italy is thirteenth and Bulgaria – 66th).[680] It has also developed its own

[679] 'Microsoft Digital Defense Report ' (October 2021) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738> accessed 22 December 2023 53.
[680] Kaspersky.

position on the applicability of international law to cyber operations and cyberspace,[681] which states that a "state is responsible under international law for cyber activities that are attributable to it in accordance with the rules on State responsibility".[682] The document also mentions technical and diplomatic factors as relevant when deciding whether to attribute publicly an attack.[683] The UK has therefore been developing a "coherent approach to both theory and practice" as regards responsible state behaviour in cyberspace,[684] manifested also in a number of attributions in the last few years (as observed in Section 2.4.).

These are all attributions that have, however, been backed by allies: having partners to support attribution claims is indispensable on such a contentious – and very political - issue. While a lonely British call voicing concerns regarding a malicious foreign cyber activity would still be an important call internationally, having partners is even more important. It appears that on this, the UK has preferred the US as a partner: when other MS, and the EU itself, stayed silent, e.g. on the 2017 WannaCry attack (as seen in Sections 2.4.1. and 3.3.2.1.), the UK, together with the US did not, and attributed the attack to North Korea.[685] In April 2018 a joint UK-US Technical Alert was announced, focusing on Russian state-led operations, where NCSC's CEO Martin stated that Russia is the UK's "most capable hostile adversary".[686] Also, the NCSC accessed with "high confidence" that the Russian military intelligence service – the GRU, was "almost certainly responsible" for having conducted attacks such as the OPCW attack in spring 2018, the June 2017 NotPetya attack on Ukrainian financial, energy and government sectors, the 2016 US Democratic National Committee hack, among others.[687] More recently, in March 2022, the UK, together with "the US and other allies" (not named), pointed a finger at the Russian Federal Security Service (FSB) as the perpetrator of "historic malign cyber activity" on the UK energy

[681] United Kingdom Mission to the United Nations, *Statement to the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law to States' Conduct in Cyberspace* (GOV.UK 3 June 2021).
[682] Ibid 4.
[683] Ibid 5.
[684] Stevens and O'Brien 24.
[685] National Cyber Security Centre, 'UK supports US charges against North Korean cyber actors' (17 February 2021) <https://www.ncsc.gov.uk/news/uk-supports-us-charges-against-north-korean-cyber-actors> accessed 22 December 2023.
[686] National Cyber Security Centre, 'Russian state-sponsored cyber actors targeting network infrastructure devices' (15 April 2018) <https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices> accessed 22 December 2023.
[687] National Cyber Security Centre, 'Reckless campaign of cyber attacks by Russian military intelligence service exposed'.

sector and US aviation.[688] The latter had been targeted by different types of attacks since February 2020 till at least April 2022, when the latest NCSC update was published.[689] The UK and the US also collectively attributed the SolarWinds hack to Russia's Foreign Intelligence Service (SVR).[690] Also, as seen, the 2022 Cyber Strategy explicitly named states perpetrators of cyberattacks.

At the same time, as seen in Sections 3.3.2. through 3.3.2.3., there have been drawbacks on EU-level attribution as the MS have been struggling to agree on it. The burdensome process of adopting a common approach makes it an avenue to be circumvented by some MS, wishing to fast-forward the attribution process and take action regardless of the EU's political agenda. This should push the EU to change the status quo, with more willingness on the MS's side, as a decision taken at EU-level rather than a single MS-one has much more weight internationally.

If this status quo changes, EU membership looks to become more crucial, as the EU is trying to gain more international importance as a cybersecurity actor and regulator with its already adopted NIS and NIS2 Directives, the Cybersecurity Act 2019, the upcoming Cyber Resilience Act, and its general digital policies which are developing fast – from data protection with the GDPR, to AI regulation with the forthcoming AI Act, and pursuing its digital sovereignty agenda.

If the status quo, however, does not change, on the topic of attribution specifically – and in relation to scholarly views on the who-has-lost-more because of Brexit addressed in Section 4.3.2. above - it is unlikely that the UK will be in a losing position. It appears that the UK has always been one step ahead of the EU and it has never really sought bilateral cooperation on attribution with other MS but rather the US, indirectly casting doubts on the EU ambitions to become a cybersecurity regulator. Hence it is more likely that as a non-MS its international influence and posture do not suffer. Wall has argued that Brexit will affect also the "special

[688] Foreign Commonwealth and Development Office, 'UK exposes Russian spy agency behind cyber incidents' (24 March 2022) <https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents> accessed 22 December 2023.
[689] Foreign Commonwealth and Development Office, 'Russia's FSB malign activity: factsheet' (*GOV.UK*, Updated: 7 December 2023) <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet> accessed 22 December 2023.
[690] National Cyber Security Centre, 'UK and US call out Russia for SolarWinds compromise' (15 April 2021) <https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise> accessed 22 December 2023.

relationship" between the UK and the US.[691] Whether this is true can be evaluated only over time. However, this sub-section has shown that, despite Brexit, the UK has always shared attribution-related intelligence with the US more than with its EU partners, even when still a part of the EU. This means that at least on this front, the UK will not have lost more than the EU because it remains ahead of the EU as a cybersecurity actor, despite recent EU efforts to become a cybersecurity *regulator*.

4.4. Conclusion

This first case study analysed the UK's cybersecurity legal regime pre- and post-Brexit. As will become clear over the next two chapters, compared to the Italian and Bulgarian frameworks, and prior to the adoption of the NIS Directive, the UK had a more advanced cybersecurity legal preparedness even if it did not have a CI protection-specific law. Its framework included preventive measures on the protection from DDOS attacks and telecoms security, as well as preemptive measures on equipment interference in overseas-based devices and interception of foreign-based data. These two dimensions have singled out the UK compared to the other case studies as the latter have both focused on preventive, defensive measures in their respective regulatory frameworks.

Brexit, however, brought major change. No longer a MS, the UK is now forced to develop its cybersecurity legal framework on its own. While it has proven that it can do it well enough without the EU's input, cybersecurity's threats of today are much different from what they were twenty years ago or even five years ago. While scholarly work, as evidenced, has agreed that Brexit will cause negative consequences for both parties, it is the UK that will lose access to great amount of cybersecurity-related data and intelligence shared across the Union via ENISA, the CSIRT Network and the EU-CyCLONe . Even if it is a cyber power, with capabilities much more developed than other MS, having access to a larger pool of data is still better than not having it. Having like-minded allies when it comes to attribution, is much better than doing it alone, especially if cyber powerhouses such as Russia and China are concerned. As Porcedda

[691] Wall3.

argued, "…from the perspective of jointly achieving cyber security, any Brexit solution can only be inferior to the legal and operational status quo [of EU membership]."[692]

A win-win possibility for the future of this bilateral relationship could be if, with time, itmorphs into the UK having an ad-hoc, but unofficially permanent presence in the EU cyber authorities responsible for handling incidents on the CI sectors. It could also informally play a role if contacted by the CSIRTs network (or vice versa). This, however, depends on the political will of - mainly - the UK. Strategically, as seen, UK cyber practitioners do want to continue to cooperate. However, the political elite might direct the focus of bilateral cooperation across the Atlantic. This would be the worst case for the EU, as the latter will lose the vital input the UK authorities have and will continue to have for the development of the EU cyber knowledge and capacities, two important ingredients for a solid policy and legal frameworks. It also highlights the shortcomings of the EU as a cyber regulatory regime, based extensively on its MS's capabilities.

[692] Porcedda in Carrapico, Niehuss and Berthélémy 113.

Chapter V: Member States' legal cybersecurity frameworks: Italy

5.1.Introduction

This Chapter will focus on Italy, one of the founding members of the EU, and one that represents a medium level of cybersecurity preparedness. It will follow the way the Italian legislature has dealt with the various aspects of cybersecurity over the course of over two decades, slowly building up a legal framework able to meet the cyber challenges states meet today. In Italy, cybersecurity was identified as a fundamental challenge to the intelligence sector only in 2009.[693] In the years to follow, cyber threats were recognised as global challenge number one,[694] the biggest challenge for the contemporary state,[695] and state-sponsored.[696]

In contrast to the vast literature on the UK's cybersecurity preparedness, there is much less academic commentary on Italy's approaches to cybersecurity. This Chapter will fill this gap.

As with the previous case study of the UK, analysis of Italy will begin with "pre-NIS Directive" legislation. Sections 5.2. through 5.2.3. will examine the criminalisation of unlawful computer activity and the gradual incorporation of security-related articles for the telecommunications sector and the intelligence agencies. It will compare how Italy viewed and understood device misuse-related criminal activity to how the UK and Bulgaria did.

Section 5.3. through 5.3.3. will then delve into the two legislative "steppingstones" in the Italian framework – the Monti and Gentiloni decrees, adopted in 2013 and 2017 respectively. Despite not being primary law, and therefore not comparable to UK Acts of Parliament, Italy signalled that cybersecurity was going to become a key topic of concern in adopting these two horizontally applicable decrees, something that was clearly missing in the UK at that stage (as seen in Section 4.2.4.). Section 5.3.1.1. will address how Italy defined those key terms underpinning

[693] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla politica dell'informazione per la sicurezza)* (2009) 100.
[694] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2011) 65.
[695] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2012) 37.
[696] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2019) 18.

cybersecurity laws, its developing strategic approach, and will conclude by analysing the various bodies and institutions given cybersecurity-related powers and responsibilities through these decrees. The aim of the section is to demonstrate the Italian approach and how it compares to the other MS analysed with the ultimate aim to demonstrate what the medium level of preparedness tells about the EU efforts to regulate the field.

An analysis of the NIS transposition law, Legislative decree 65/2018, will follow in the next Sections 5.4. through 5.4.3. It will consider issues that arose around the transposition law, such as institutional hurdles, incident notification and response, which proved challenging for the Italian lawmakers, and will evaluate how the newly adopted law fit into the existing legislative framework and to what extent it complemented existing measures.

Section 5.5. will see the "post-NIS" legislative developments, namely the National Cybersecurity Perimeter, praised as "far-sighted" and one that put Italy one step ahead of its fellow MS.[697] The aim of this section is to evaluate whether Italy's efforts are equivalent to those of the UK, a state which has long maintained a comprehensive cybersecurity strategy, and whether, in the absence of the UK post-Brexit, Italy might be able to take the leadership role of shaping the EU's approach to cybersecurity.

The final section will examine how cyber defence and cyber offence have been incorporated into the Italian legal system. They fall out of the scope of the NIS Directive but deserve attention because they provide a fuller picture of the relevant adopted measures. This way, conclusions can be drawn as to whether Italy is legally prepared to tackle the many challenges of the cyber domain – and what its preparation tells about the EU's legislative efforts for cyberspace's protection more generally, especially when compared to the UK and Bulgarian approaches.

[697] 'The cybersecurity perimeter: Italy's cyber defense (Perimetro di sicurezza cibernetica: la cyber difesa dell'Italia)' (*Cyber Trends*) <https://www.cybertrends.it/perimetro-di-sicurezza-cibernetica-la-cyber-difesa-dellitalia/> accessed 19 November 2023.

5.2. The Italian legal framework pre-Monti decree and pre-NIS transposition law

As demonstrated in the previous Chapter, which analysed the UK's cybersecurity preparedness, network and information security, as well as other cybersecurity-related issues, were tackled in the MS by several different legislative measures prior to the entry into force of their respective NIS transposition laws. The same goes for Italy. This section analyses the legislative framework that existed before the NIS transposition law was introduced and will demonstrate how it shaped the current Italian legal cybersecurity system.

There is a tendency when Italian officials talk about the legislative framework for cybersecurity to refer only to *sensu stricto* pieces of legislation. While cybersecurity governance was first debated in the early 2000,[698] the DPCM of 24 January 2013 (Monti decree) is often referenced as a starting point and the DPCM of 17 February 2017 (Gentiloni decree) as the second stepping-stone when discussing cybersecurity legal texts.[699] The NIS transposition law has also been referenced as a first "piece of the mosaic of the Italian cybersecurity legislation".[700] However, these documents merely represent pieces of the puzzle, and indeed, not the first ones.

Prior to the adoption of the Monti decree and the NIS Directive, Italy had decent amount of legislation regulating various offences related to the security of network and information systems. Starting from the unauthorised access to computer systems first addressed in 1993 with the Penal Code, followed by the gradual securitisation in the telecoms sector at the beginning of the 2000s, and the strengthening of the intelligence agencies' capabilities to manage the

[698] Roberto Baldoni and Rocco De Nicola, *White paper on the Future of Cybersecurity in Italy (Il Futuro della Cyber Security in Italia)* (October 2015) 15.

[699] House of Deputies, *Bulletin of the parliamentary committees, Special Committee for the Examination of Government Acts* (XVIII Legislature, 18 April 2018), sec 13;
Senato della Repubblica (Senate) and Camera dei Deputati (House of Deputies), *Schema di decreto legislativo recante attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, Atto del Governo n.10 (Outline of Legislative decree 65/2018 transposing the NIS Directive)* 1;
Parliamentary Committee on Defence, *Study on the security and defence of cyberspace* (20 Dicember 2017) 11; A few pages later, this report correctly introduces pre-DPCM 2013 legislative measures as the setting-of-the-ground cybersecurity legislation – 14.
Banca d'Italia's report on Cybersecurity from 2018 does in fact name the respective Penal Codes in Italy and across the EU as the first steps in cybersecurity legislation – one of the few sources to do that. Banca d'Italia and IVASS, *Cybersecurity: contribution of Banca d'Italia and IVASS (Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass)* (August 2018) 18.

[700] Stefano Rossa, 'Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy' (2022) 14 Italian Journal of Public Law 426, 435.

cybersecurity risks posed to the critical infrastructure sectors a decade later, Italy, similarly to other EU MS (including the UK and Bulgaria) and the EU itself, was slowly building up a framework that was later built upon when cyber threats rose to national security threats.

5.2.1. Unlawful computer activity

In 1989, then-Minister of Justice Vassalli commissioned a group of judges, IT experts and academics to amend the Penal Code to counter the raising threat of cybercrime and also fill a legislative gap, already addressed across other EU MS like the UK (as seen in Section 4.2.1.1.).[701] As also pointed out by La Greca, Italy was approaching the issue with "some delay" compared to other states such as Denmark, Norway, Austria and France.[702] Around the same time, the Council of Europe also recommended to its member states to focus on computer-related crime such as computer-related fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of a protected program, unauthorised reproduction of a topography, and, optionally, also on the alteration of computer data or computer programs, computer espionage, unauthorised use of a computer, and unauthorised use of a protected computer program.[703] These initiatives brought to light the first concrete steps towards acknowledging the threat of malicious use of IT systems in Italy: Act of Parliament 547/1993 amended the Penal Code and introduced much needed provisions on unlawful computer activity.[704] To avoid "a real indecipherability of the

[701] Giovanni Ziccardi, *Cyber Law in Italy, 3rd edition* (Kluwer Law International e-Book January 14 2020) Section 1344.

[702] Federico Tavassi La Greca, 'The regulatory approach to cybercrime (L'approccio normativo alla criminalità informatica)' [2003] ADIR, L'altro diritto 1.

[703] The Council of Europe's Recommendations on computer-related crime recommend to the member states to take into consideration the European Committee on Crime Problems' report on computer-related crime when reviewing or initiating new legislation. Council of Europe's European Committee on Crime Problems 5.

[704] An understanding of the Italian legislative system is needed to guide the reader through the next sections. In the hierarchy of sources, the Constitution is an extra ordinem source of law and appears on the first step of the ladder. Primary law follows – here we find not only the – what would be called 'Acts of Parliament' in the UK legal system (legge ordinaria), but also legislative decrees (decreto legislativo), decree-laws (decreto-legge), abrogative referendum (referendum abrogativo), parliamentary regulations (regolamenti parlamentari), regional statute (statuto regionale) and regional laws (legge regionale). Secondary law consists of governmental regulations (regolamento governativo), among which we find ministerial decrees (decreto ministeriale, hereinafter DM), interministerial decrees (decreto interministeriale), as well as Prime Minister decrees (decreto del Presidente del Consiglio, hereinafter DPCM). As secondary sources qualify also regulatory power for local authorities (potere normativo degli

system", the Italian legislature chose to amend the Penal Code rather than to introduce a sole-standing law,[705] despite voices in favour of the latter.[706]

The new provision addressed unauthorised access to a computer or electronic systems,[707] unauthorised possession and distribution of access codes to computer or electronic systems,[708] and dissemination of programs aimed at damaging or interrupting computer systems.[709] These are very similar to those introduced with the UK Computer Misuse Act 1990 (Section 4.2.1.1.), but a peculiarity of Italy's legal practise shows that unauthorised access to a computer has been often compared to the unauthorised access to private property and private domicile[710] - which was not observed in the UK. The Italian legislator went even further and introduced other provisions which addressed unauthorised interception or interruption of computer or electronic communications,[711] installation of equipment designed to intercept, prevent or interrupt computer or electronic communications,[712] falsification, alteration or suppression of the content of computer or electronic communications,[713] interception of computer or electronic communications,[714] damage to computer or communications systems,[715] computer fraud,[716] and interception of computer or electronic communications.[717] These again remind of the UK legal framework, though the scope is different, as interception, acquisition and equipment interference – as per UK's phrasing, as seen in Sections 4.2.1.3. through 4.2.1.3.C)i) – were powers attributed to the Intelligence Agencies and the UK legislature's main concern was not single individuals performing them, as is the case with the Italian framework. Indeed, the Italian provisions aimed at criminalising illegal activity online and therefore their focus was the punishment of an

Enti locali) and regulatory authority for the public administration (potestà normativa della pubblica amministrazione). The following sections will provide a detailed examination of the Acts of Parliament, the decree-laws and the legislative decrees, as well as the governmental regulations tackling cybersecurity issues. For more details view Giovanni Guzzetta and Francesco Saverio Marini, *Lineamenti di diritto pubblico* (Giappichelli - Torino 2014) and Fabrizio Politi, *Diritto Pubblico* (Giappichelli – Torino 2010).

[705] Greca 2.

[706] Ibid 3.

[707] Italian Penal Code Article 615-ter.

[708] Ibid Article 615-quarter.

[709] Ibid 615-quinquies

[710] Greca 7 and Marco Grotto, 'Council of Europe Convention on cyber crime and its ratification in the Italian legal system' (2010) 2 Sistema Penal & Violência 1, 7.

[711] Italian Penal Code Article 617-quarter.

[712] Ibid Article 617-quinquies.

[713] Ibid Article 617-sexies.

[714] Ibid Article 266-bis

[715] Ibid Article 635-bis.

[716] Ibid Article 640-ter.

[717] Ibid Article 266-bis.

individual found to have breached the law. Moreover, they focused on the misuse of a single computer rather than the computer as part of an interconnected system,[718] as at the time wide-spread viruses were a rarer occasion than today. Granularity, such as origin or purpose of the attack, whether it was conducted by an Italian national or a foreigner acting outside the territory of the state, whether it was politically or ideologically motivated, was not present at this early stage.

5.2.2. Securitisation in the telecommunications sector

Security of systems was addressed again nearly ten years later. With the DPCM of 16 January 2002 on the IT security of the telecommunication services of the public administration, the latter were instructed to tighten their information security levels and to equip themselves with minimal security preparedness.[719] The fact that Italy adopted legal provisions regulating these two sectors puts it among the better prepared states in terms of security preparedness, as it articulated the possibility of intrusion into the public sector through its telecommunication services in the early era of cyber threats. At that stage, the UK had not done the same yet, as we saw in Section 4.2.1.2.

The DPCM also laid the groundwork for the transposition of the EU Directive on a common regulatory framework for electronic communications networks and services (Framework Directive), adopted in 2002, which was transposed into the national system via Legislative decree 259/2003, the Italian Electronic Communications Code. The Code set requirements for companies providing public communication networks or electronic communication services accessible to the public to adopt measures in order to "achieve a level of network security adequate to the existing risk, and to guarantee the continuity of the provision of services on these networks" and also to contact the Ministry of Economic development in case of a breach of security.[720] This particular legislative act is of crucial importance for the development of cybersecurity legislation, because it also provides the definition of "electronic communications

[718] Grotto 2.
[719] DPCM 16 January 2002 Recitals.
[720] Legislative decree 259/2003 Article 16-bis (2) a), b).

networks", which is the basis of the NIS Directive (as addressed in Section 3.3.1.1.A)) . It also confirms the tendency seen across MS, including the ones evaluated in this thesis, that this sector was one of the first to embrace cybersecurity and the need for a legal framework to help mitigating malicious attacks.

Telecoms security was subsequently touched upon with Act of Parliament 155/2005, named "Urgent measures to combat international terrorism". Spataro observed that it was introduced as a consequence of the terrorist attacks in Madrid in March 2004 and London in July 2005.[721] Article 7-bis, *Electronic security*, enhanced the telecommunications legislation and addressed its importance for critical infrastructure. It stated that "the body of the Ministry of Interior responsible for the security and regularity of telecommunications services ensures the IT protection services of computerised critical infrastructure sectors of national interest".[722] This demonstrates that back in 2005, when "cyber" was not a buzzword or a hot political topic, Italy was amongst the states focused upon possible cyberattacks targeting the telecommunication services of CI sectors. More importantly, Italy was introducing legislation, whose roots were found in the realisation that there were vulnerabilities stemming from the digitalisation of the CI sectors and that the telecoms sector could have become the weak spot of protecting these sectors from intrusions online. On this, the UK legal framework did not present such granularity in addressing the issue of the telecoms security, as said framework followed the developments required by the EU without going further (as seen in Section 4.2.1.2.). Similar was the case for Bulgaria (Section 6.2.2.). Without going too much off topic, it is clear that in terms of securitisation of the telecoms sector therefore there was ample scope for the EU to move forward. This led to the adoption of the European Electronic Communications Code in 2018,[723] which has not been discussed in detail in this thesis because of the completely different scope.

5.2.3. Securitisation in the intelligence sector

[721] Armando Spataro, 'Security policies and fundamental rights (Politiche della sicurezza e diritti fondamentali)' Speciale Questine Giustizia: Terrorismo internazionale Politiche della sicurezza Diritti fondamentali 167, 178.
[722] Act of Parliament 155/2005 Article 7-bis.
[723] Directive 2018/1972 establishing the European Electronic Communications Code (Recast).

The security framework of the CI sector in cyberspace was also slowly taking shape in Italy around this time. After the telecoms sector, the intelligence sector was another one to adopt cybersecurity measures. The legislative act in question was Act of Parliament 124/2007, named "Intelligence system for state security and new intelligence regulations". The important cybersecurity provisions to the Act of Parliament 124/2007 were introduced as amendments by Act of Parliament 133/2012 and the reason was technological advancements: the intelligence agencies had to be equipped and prepared to meet the new security threats as national IT security's importance had risen.[724]

In line with the new provisions, the PM was assigned the power to instruct the Security Intelligence Department (*Dipartimento Informazioni per la Sicurezza*, hereinafter DIS), established within the Presidency of the Council of Ministers, via *direttive*,[725] to strengthen the protection of physical and non-physical critical infrastructure with a special focus on cybersecurity and information security.[726] New tasks were attributed to the DIS, one of which was to coordinate research activities aimed at strengthening cybersecurity and information security at national level.[727] Additional measures were adopted on the institutional relations between the Government and the Parliament, adding to the already existing obligation for the former to send the latter, at the beginning of every year, a Written Statement on the information security policies of the previous year, the additional obligation to also attach an annex on all cybersecurity and information security-related activities regarding the protection of physical and digital critical infrastructure.[728]

These measures clearly could not be compared to the way the UK had regulated its Intelligence Agencies, which were attributed very vast powers in cyberspace as early as the beginning of the 2000s (as observed in Sections 4.2.1.3. through 4.2.1.3.i)). This clearly indicates a lower level of legal preparedness as compared to the UK. Here it needs to be noted that despite these evident

[724] Gino Scaccia, 'Intelligence and state secrecy in law no. 133 of 2012 (Intelligence e segreto di Stato nella legge n. 133 del 2012)' Editoriale Scientifica 585, 585.
[725] The instrument used is called "*direttiva*", which has a meaning completely different from the EU directives and the two are not related or connected in any way. The meaning of *direttiva* here is more in the sense of *instructions* in English. The *direttive* are issued in the form of *DPCM*s or other sources of law; a *direttiva per se* is not a source of law in the Italian system. The concept finds its legal basis in article 5 para 2 a) of Act of Parliament 400/1988 according to which the Italian PM directs to the Ministers political and administrative directives, as well as those related to the general policy of the Government.
[726] Act of Parliament 124/2007 Article 1 (3-bis).
[727] Ibid Article 4 (3) d-bis).
[728] Ibid Article 38.

differences between the MS' level of preparedness, there was little scope for the EU to act as, evidently, the roles and responsibilities of the MS' Intelligence Agencies were closely related to national security, an area which the EU has no competence over.

5.3. Adoption of decreto Monti and decreto Gentiloni

In 2010 the Parliamentary Committee for the Security of the Republic published a report on cyber threats relevant to national security which provided an overview of the then geopolitical environment and how it applied to cyberspace.[729] It summarised the main state-sponsored threats happening at the time, which saw Russia, China and the US as lead actors and demonstrated how Italy was responding to that international environment. Despite the abovementioned legislative steps, Italy was lagging behind with no cybersecurity strategy or an agency responsible for tackling cyberattacks targeting Italian infrastructure, and the report recommended that the Government filled this gap,[730] while at the same time it provided a classification of the different types of attacks.[731] This report, however, was "largely ignored"[732] and defining the legal concepts of critical elements applicable to cyberspace required other legal measures to be adopted. Worth mentioning is that experts insisted systematically on the need for a cybersecurity agency throughout the years[733] (which only came into being in 2021 with Act of Parliament 109/2021 and will be addressed below).[734]

Only in 2013 – with DPCM of 24 January 2013 - did Italy begin to slowly strengthen its legislative framework with *sensu stricto* cybersecurity-related measures by introducing some initial legislative steps and identifying the key differences between the various types of cyber threats (as will be seen, the Italian taxonomy analysed in Section 5.3.1.2. is similar to – and was

[729] Parliamentary Committee for the Security of the Republic, *Report on cyber threats relevant to the national security, Doc. XXXIV n. 4* (2010).
[730] Ibid para 52.
[731] Ibid para 17.
[732] Melissa Hathaway and others, *ITALY CYBER READINESS AT A GLANCE* (Potomac Institute for Policy Studies November 2016) 4.
[733] 1. Marco Angelini, *Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness* (CIS Sapienza 2013) 60.
2. House of Deputies, *National cybersecurity, experts hearing (Sicurezza nazionale cibernetica, audizione di esperti)* (16 Ottobre 2019).
[734] Act of Parliament 109/2021 Article 1.

one of the main inspirations of - the one used in Sections 2.3. through 2.3.4.). Italy was thus moving hand-in-hand with the EU who also adopted its first Cybersecurity Strategy in 2013, which put forward the proposal for the NIS Directive (Section 3.2.1.). By that time, the UK was light years more advanced, as it has not only had a legal basis for performing cyber offensive operations abroad for over 20 years, but it was officially publicising performing them (as seen in Section 4.2.1.3.C)i)).

5.3.1. Decreto Monti

The DPCM of 24 January 2013, or the so called "decreto Monti",[735] the first legislation horizontally applicable to all critical infrastructure sectors[736] (as opposed to sectoral legislation), was a major leap forward for the development of the Italian legal framework. A real change in the approach to tackling cybersecurity was needed, which would include organisational and cultural aspects.[737] It is safe to conclude that decreto Monti did bring a real change in approach because it addressed the topic of cybersecurity in its entirety and in a consistent and substantial manner. Baldoni *et al* in fact recognised decreto Monti as "extremely important in the national cyber panorama" because it came at a time when very little was being done and in a rather unstructured way in terms of addressing cyber threats.[738]

While a significant step in the right direction, Setola observed that decreto Monti came almost ten years later than similar pieces of cyber legislation did in other countries.[739] No reference was made to specific countries, but the UK would have certainly made that list, as what we would today define as offensive and defensive cyber operations, defined as 'equipment interference' under British legislation, had had legal basis since the early 2000s (see details in Sections 4.2.1.3. through 4.2.1.3.C)i)). That said, as we saw in Section 4.2.4., the UK legal framework did

[735] Decreto Monti was named after the then Prime Minister Mario Monti.
[736] DPCM (PM Decree) 24 January 2013 Article 1 (1).
[737] Banca d'Italia and IVASS 13.
[738] Roberto Baldoni, Rocco De Nicola and Paolo Prinetto, *The Future of Cybersecurity in Italy: Strategic Project Areas (Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici)* (Laboratorio Nazionale di Cybersecurity; CINI - Consorzio Interuniversitario Nazionale per l'Informatica, January 2018) 17.
[739] Roberto Setola, 'Istituito il 'Nucleo per la Sicurezza Cibernetica' (Establishment of the Cybersecuirty Unit)' II Sicurezza e Giustizia 8, 9.

not have a cybersecurity law comparable to decreto Monti, as the scope and focus of the abovementioned UK laws was not specifically cybersecurity (or equipment interference), but more generally the powers attributed to the British Intelligence Agencies. Setola's observation therefore is true when it comes to the general preparedness and understanding of the cyber domain and its potential uses, but is not strictly applicable to the legislative framework.

5.3.1.1. Definitions underpinning cybersecurity laws

Despite the criticism, decreto Monti still had an added value from a cybersecurity legislative measures perspective. Most importantly, it included a list of definitions, which illustrates how Italy saw the cyber threats phenomena back in 2013. Together with the obvious definitions of cyberspace and cybersecurity, Article 2 elaborates on what constitutes threat, event, alarm and crisis in cyberspace.[740] Their inclusion in the Italian legal framework is important, as having additional granularity on attacks' *nature*, on how they can evolve, demonstrates an understanding of the threat landscape. According to decreto Monti:

- cyber threat is "a set of conducts that can be carried out in cyberspace or through it, in order to damage it or its elements, which manifests in the actions of **single individuals or organisations, whether state or not, public or private** [*emphasis added*], aimed at the undue acquisition and transfer of data, their modification or unlawful destruction, or at damaging, destroying or hindering the regular functioning of network and information systems or their elements";
- cyber crisis is "a situation in which a cyber event takes dimensions, **intensity or nature likely to affect national security** [*emphasis added*], or a situation which cannot be

[740] DPCM 2013 Article 2 (1) h) cyberspace is "the set of interconnected IT infrastructures, including hardware, software, data and users, and the interaction between them";
i) cybersecurity is "a condition which ensures the protection of cyberspace by adopting suitable physical, logical and procedural security measures when facing events of a voluntary or accidental nature, consisting of the acquisition and the undue transfer of data, in their illegitimate modification or destruction, or in the damage, destruction or blocking of the regular functioning of network and information systems or their elements";
m) cyber event is "a significant event, of voluntary or accidental nature, consisting of the acquisition and the undue transfer data, in their illegitimate modification or destruction, or in the damage, destruction or blocking of the regular functioning of network and information systems or their elements";
n) cyber alarm is "a warning of a cyber event, to be evaluated in order to activate planned response measures".

tackled by the single competent administrations in the ordinary way, but by taking a coordinated inter-ministerial decision"[741]

The fact that the Italian lawmakers considered the possibility of a state-sponsored interference, detailing it in a legislative measure back in 2013, demonstrates attentiveness to this issue. On this, Italy took a similar stance to the UK (as seen in Section 4.2.). The difference with the UK is that it had incorporated these observations in legally-binding measures, not a strategy, as was the British case. The Italians also recognised the likelihood of a cyberattack threatening national security. While this undoubtedly is due to the political narrative at the time, when concepts like "cyberwar" were used rather often and not always correctly, and the possibility of another state targeting CI sectors in cyberspace was presented as a major threat, acknowledging the possibility still presents a step forward for the development of a solid legislative framework for cybersecurity and cyber defence.

5.3.1.2. The new strategic approach

Similarly to the UK's, Italy's cybersecurity strategy has evolved at the same pace as the legislation. Analysis of the strategy is thus needed to provide a complete overview of the cybersecurity state of play and its evolution. The two documents released after the adoption of the DPCM 2013 - the National Strategic Framework for Cybersecurity and the Italian Cybersecurity Action Plan of December 2013 – were the first Italian cybersecurity strategic compass. Although Setola criticised the Framework as being a missed opportunity to call for a better cooperation between the stakeholders,[742] the document was of crucial significance for the development of a general understanding how the cyber domain could be maliciously exploited. Chapter 1 of the Action Plan addressed the evolution of threats and public network and information systems' vulnerabilities, providing a list of definitions supplementing those found in the DPCM 2013. The types of threats were classified based both on their *nature* and the *damage*

[741] Ibid Article 2 (1) l), o).
[742] Roberto Setola, 'Il Quadro Strategico Nazionale per la Cybersecurity (The National Strategic Framework for Cybersecurity)' I Sicurezza e Giustizia 26, 27.

they have caused – and so, for the first time in Italy, definitions of cybercrime, cyberespionage, cyber terrorism and cyber warfare were included in an official document:

- cybercrime is "all malicious activities with a criminal intent carried out in cyberspace such as swindles or internet fraud, identity theft, stealing of data or of intellectual property";

- cyber espionage is "improper acquisition of confidential or classified data, not necessarily of economic or commercial value";

- cyber terrorism is "ideologically motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organisation";

- and cyber warfare is "activities and operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance".[743]

This taxonomy was in part used as the basis of the taxonomy on cyber threats observed in Sections 2.3. through 2.3.4. But these definitions present some gaps: apart from cyber terrorism, which is "ideologically motivated", none of the other three concepts encompasses the political aspects. As seen throughout Chapter II, cybercrime and cyber espionage for instance can indeed be politically motivated and there have been many examples of such state-on-state operations. Moreover, as often happens, although definitions exist, their understanding and interpretation continue to differ among experts: during a joint hearing of the Defence and the Constitutional Affairs Parliamentary Committees in March 2017, Antonello Soro, the then-President of the Authority for the Protection of Personal Data stated that cyberwarfare-type of attacks have increased by 117%, data "substantially confirmed" by the Bank of Italy.[744] The same number for cyberwarfare attacks appeared also in the Defence Committee Study of 2017, clarifying that the number was comparing year 2016 with 2015.[745] While these reports were produced by trustworthy sources, there is little doubt that the conclusions were inaccurate. As Sections 2.3.3.

[743] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *National Strategic Framework for Cybersecurity (Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico)* 13. Translation taken from the English version of the document.
[744] House of Deputies, *Joint hearing of the Constitutional Affairs and Defence Committees, 7 March 2017* (XVII Legislature) 4.
[745] Parliamentary Committee on Defence 21.

through 2.3.3.2.A) account, it has now been largely agreed that the only cyber *use of force* operation to date has been the US-Israeli-sponsored Stuxnet worm targeting Iran. Most of the other state-on-state operations (such as the DNC hack, the WannaCry ransomware, the SolarWinds hack, cyberattacks against the health sector during the COVID pandemic, Russian-sponsored cyberattacks against Ukraine and so on) analysed across Chapter II have never crossed the threshold to *use of force*. Hence had the data on cyberwarfare provided by the Italian authorities been true, we would have seen cyberwars escalating to kinetic wars very easily. If what was meant were low intensity state-on-state cyberattacks, not amounting to actions equivalent to a *use of force*, these cannot be labelled "cyberwar". Despite years of having a definition of cyberwarfare, Italian experts therefore still could not differentiate between the different types of attacks. This potentially provides scope for the EU to act and adopt its own definitions on the spectrum of cyberattacks which are then endorsed by the MS – but this has not happened to date (this issue is further discussed in Section 7.2.2.).

Despite this misalignment of interpretations, around the same time, the UK, which had clearly identified state-led cyberattacks as a cause of concern, had not adopted such clear-cut definitions. Whilst the reason for this could be to preserve some level of flexibility, Italy's explicit definitions can only contribute to consolidating an EU-level definitions of cyberattacks. Not having adopted such definitions at national level means, in practice, having no way of contributing to this essential EU – and consequently – international debate. A debate of key importance for an EU with ambitions to become a cybersecurity regulator.

5.3.1.3. The institutional architecture

The institutional architecture needed to protect the CI sectors from cyberattacks was set in decreto Monti in 2013. It identified the responsibilities for the various actors, with the aim to reduce vulnerabilities, prevent cyber risks, prepare to respond "in a timely manner" to assaults and to restore "immediately" the targeted system's functionality.[746] In this framework, cybersecurity tasks were spread across a number of roles and bodies such as the PM, who

[746] DPCM 2013 Article 1 (1).

became responsible for adopting the cybersecurity strategic framework,[747] the Interministerial Committee for the Security of the Republic (*Comitato Interministeriale per la Sicurezza della Repubblica*, hereinafter CISR), which would advise the PM on the strategic framework, and the Military Councillor of the PM, within which was established the Cybersecurity Unit (*Nucleo per la Sicurezza Cibernetica,* hereinafter NSC). The "complex crisis management structure" caused lack of coordination, "especially in the case of a wide-ranging crisis".[748] Complexity and fragmentation, however, were unavoidable, as new roles and responsibilities had to be assigned to different bodies to build their knowhow and operational capacity to protect against attacks on Italian CI sectors.

A) The Cybersecurity Unit (NSC)

The NSC deserves to be analysed because of its newly assigned key role in the cybersecurity institutional infrastructure. A political body, the NSC's members included the Military Councillor as chair, and representatives of the Information Security Department (Dipartimento delle informazioni per la sicurezza, DIS), the External Intelligence and Security Agency (*Agenzia informazioni e sicurezza esterna,* AISE), the Internal Intelligence and Security Agency (*Agenzia informazioni e sicurezza interna,* AISI), the Agency for Digital Italy and the Ministries of Foreign Affairs, Internal, Defence, Economic development and Economy and finance.[749] Its main task was to support the PM for the prevention of and preparation for cyber crises,[750] meaning that the NSC would have a decisive part when a cyber event would evolve into a national security threat. A Unit within the NSC was to be responsible for alerting and responding to cyber crises 24/7,[751] a responsibility Setola wrongly described as a novelty of the Gentiloni decree.[752]

[747] Ibid Article 3.
[748] Samuele De Tomas Colatin, *National Cybersecurity Organisation: ITALY* (NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2020) 8.
[749] DPCM 2013 Article 8 (2).
[750] Ibid Article 8 (1).
[751] Ibid Article 9 (2) b).
[752] Andrea Chitarro and Roberto Setola, 'Nuova Direttiva per la protezione cibernetica e la sicurezza informatica (New Directive on cybersecurity and information security)' II Sicurezza e Giustizia 28, 28.

To this – rather political – task was added a technical role: the NSC was also appointed as a point of contact for private bodies providing essential services to the public via computer or electronic systems to communicate to the NSC every "significant violation" of the security or integrity of their information systems.[753] The immaturity of the cybersecurity framework transpires from this provision as the text did not specify a timeframe within which such reporting had to take place, or how "significant violation" was to be measured, despite these two elements being crucial for clarifying how the incident-reporting mechanism should work in Italy. Moreover, considering its membership, it appears that the NSC is a political body with no technical expertise. The fact that it was attributed a responsibility of such calibre shows that there was a huge gap in the Italian preparedness as – evidently - there was no other body that would better fit the profile for the job. Choosing the NSC for this role was acknowledged to be a controversial move, as, according to Setola, the Computer Emergency Response Team (CERT) should have been assigned the role.[754] This would have been difficult, however, as, at the end of 2013 it was reported that the CERT was still not operational and its role in the national cybersecurity strategy was unclear.[755] This makes the NSC hybrid in nature, with tasks of rather different nature and scope. The effectiveness of performing its tasks, however, could only be evaluated over time.

5.3.1.4. Decreto Monti post-adoption analysis

In addition to the criticism related to choosing the NSC as the body handling cyber crises and incident notifications, the entirety of the decree was criticised for being "cumbersome" because of the many subjects it addressed.[756] Experts argued that decreto Monti did not fill the knowledge gap, as well as legal and technical knowhow and capabilities gap between Italy and states such as the UK.[757] Alessandro Pansa, the Director of the DIS, also admitted that although decreto Monti had indeed created more awareness among users and the public administration, the post-adoption

[753] DPCM 2013 Article 11 (1) a).
[754] Setola, 'Istituito il 'Nucleo per la Sicurezza Cibernetica' (Establishment of the Cybersecuirty Unit)' 8, 8.
[755] Angelini 58
[756] Setola, 'Il Quadro Strategico Nazionale per la Cybersecurity (The National Strategic Framework for Cybersecurity)' 27 and Baldoni, Nicola and Prinetto 17.
[757] Setola, 'Il Quadro Strategico Nazionale per la Cybersecurity (The National Strategic Framework for Cybersecurity)' 27.

analysis showed that it did not help to overcome the "critical aspects" that the strategic information systems kept identifying, in that they were still undergoing persistent cyberattacks.[758] Not surprisingly, he identified responding to serious attacks as one of these critical aspects, adding that there was no set team to deal with them, but only some experts working for the Ministries of Interior and Defence "running around" to find the proper solutions.[759] Despite, therefore, being a good first step, setting the frame, political agenda and institutional responsibilities for cybersecurity, decreto Monti had to go through a review to address the valid concerns raised by experts. This happened four years later, with the adoption of decreto Gentiloni.

5.3.2. Decreto Gentiloni

Decreto Monti's successor, decreto Gentiloni,[760] was adopted on 17 February 2017. Similar in content and structure to the 2013 decree, it helped with the understanding and assigning of responsibilities, as four years had helped crystalise the cyber domain's peculiarities and the different roles public bodies should have. One of the main objectives was to "improve and simplify" decreto Monti's institutional-structural challenges.[761] Indeed, the Gentiloni decree brought a clear line of command.[762] It simplified the decision-making process and crisis management structure, "streamlining both ordinary and emergency procedures".[763] The PM, the CISR, and the Director of DIS all had their roles strengthened and better defined in cases of national cybersecurity emergencies.[764] The PM, when having to protect national security in cyberspace, was attributed the power to summon the CISR.[765] The latter was also given a much

[758] House of Deputies, *Joint hearing of the Constitutional Affairs and Defence Committees, 14 June 2017* (XVII Legislature) 5.
[759] Ibid 5.
[760] Decreto Gentiloni was named after the then PM Paolo Gentiloni.
[761] DPCM (PM Decree) 17 February 2017 Recitals.
[762] Stefano Mele et al, 'Cybersecurity: the role of engineers and the possible synergies between Government, Industry and University (Cyber Security: il ruolo degli Ingegneri e le possibili sinergie tra Governo, Industria e Università)' (*Radio Radicale*, 6 December 2019) <https://www.radioradicale.it/scheda/592274/cyber-security-il-ruolo-degli-ingegneri-e-le-possibili-sinergie-tra-governo-industria> accessed 28 November 2023.
[763] Colatin 17.
[764] House of Deputies, *Joint hearing of the Constitutional Affairs and Defence Committees, 14 June 2017* 5.
[765] DPCM 2017 Article 3 (1).

more important role during cyber crises,[766] in line with article 7-bis of the Decree law 174/2015, which identifies in the CISR as the body responsible for managing national security emergencies.[767] The DIS's role was also reinforced – it was put at the centre of the national cybersecurity governance and took over the management of the NSC.[768] While this move was in line with the overall cybersecurity strategy Italy was following, it should be clarified that the DIS is, after all, a political body, part of the Presidency of the Council of Ministers, and not an operational body with IT staff. This could once again potentially lead to lack of expertise and create knowhow hurdles, and in case of a cyberattack against a CI sector, it could lead to a slow response and recovery procedures. Hurdles like this were in fact among the elements that led to the EU deciding to take the lead in cybersecurity regulation. An attack with a cross-border impact would have caused major damage if there were uncertainties regarding the steps to take and bodies to contact in the other MS (as seen in Sections 3.3.1. thorough 3.3.1.2.A)i)).

5.3.2.1. The NSC's new status

With decreto Gentiloni, the NSC saw the Deputy Director of the DIS as president.[769] Possibly to address the shortcomings stemming from the political dimension of both DIS and NSC, technical support for the crises' management was to be provided by the National CERT (CERT-N) and the Public Administration CERT (CERT-PA).[770] Undoubtedly in preparation for the implementation of the NIS Directive into Italian national law, decreto Gentiloni included provisions which imposed obligations for operators of essential services (OES) and digital service providers (DSP), as identified by the NIS Directive, to also report incidents to the NSC were included.[771]

To evidence its importance in the framework of Italian cybersecurity preparedness, the Unit was convened after both WannaCry and NotPetya attacks in May and June 2017 respectively to

[766] Ibid Article 4 (1) a).
[767] Decree law 174/2015 Article 7-bis (5) established that the CISR, upon being summoned by the PM, would have the power of proposal, deliberation, and being consulted during crisis situations involving national security.
[768] DPCM 2017 Article 8 (1).
[769] Ibid Article 8 (2)
[770] Ibid Article 10 (3)
[771] Ibid Article 11 (1).

discuss their impact and necessary response.[772] The Unit was summoned also in spring 2020 because of the Coronavirus pandemic, after a failed attempt to infiltrate the Spallanzani hospital for infectious diseases in Rome,[773] as well as after the SolarWinds software hack in December 2020.[774] More recently, the Israel-Palestine conflict resulted in the Unit being convened once again in early autumn 2023.[775] Research has not been able to identify the outcome of these meetings as there has been no public record of them. Considering the significance of the security issue and potential treatment of sensitive or confidential information, some level of restrictions around the role of the NSC in relation to cyber crises is due, yet an official report of some sorts could have been published, not least to demonstrate the Italian preparedness to respond, or even contribute to an EU-level response. As seen in Section 3.3.2.1. the MS have different methods of identifying a perpetrator of an attack and their forensics capabilities vary. In an EU dependent on its MS which hold the keys and need to agree unanimously about a potential response, if Italy wants to raise its level of preparedness (as will be demonstrated in Sections 5.5. through 5.5.3.), a more active role on the EU decision-making table is needed.

Sections 5.4.2.3.A) and 5.5.1.2. will further address the role of the NSC in light of transposing the NIS Directive and the adoption of the National Cybersecurity Perimeter as its hybrid nature with political and technical responsibilities makes it a unique body with no counterpart in the other analysed MS. To reiterate, Italy could use this fact to its advantage and have a more active role in shaping the EU regulatory framework in both the NIS and cyber diplomacy fields.

5.3.2.2. Testing the legal framework

[772] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2017) 5.
[773] P. Sol., 'Coronavirus, hackers attack on Spallanzani in Rome. The Prosecutor's Office investigates (Coronavirus, attacco hacker allo Spallanzani di Roma. Indaga la Procura)' (*Il Sole 24 Ore*, 1 April 2020) <https://www.ilsole24ore.com/art/coronavirus-attacco-hacker-spallanzani-roma-indaga-procura-roma-ADtLHTH?refresh_ce=1> accessed 28 November 2023.
[774] 'The hacking of the solarwinds platform: the Cyber Security Unit is summoned (Hackeraggio della piattaforma solarwinds: riunito il Nucleo per la Sicurezza Cibernetica)' (*Italian CSIRT*, 24 December 2020) <https://www.csirt.gov.it/contenuti/hackeraggio-della-piattaforma-solarwinds-riunito-il-nucleo-per-la-sicurezza-cibernetica-ne01-201224-csirt-ita> accessed 18 Novembre 2023.
[775] Gabriele Carrer, 'Crisis in the Middle East at the center of the Cybersecurity Unit meeting (Crisi in Medio Oriente al centro della riunione del Nucleo per la cybersicurezza)' (*Formiche.net*, 21 Ottobre 2023) <https://formiche.net/2023/10/nucleo-per-la-cybersicurezza-medio-oriente/> accessed 18 November 2023.

Cybersecurity – and more precisely, cyber espionage – shot to the spotlight in late 2017, when malware was discovered to have been used to spy on leading Italian political figures and Governmental institutions.[776] The incident indicated that Italian authorities failed at the technical level to intercept even dated examples of malware. This intrusion did not stop Antonino Moscatt MP from claiming only a few months later that, considering the amount of legislation Italy had on the matter, it had a certain cyber advantage compared to other states.[777] While true compared to states such as Bulgaria (as will be seen in Sections 6.2. through 6.2.6. analysing its pre-NIS Directive regulatory framework), it could have hardly been true compared to countries like the UK (as seen in Sections 4.2.1. through 4.2.3.). Moreover, the mere existence of legislation does not mean it is properly enforced: this incident demonstrated that despite the public administrations being covered by the legal framework, the cybersecurity requirements under the latter were evidently not implemented. This once again demonstrates that the effectiveness of the law is measured by its enforcement, not by its mere existence. Clearly, when the national law, however, derives from EU law, it is the EU that monitors implementation and enforcement. This once again shows that in an area of cross-border relevance the EU's role as a regulator is key in achieving a harmonised level of resilience across all MS: in the case of a MS with weak regulatory framework and lack of proper national cybersecurity laws' enforcement (and, as a consequence, preparedness), an attack against a MS, could have easily caused damage to other MS too.

5.3.3. Summary

Before the entry into force of the NIS Directive transposition law, the Italian cybersecurity legal framework consisted of a range of provisions scattered across different pieces of legislation covering various criminal offences online, as well as two administrative acts explicitly

[776] Redazione ANSA, 'The Occhionero siblinges, between masonry and finance (I fratelli Occhionero, tra massoneria e alta finanza)' (*ANSA*, 12 December 2017) <https://www.ansa.it/sito/notizie/cronaca/2017/01/10/chi-i-sono-i-fratelli-occhionero-gli-spioni-tra-massoneria-e-alta-finanza_d4a65eeb-3cd1-4b59-a223-92555cc77728.html> accessed 28 November 2023.
[777] House of Deputies, *Joint hearing of the Constitutional Affairs and Defence Committees, 14 June 2017* 9.

addressing cybersecurity - the 2013 and 2017 PM decrees, defining the cyber threat landscape and the institutional architecture.

The adopted legislative measures discussed in Sections 5.2. through 5.3.3. contributed to the development of the public opinion on cybersecurity, of building of knowhow among Italian experts, of widening the overall cybersecurity knowledge and narrowing the competence gap across various public and private actors. Politically and strategically, Italy was on the right road to tackle the challenges of the cyber domain. However, at institutional level, reality appeared different: the architecture, where various bodies were attributed different responsibilities, complicated the process of reporting incidents, and preventing and recovering from or responding to cyberattacks. The legal framework might have been in place, but it was too burdensome – the adoption of the NIS Directive was needed to bring some clear institutional architecture, to synthesise all existing legislative measures into one legally binding piece of legislation and to streamline the reporting mechanism. The need for a strong EU regulatory in cybersecurity has thus been evidenced by the limitations of the Italian framework.

5.4. Transposing the NIS Directive into national law

This section will explore the Italian transposition of the NIS Directive which took the form of a legislative decree. Legislative decree 65/2018 came into force on 24 June 2018, over a month after the transposition deadline of 9 May 2018 (achieved only by a few MS, among which the UK). The text is almost identical to the NIS Directive's and no major surprises appear in terms of innovative provisions: the decree is not too ambitious but at the same time is a major step forward, which, for instance, the UK NIS Regulations (discussed in Sections 4.2.3. through 4.2.5.) were not due to the already mature legal framework. The new legislative decree's provisions (as described in 3.3.1.1.A)) included improving national cybersecurity risk management and incident reporting, defined risk, incident and incident handling, encouraged a strengthened cooperation at national and EU level, posed obligations on identification of OES and DSP and the follow-up technical requirements for these bodies, and established the Italian Computer Security Incident Response Team (CSIRT), the single points of contact (SPOC) and

the NIS authorities. Achieving a high level of network and information security was finally required by a "primary law".

In his introductory remarks, Legislative decree 65/2018's Rapporteur Stefano Buffagni MP claimed that the economic impact of cybercrime had increased five-fold between 2013 and 2017 and that "[i]t is known that cyber incidents are a daily cause of serious economic damage and that the risks of cybercrime increase exponentially due to increasingly sophisticated and unpredictable threats".[778] Leaving aside that both "economic damage" and "cybercrime" are used as very generic terms, the statement is still missing the point of the NIS Directive because its objective is not to protect *all* of the existing network and information systems in the MS from *any* cybercrime (as seen in Section 3.3.1.1.A)). Its scope encompasses *only* the OES operating in the CI sectors and DSP[779] and their task to secure a high level of network and information security of their systems through which they provide their services which are vital for the society. These are those organisations, whose disruption of systems would have major impact on the state in terms of geographical impact or number of people impacted.[780] Therefore, not all cyber-intrusions against any hospital network would qualify as the type of "incident" found in the NIS provisions, nor will all hospitals be covered despite all falling within the health sector. Arguably, the vagueness of the MP's words might have been intentional as not to create confusion around the topic, but being vague when discussing the scope and subject matter of a law is rarely desirable, especially by the MP vested as a Rapporteur of the file.

This and other peculiarities of Legislative decree 65/2018 will be assessed in Sections 5.4. through 5.4.3. with the aim of drawing a conclusion on whether the EU law was correctly transposed in Italy, whether the changes it brought contributed to better legal, institutional and technical preparedness, and whether a more coherent and streamlined cooperation with the other MS was achieved when having to deal with cross-border cyberattacks. Ultimately, the analysis will allow to consider where the EU sits as a regulator, more specifically its role in overcoming the MS' national frameworks' limitations.

---

[778] House of Deputies, *Bulletin of the parliamentary committees, Special Committee for the Examination of Government Acts* 13.

[779] While it was wrongly reported during a Parliamentary debate that public administrations fall within the scope of the NIS Directive (House of Deputies, *Bulletin of the parliamentary committees, Special Committee for the Examination of Government Acts* (XVIII Legislature, 8 May 2018) 10), Italy is one of the countries, which, as oppose to Bulgaria, has left them out of the scope of Legislative decree 65/2018.

[780] Legislative decree 65/2018 Article 5 and NIS Directive 2016 Article 6.

5.4.1. Definitions

Similarly to the UK transposition law (see Sections 4.2.4. through 4.2.5.), the Italian transposition law did not provide additional definitions to those included in the original NIS Directive. Considering the pre-NIS legal framework in Italy, the missing presence of these terms in a legally binding document was a gap that remained unfilled. As will be seen in Section 6.3.1., Bulgaria's transposition law incorporated a much broader list of definitions than the EU law's, including cyber threat, cyber incident and cyber defence. On this front therefore, Italy decided that its already adopted position on interpreting the various cyberattacks was sufficient.

5.4.2. The new institutional infrastructure

5.4.2.1. National competent authorities and single points of contact

As previously mentioned, it was argued that Italy needed a national agency for cybersecurity, similarly to other MS such as Germany, France or the Netherlands, that would benefit coordination activities as well as fast decision-making process when facing a threat.[781] The idea of having a centralised approach was echoed a few years later in Italy, by pointing out that taking a decentralised approach contrasts the very nature of the digital revolution and in order for a state to be efficient in cyberspace it needs to act quickly, with a clear line of command.[782] Attacks unfold quickly and a "strong coordination" between threat detection and response was needed.[783] The apparent lack of security experts in Italy further required a centralised approach.[784]

Despite these observations, Italy adopted a sectorial and decentralised model when appointing the competent authorities,[785] tasked to monitoring the application of the NIS Directive in the Member State.[786] These were the Ministry of Economy and Finance (for the banking and

[781] Angelini 60.
[782] Baldoni and Nicola 15.
[783] Ibid 60.
[784] Ibid 60.
[785] Roberto Setola and Giacomo Assenza, 'Ricepimento della Direttiva NIS sulla cyber-security delle reti (Transposition of the NIS Directive)' IV Sicurezza e Giustizia 32, 34.
[786] NIS Directive 2016 Article 8 (2).

financial markets sectors), the Ministry of Infrastructure and Transport (for the transport sector), the Ministry of Economic development (for the energy and digital services sectors), the Ministry of Environment, together with the Regions and the autonomous Provinces of Trento and Bolzano (for drinking water supply), and the Ministry of Health, together with the Regions and the autonomous Provinces of Trento and Bolzano (for the health sector).[787] Despite the clear indications from experts that a different approach should have been taken – similarly to other MS such as Belgium, Estonia and Germany[788] - Italy chose the decentralised approach. The reasoning might have been rooted in the fact that these ministries had technical knowledge on the topic – and in the absence of a centralised Agency that deals with all-things-cybersecurity, this was the only option left.

The SPOC, on the other hand, was established within the DIS.[789] Choosing the DIS was in line with previous normative framework, e.g. the Acts of Parliament 124/2007 and DPCM 17 February 2017, which has always envisaged an important role for it in the national "cybersecurity architecture".[790] The newly acquired responsibilities for the DIS included a liaison role "to ensure cross-border cooperation" with the authorities of the other MS, the cooperation group and the CSIRT network.[791]

5.4.2.2. Operators of essential services (OES)

As per Article 5 of the NIS Directive, every Member State had to identify the OES for the seven CI sectors (as seen in Section 3.3.1.1.A)). Prior to the NIS Directive, Italy had listed four main types of CI sectors, but having four sectors might seem misleading compared to the UK's thirteen and Bulgaria's nineteen; Italy had taken a different approach, grouping different thematic sub-sectors into one main sector: Ministries, the Bank of Italy, state-owned companies

[787] Legislative decree 65/2018 Article 7 (1) a) – e).
[788] European Commission, 'State-of-play of the transposition of the NIS Directive' (7 June 2022) <https://digital-strategy.ec.europa.eu/en/policies/nis-transposition> accessed 28 November 2023.
[789] Legislative decree 65/2018 Article 7 (3).
[790] Setola and Assenza 32, 34.
[791] NIS Directive 2016 Article 8 (4) and Legislative decree 65/2018 Article 7 (4).

operating in certain sectors, public authorities.[792] The list of CI sectors in Italy was introduced via Interior Ministry Decree (*decreto ministeriale*) of 9 January 2008, which also established the National anti-crime informatics centre for the protection of critical infrastructure (CNAIPIC).[793]

With the introduction of the NIS Directive, Italy aligned the identification of the sectors to those required[794] and identified the respective OES accordingly: 465 bodies were identified in December 2018,[795] with the number rising to 553 as per a report of the European Commission published a year later.[796] The report stated that the UK had identified 470 and Bulgaria 185.[797] The list – similarly to the other MS – is of course classified, as declassifying it would reveal which bodies must be cyber-secured by law and which not.

5.4.2.3. CSIRT

The last piece of the new NIS institutional puzzle was the establishment of a national Computer Security Incident Response Team (CSIRT).

CERTs have existed in many MS before the NIS Directive – this was also the case with Italy which had CERT-N (with ten people as staff) and CERT-PA (with two full-time staff members and three tech people on temporary contracts)[798], responsible for coordinating and providing cybersecurity services to all public and private entities across the country, and for guaranteeing cybersecurity for state and local authorities. These numbers show a certain underestimation of

[792] The full list of CI sectors comprises Ministries, agencies and supervised authorities, operating in the fields of international relations, security, justice, defence, finance, communications, transport, energy, environment, health; bank of Italy and independent authorities; state-owned companies, regions and metropolitan areas covering at least 500,000 people, operating in the fields of communications, transport, energy, health and water conservation; any other institution, administrative office, authority, public or private legal person whose business is considered of national interest because of public order or security, by the Minister for the Interior or at the proposal of the prefects - provincial authorities, public security.
[793] DM Interior Ministry 9 January 2008 Articles 1 and 3 respectively.
[794] Legislative decree 65/2018 Annex II.
[795] 'Cybersecurity: Italy's steps ahead (Cybersecurity: ecco i passi avanti dell'Italia)' (*Sicurezza Nazionale*, 21 December 2018) <https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-ecco-i-passi-avanti-dell-italia.html> accessed 18 November 2023.
[796] European Commission, *Report on assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems* 27.
[797] Ibid 27.
[798] House of Deputies, *Parliamentary debate Sitting n. 734 1 February 2017* , 52.

the ever-evolving threat and an evident need for a change. They also once again confirm the role of the EU in guiding the MS towards the adoption of more stringent and harmonised rules across the MS as huge discrepancies in MS' legal preparedness – and, consequently, operational capabilities - would hardly be the way forward in an economy so interconnected as the EU MS'.

The Italian transposition law therefore established the Italian CSIRT within the Presidency of the Council of Ministers, with the two CERTs filling in on performing its tasks only before the body was officially set up.[799] This happened on 9 May 2020, almost two years after the adoption of the Legislative decree 65/2018, in accordance with DPCM of 8 August 2019, which further specified that the Italian CSIRT was established within the DIS,[800] thus adding to the political dimension of the DIS also an operational one. Both CERTs officially stopped existing and gave all their power of "proactive, reactive and incident response services" to the CSIRT,[801] a decision identified as an "important turning point".[802]

A) Incident notification and response

A key element created by the NIS Directive was the mechanism for cross-border incident notification and information sharing via the CSIRT network (see Section 3.3.1.1.A)). The UK chose the NCA to be the body that would be notified in case of incidents (see Section 4.2.4.2.A)) whereas Italy chose the CSIRT.[803] As opposed to the 72 timeframe the UK gave to the victims of attacks, the Italian framework provided for the vague wording the EU provided: "without undue delay".[804] From this transpires the level of preparedness: whilst the EU and the majority of its MS did not have the necessary practical experience with handling cyberattacks, the MS with high level of preparedness such as the UK did. Italy and Bulgaria did not (see Section 6.3.4.)

The establishment of the Italian CSIRT and its newly assigned tasks, however, created an interesting legislative dynamic as, as seen above, Italy already had a body responsible for

[799] Legislative decree 65/2018 Articles 8 (1) and (3).
[800] DPCM 8 August 2019 Article 3 (1).
[801] 'CERT Pubblica Amministrazione' <https://www.cert-pa.it/> accessed 12 August 2020.
[802] Setola and Assenza 35.
[803] Legislative decree 65/2018 Article 12 (5).
[804] Ibid (5).

incident handling and response – the NSC. According to the NIS Directive, "incident handling" means "all procedures supporting the detention, analysis and containment of an incident and the **response** thereto" [emphasis added].[805] In the Italian translation of the Directive, whose text was later copy-pasted into Legislative decree 65/2018, the word "response" is cautiously translated "*intervento*", the meaning of which is "*intervention*", not response. "*Risposta*", response, however, appears throughout prior legislation – DPCMs 2013 and 2017. Clearly, there is a difference between "*risposta*" and "*intervento*" - intervention has a different meaning than response. Not only does this create a problem with interpreting the law, but it also creates confusion regarding the competencies of the different bodies. According to the NIS Directive, the CSIRT should be responsible for responding to cyber incidents.[806] However, the Italian CSIRT is only responsible for an *intervention* in those cases, while the NSC, in line with DPCM 2017, is responsible for promoting the operational planning of the **response** to cyber crises,[807] and has a Unit that is active 24/7 "to alert and **respond** to cyber crisis situations" [emphasis added].[808] To cause further confusion, the transposition law does not mention the NSC, at least not explicitly: according to Legislative decree 65/2018 the CSIRT (which is also supposed to be operational 24/7)[809] should "promptly forward" incident notifications to "the body established within the DIS […] responsible for prevention and preparation for possible crisis situations"[810] – which is indeed the NSC. This seemingly creates a two-step incident handling system, with the first step being incident notification by the affected OES and DSP to the CSIRT,[811] second step being notification being forwarded to the NSC. The effectiveness of this system is rather questionable as it was never explained why a two-step process was created. Moreover, it does not become clear whether the CSIRT should send *all* notifications to the NSC or only the suspected crisis situations. Consequently, as both bodies have "intervention/response" duties, what remains an issue is the uncertainty regarding who does what and when. Seemingly, if the incident amounts to a crisis threatening national security for instance, the NSC would "respond", implying that the CSIRT would "intervene" in the milder cases. This is, however, speculative, as no clear roadmap was provided.

[805] NIS Directive 2016 Article 4 (8).
[806] Ibid, Annex I, (2) (a) (iii).
[807] DPCM 2017 Article 9 (2) a).
[808] Ibid Article 9 (2) b).
[809] Legislative decree 65/2018 Annex I (1) c) ii.
[810] Ibid Article 12 (6).
[811] Ibid Article 9 (2).

5.4.3. Summary

Legislative decree 65/2018 successfully transposed the NIS Directive into the Italian legal system. It set up new bodies and their respective tasks. What it appears to have failed to achieve, however, is the much-needed clarification and simplification of the institutional architecture: new and old bodies seem to have overlapping responsibilities specifically on incident response and notification procedure, which are the core of tackling cyber threats. It appears that the NIS transposition law does not build on existing measures efficiently and further deepens the institutional hurdles: the role of the NSC has not been explicitly addressed, and the PM and the CISR's tasks were only mentioned in reference to issuing cybersecurity strategies.[812] Instead, their role should have been reinforced. A systematic approach, developing a clear cybersecurity framework, was hence still missing. Here, despite the looming shadow of Brexit, the UK's transposition law did appear to complement existing legislation without creating an unnecessarily burdensome new framework for addressing cyber incidents, a task that Italy failed to achieve. A task that, however, should definitely be on the Italy's agenda when discussing the NIS2 transposition law, whose aim was precisely to iron out inconsistencies in the MS' approaches (as seen in Section 3.3.1.1.C)).

5.5. Post-NIS transposition developments

Back in 2013 it was argued that to have a solid risk framework, it is key to understand the motivation of the threat actors as well as the classification of the cyber threats, whether state-sponsored or performed by criminals.[813] It appears that after years of work on cybersecurity legislation, Italy finally realised the importance of this principle: in the aftermath of the NIS transposition law, Italy's legislation has been developing at a fast pace.

[812] Ibid article 6 (1).
[813] Angelini 56.

5.5.1. National Cybersecurity Perimeter

The first step was taken with Decree law 105/2019, converted into Act of Parliament 133/2019, entitled National Cybersecurity Perimeter, which signalled the beginning of a series of cybersecurity measures adopted through 2020 and 2021. The Perimeter focused on the most sensitive areas that would affect the national cybersecurity and that were not covered in the NIS transposition law.[814] Gennaro Vecchione, then Director of DIS, declared that these measures put Italy at the forefront of cybersecurity in Europe.[815] The new law has also been labelled a "unique and avantgarde instrument in the panorama of the various national cybersecurity frameworks".[816] Indeed, compared to both the UK and Bulgaria, Italy was ahead of them in terms of further developing its regulatory framework, which, in the UK's case had to wait for the reviewed NIS Regulations, announced in late 2022 and to be adopted sometime in 2024,[817] and in Bulgaria's case – the NIS2 transposition law, also to be adopted in 2024. The Perimeter's aim is to achieve a high level of NIS of the public administration and the national operators – public and private - providing an essential functions for the state, whose interruption of service could cause a national security threat.[818] The Perimeter did not introduce new concepts, but set the scene and timeframe for the future steps to be adopted via DPCMs, namely the choice of which exactly public administration entities and national operators would fall within the scope of the Perimeter[819] and the criteria through which they will be chosen.[820] In a way, it is similar to the revised UK NIS Regulations as both measures expand the scope of the NIS transposition laws, though the Italian Perimeter is a much more ambitious piece of legislation as its scope is much wider than the reviewed UK Regulations discussed in Section 4.3.4.

The steps that were adopted as part of the Perimeter include: DPCM 131 of 30 July 2020 (DPCM 1), which identified the entities, public and private, that fall within the Perimeter; DPCM 81 of 14 April 2021 (DPCM 2) addressed incident reporting; DPR (DPR 3) 54 of 5 February 2021

[814] Brunella Bruno, 'Cybersecurity between legislation, national interests and the market (Cybersecurity tra legislazioni, interessi nazionali e mercato)' (2020) 14 Federalismiit 10, 20.
[815] , 'The cybersecurity perimeter: Italy's cyber defense (Perimetro di sicurezza cibernetica: la cyber difesa dell'Italia)'.
[816] Rossa 435.
[817] UK Department for Digital/Culture/Media and Sport, 'The NIS Regulations 2018' (20 April 2018) <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 28 November 2023.
[818] Decree law 105/2019 Article 1 (1).
[819] Ibid Article 1 (2) a).
[820] Ibid Article 1 (2) b).

discussed the procedural framework for the procurement of ICT goods to be used on networks, information systems and IT services by the entities within the scope of the Perimeter; and DPCM of 15 June 2021, which identified the categories of these assets.[821] The last step was the adoption of DPCM 92 of 18 May 2022 (DPCM 4) which established the procedures, requirements and the terms for the accreditation of testing laboratories which will support the National Evaluation and Certification Centre. The key points addressed in DPCM 1 and 2 will be analysed below. DPR 3 and DPCM 4 will not, as they address mainly technical, organisational and structural issues which have not proved problematic from a regulatory perspective. Decree law 82 of 14 June 2021, which defined the legal status and responsibilities of the Italian Cybersecurity Agency, was not initially to become part of the Perimeter, as it "significantly reshapes the normative architecture" set by the latter,[822] but in the grand scheme of things, it fits well with the other steps and will therefore be analysed as part of this section. It also goes beyond the EU requirements signalling an ambition on the Italian side to raise its level of legal preparedness.

5.5.1.1. National Cybersecurity Perimeter: newly covered entities

Having been delayed because of the COVID pandemic, DPCM of 30 July 2020 set the criteria for the identification of the public and private entities that would be subject to the law.[823] It was again argued that the DPCM shot Italy into the forefront position, leaving other EU states behind.[824] The DPCM's scope covered the public administrations and other entities (e.g. in the interior sector; defence; space and aerospace; energy; telecommunications; economy and finance; transport; digital services; critical technologies; social security institutions and labour)[825] building on the NIS Directive's cybersecurity requirements.[826] On the point of including the

[821] Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) 3 International Cybersecurity Law Review 289, 297.
[822] Ibid 297.
[823] Stefano Mele, 'National Cybersecurity perimeter: Prime Ministerial Decree 131/2020 is taking shape (Perimetro di Sicurezza Nazionale Cibernetica: ecco come prende forma con il DPCM 131/2020)' (*Altalex*, 3 November 2020) <https://www.altalex.com/documents/2020/11/03/perimetro-di-sicurezza-nazionale-cibernetica-ecco-come-prende-forma-con-il-dpcm-131-2020> accessed 19 November 2023.
[824] , 'The cybersecurity perimeter: Italy's cyber defense (Perimetro di sicurezza cibernetica: la cyber difesa dell'Italia)'.
[825] DPCM 30 July 2020 Entities Article 3 (1).
[826] al.

public administrations, however, Italy was hardly the frontrunner as the sector was included in the scope of the Bulgarian transposition law, adopted in 2018, as will be seen in Section 6.3.2.3.. Moreover, as a reminder, public administrations were part of the proposal for NIS Directive adopted by the European Commission back in 2013 but MS with high level of preparedness, among which the UK, strongly opposed including it in the scope (as seen in Section 3.3.1.2.C)i)).

5.5.1.2. National Cybersecurity Perimeter: incident notification

DPCM 2 defined the procedures for incident reporting. It included a broadened definition which identified incident as "any event of an accidental or intentional nature that determines the malfunction, interruption, even partial, or the improper use of networks, information systems or IT services".[827] Whilst a new sanctioning regime was introduced, doubts as to its effectiveness remained. As opposed to the open-to-interpretations "without undue delay" found under the NIS Directive's Article 14 (3) and Legislative decree 65/2018's Article 12 (5), the DPCM introduced a rather strict timeline for incident reporting: within six hours for certain types of less serious attacks e.g. initial exploitation, breach of confidentiality and integrity of the systems, losses or thefts of encryption keys, unauthorised access, among others,[828] or within an hour for more serious attacks such as compromised control processes, disclosure of corrupted data, execution of corrupted operations via an ICT asset, among others.[829] Such short timelines are rather insufficient as not all security breaches will be of major concern and not all breaches would require the full attention of the notified body. Overflooding the CSIRT with incident notifications would undermine its operability and its readiness to act when needed for more serious attacks. On the matter, Schmitz-Berndt and Chiara have argued that the DPCM was rather similar to the NIS2 Directive proposal,[830] which, however, is not entirely true in view of the completely different timelines for reporting: as opposed to the DPCM's very short deadlines, the NIS2 proposal gives a 24-hour margin of manoeuvre. As this timeframe, however, was also considered "unreasonable" by the NIS2 Rapporteur Bart Groothuis, the adopted version of the

[827] DPCM 14 April 2021 Incident notification Article 1 (1) h)
[828] Ibid Annex I Table 1.
[829] Ibid Annex I Table 2.
[830] Schmitz-Berndt and Chiara 300.

NIS2 Directive introduced 72 hours timeline (as seen in Section 3.3.1.1.C)). It will be interesting to see how the Italian legislator approaches the issue when the NIS2 Directive has to be transposed.

Another issue with this DPCM 2 was the incident notification process. The not-very-effective approach chosen by previous legislative measures, and most importantly by the NIS transposition law, was still not addressed effectively. On the contrary, the multi-steps approach was chosen again: step one would entail informing the CSIRT; step two would require the CSIRT to send these notifications to the DIS, including for "activities" delegated to the NSC; step three would see the DIS transferring these notifications to the body within the Ministry of Interior responsible for security and integrity of telecommunication services, the PM or the Ministry of Economy.[831] Again, details as to what types of incidents – or all – would follow this procedure are missing. Granularity here is key as for such a three-step process to make sense, there needs to be a reason why three - as opposed to one - entities would need to be notified and involved. Moreover, it is not clear whether, in line with previous legislative measures, there is a possible step four: the NSC being summoned in case of a cyber crisis. Improvement and clarity were, therefore, hardly achieved.

5.5.2. National Cybersecurity Agency

As mentioned, Italy finally established the long-requested Cybersecurity Agency with Act of Parliament Act of Parliament 109/2021 and its tasks and functions with Decree law 82 of 14 June 2021, making it the national cybersecurity authority.[832] The hope for "rationalising" the responsibilities spread across various entities and assigning them to only one body, raised by Sciacovelli, were met.[833] Its establishment happened thanks to financing coming from the EU programme Next Generation, adopted to help MS affected by the COVID-10 pandemic.[834]

[831] DPCM 2 (Incident notification) Article 5 (1) a)-c).
[832] DPCM 14 June 2021 Cybersecurity Agency Article 7 (1) a).
[833] Piermario Boccellato, 'Interview with Prof. Annita Sciacovelli: Italy needs a public and private cyber intelligence strategy based on the Israeli model' (19 July 2021) <https://www.cybersecitalia.it/cybersecurity-annita-sciacovelli-in-italia-serve-una-strategia-di-cyber-intelligence-pubblica-e-privata-basata-sul-modello-israeliano/12835/> accessed 25 November 2023.
[834] Rossa 435.

Despite such funding available to all MS, such development was not observed in Bulgaria and, as of summer of 2023, was still not being planned.

The Agency was set as a coordinating and advisory body,[835] and as Nunzia Ciardi, current President of the Agency as of November 2023, put it – it deals with cyber resilience and its "objective is to prevent cyber threats and defend" Italy.[836] It took over the Council of Ministers and the DIS' cybersecurity responsibilities that the Perimeter had attributed to them.[837] The NSC was moved under its cap,[838] and so was the CSIRT.[839] The Agency was also given the tasks to "develop national capacities for the prevention, monitoring, detection, analysis and response, and to prevent and manage cybersecurity and information security incidents".[840] It has also become the national competent authority and the SPOC.[841] Romano sustained that the new body finally created a streamlined architecture, with fragmentation of tasks and duties were overcome.[842] Which indeed was much needed. One issue it did not fix, however, was the incident notification process, but because all the responsible bodies were moved under its umbrella, it should be expected that NIS2 transposition law offers a more streamlined incident notification process in line with the EU timelines.

5.5.3. Summary

After years of building capacity, it seems that with the National Cybersecurity Perimeter and with the establishment of the Cybersecurity Agency, Italy is heading in the right direction.

[835] Ibid 437.
[836] National Cybersecurity Agency, 'Nunzia Ciardi: The digital revolution has enormous potential. But be careful about privacy: the internet does not forget (Nunzia Ciardi: La Rivoluzione digitale ha potenzialità enormi. Ma attenti alla privacy: la rete non dimentica)' (24 Maggio 2023) <https://www.acn.gov.it/notizie/contenuti/nunzia-ciardi-la-rivoluzione-digitale-ha-potenzialita-enormi-ma-attenti-alla-privacy-la-rete-non-dimentica> accessed 25 Novemner 2023.
[837] DPCM Cybersecurity Agency Article 7 (1) h) and i) respectively.
[838] Ibid Article 8 (1).
[839] Ibid Article 7 (3).
[840] Ibid Article 7 (1) n).
[841] Ibid Article 7 (1) d).
[842] Bianca Nicla Romano, 'Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione" (The risk of "attacks" on computer systems between relevant cases, data protection and requirements for "good administration")' (2021) 3 Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico" 545, 594.

Neither the UK nor Bulgaria have progressed their legal frameworks so quickly. These steps demonstrated that officials finally realised that the subject of cybersecurity is tightly linked to national security. With stakes that high, leaving legislative gaps, unclear processes and understaffed entities was no longer an option. Yet significant gaps remained, especially in the field of incident notification. It will be seen whether the NIS2 transposition law will address them and whether Italy will align its framework with the EU one, which names only one body and a 72-hour margin for reporting.

5.6. Cyber defence and offence

Even though outside the scope of the NIS Directive, any analysis of the cybersecurity legal framework in a given state would be incomplete without presenting how cyber defence and offence are incorporated into the legislative puzzle; much like in Chapter IV, therefore, an analysis of the Italian approach to cyber defence and offence is presented. The difference is that in the UK regulatory framework the matter is found further up in the analysis (see Section 4.2.1.3.) because prior to the adoption of the NIS Directive the UK framework circled around cyber defensive and offensive operations (labelled in British legislation as ‘equipment interference’ and ‘interception of communications data’ of devices located outside the territories of the UK).

5.6.1. Cyber defence

With regards to cyber defence, Italy has acknowledged that cyberspace is the fifth domain of war.[843] The Military was one of the first governmental institutions to follow “since the beginning” how the legal framework adapted to the new battlefield domain.[844] In 2015 the

[843] Colatin 17.
[844] Ministry of Defense, ‘The role of engineers for cybersecurity - Speech by General Leverano, then Defence Deputy Chief of Staff’ (6 December 2019) <http://www.difesa.it/SMD_/Staff/Sottocapo/Messaggi/Pagine/cyber_security_convegno_Napoli.aspx> accessed 28 November 2023.

Ministry of Defence seemingly implied that Italy was developing defensive cyber capabilities,[845] and that a "Cybernetic Operations Command" was envisaged.[846] This was later confirmed with the 2017 National Action Plan,[847] which also announced the establishment of a Joint Command for Cyberspace Operations (Comando Interforze per le Operazioni Cibernetiche – CIOC)).[848] Its tasks included conducting cyber defence operations, as well as networks defence and vulnerability assessments and penetration tests.[849]

Back in 2017, it was revealed that Italy had allotted roughly 30 personnel as part of military preparedness in cyber defence. At the same time, Germany had allocated €1 billion and employed 13,500 military staff to protect state agencies and private entities.[850] Italy was also very far from being "completely efficient" in cyber defence because it failed to organise simulation exercises to check on response capabilities to cyberattacks of the CI sectors. Gori observed.[851] The lack of expert personnel is probably why the nuanced distinctions between cyberattacks often escape Italian officials, especially in terms of cyber defence preparations. Admittedly, very often the nature of cyberattacks is not easy to identify, their real damage difficult to access and their originator only presumably identifiable (as observed throughout Chapter II). This was confirmed also by the Director of the DIS Pansa, who stated that it is incredibly difficult to define which attacks amount to triggering the defence systems of the state. Identifying the attack would lead to identifying the proper response. If defence is at stake, a military action would be required, while if the attack is "non-conventional", the response could be in the hands of different bodies.[852] This again highlights the importance of the shortcoming Italy still experiences on the effectiveness of the incident response mechanism and it is an exemplary manifestation of why incident response needs to be clear: when there is no streamlined process, doubts will always exist. The difficulty in identifying the type and nature of an attack should not imply a check-mate situation where first a thorough analysis of whether

[845] Ministry of Defence, *White Paper for International Security and Defence* (July 2015) 23.
[846] Ibid 76.
[847] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *The Italian Cybersecurity Action Plan* (March 2017) 7.
[848] Ibid 12.
[849] Francesco Vestito, *Cyber Command Panel* (CyCon 2019).
[850] House of Deputies 52.
[851] Umberto Gori, *Cyber Warfare 2017. Information, Cyber and Hybrid Warfare: contents, differences, applications (Cyber Warfare 2017. Information, Cyber e Hybrid Warfare: contenuti, differenze, applicazioni)* (Franco Angeli 13 September 2018) 223.
[852] House of Deputies, *Joint hearing of the Constitutional Affairs and Defence Committees, 14 June 2017* 7.

defence is at stake is conducted, *then* assignment of the incident to the military is done, and *then* the way forward is decided. Also, here again the gap that is left at national level can – and should be – filled by the EU. As Section 3.4. described, the EU approach to cyber defence suffers from major limitations itself. However, considering the struggles Italy (and also Bulgaria, as will be seen in Section 6.5.) experience at national level, with these two states representing the majority of the MS in terms of medium and low level of preparedness, this clearly opens the door for a more active EU on the matter.

5.6.2. Cyber offence

It would be difficult to imagine that developing any kind of defensive cyber capabilities would mean they could be used merely for defensive purposes. Hence it should not be surprising that offensive cyber also came up on the political agenda when the legislature considered Italy's military preparedness in cyberspace.

During a parliamentary debate in February 2017, the case for developing offensive cyber capabilities was made.[853] But prior to conducting offensive cyber operations, there should be a legal basis – and so far no such provision is found in the Italian legal framework (as opposed to the UK one which explicitly legalises equipment interference on devices placed abroad as seen in Section 4.2.1.3.C)). Offensive cyber was also touched upon by the Defence Committee and the Bank of Italy's studies of 2017 and 2018 respectively. In the former, it was vaguely suggested that, together with the latest developments in the field of cyber defence, also cyber offensive capabilities were progressing. The words "development of capacities to conduct cyber military operations in the digital domain"[854] leave little to the interpretation. Similar text was used in the Bank of Italy's study: it underlined the importance of being up to date with existing information system vulnerabilities and the ways they could be exploited by malicious actors, because this created the possibility of advantageous defensive "proactive" operations, much more effective than the reactive operations.[855] Whichever way is chosen to describe it, having cyber offensive capabilities is incredibly advantageous for the contemporary state. If Italy aspires to become a

[853] House of Deputies, 52.
[854] Parliamentary Committee on Defence 13.
[855] Banca d'Italia and IVASS 8.

relevant actor in cyberspace, similarly to the UK, or even to take over the UK's leadership position at the EU cybersecurity negotiation table, possessing such capabilities is a must. But in the absence of a legislative basis, it is questionable how far along Italy can really go.

5.7. Conclusion

This Chapter analysed the development and evolution of the cybersecurity legislation in Italy. Prior to the adoption of the NIS Directive, the state had some sectoral legislation in place, as well as two governmental regulations, the Monti and Gentiloni decrees of 2013 and 2017 respectively. On a number of fronts such as security of the public administrations, specifying CI sectors or recognising the possibility of a foreign state-sponsored attacks, Italy was ahead of the game compared to the rest of the EU – and the other two MS analysed more specifically. The introduction of the NIS Directive into the national system, however, evidenced the profound misunderstanding and unpreparedness of decision-makers and legislators regarding cybersecurity, undermining the credibility of its legislative approach. Legislative decree 65/2018, the NIS transposition law, was introduced as a separate measure instead of building upon the existing ones, creating a mismatch between them. This contributed to discrepancies between the tasks of responsible bodies, duplication of powers, unclear procedural mechanisms to notify and respond to incidents, and created scope for possible non-compliance with the new provisions. These are some of the problems currently observed as regards the implementing process in Italy. High level of network and information security was achieved on paper, but it has not contributed enough to achieving better legal, institutional and technical preparedness. The National Cybersecurity Perimeter, announced, and the establishment of the Cybersecurity Agency, was therefore a necessary step forward. It expanded the NIS requirements to the public administration and other national operators, but did not fill all the gaps left from previous laws in terms of incident notification.

In conclusion, Italy's overall framework is still not comparable to the UK's, despite the UK's post-Brexit developments not living up to the expectations (as seen in Section 4.3.). Taking the UK's place as one of the locomotives of the EU regulatory regime did not entail Italy disagreeing

with the EU position. Impacting the EU regime is not only manifested by challenging the EU's views, but also by showcasing good practises at national level which can be replicated at EU level. Italy had the chance to do this with its Cybersecurity Perimeter, but failed to do so.

But as will be seen in the next Chapter, Italy was still ahead of Bulgaria in terms of legal preparedness. The key here is for Italy to keep the good pace and further enhance its legal approach facilitated by the NIS2 Directive and upcoming transposition law.

Chapter VI: Member States' legal cybersecurity frameworks: Bulgaria

6.1. Introduction

This Chapter will focus on Bulgaria, a relatively "new" MS, and a relative newcomer on the cybersecurity scene. Bulgaria provides a useful case study because the country had not explicitly addressed cybersecurity with a legally binding measure before the NIS Directive came into force, which makes the EU's role as a leading regulator very important in the Bulgarian developments. With its first Cybersecurity Strategy 2016 and the first cyber law – the Bulgarian Cybersecurity Act 2018 (hereinafter BCSA), Bulgaria provides for a case study of a MS with relatively low level of cybersecurity legal preparedness, especially compared to the UK and Italy.

Research has identified very little peer-reviewed literature on cybersecurity, computer security, the NIS Directive or other relevant legislation and information in Bulgaria in Bulgarian and even fewer sources in English. This Chapter will hence provide a much-needed overview and analysis of the pre- and post-NIS Directive legal preparedness in Bulgaria. Being the final MS analysed, the case study will complete the analysis of legal approaches taken across the three MS and will help finalise the concluding observations of this thesis on the role the EU is currently playing as a cybersecurity regulator.

The structure of this chapter will follow that of the other case studies: Sections 6.2. thorough 6.2.6. will provide a short overview of the broader cybersecurity preparedness pre-NIS Directive. The Sections will examine the insertion of criminal offences online to the Penal Code, and the gradual securitisation in the telecommunications sector and the public administration. Cybersecurity was occasionally addressed in various existing pieces of legislation before the BCSA came into force, but in a sparse and insufficient manner. Sections 6.2.4. through 6.2.4.2. will also discuss how key terminology was defined in Bulgaria and Section 6.2.5. will conclude with the institutional architecture that existed pre-NIS Directive. This overview will help the reader understand the reasons for Bulgaria's sluggish embrace of cybersecurity as a critical national security domain, as well as the reasons for the slow implementation of the NIS Directive, highlighting the ample scope for the EU to act and provide regulatory guidance and leadership.

Sections 6.3. through 6.3.4. will then discuss the BCSA and the fundamental changes it introduced into the Bulgarian legal system: from defining key terms such as cybersecurity and cyber defence, to assigning new responsibilities - such as fighting cybercrime, building cyber defence capabilities, working on cyber risk management - to the relevant authorities.

The analysis in Section 6.4. will then briefly examine the most devastating incident in Bulgarian history to date – the 2019 hack on the National Incomes Agency which led to a leak of the personal data of 5 million (out of 6.8 million in total) Bulgarian citizens. The hack is relevant as it showcases where the enforcement of the BCSA might have cracked and how important it is for critical sectors to adopt the required cybersecurity measures. The Chapter will finish with a discussion on cyber defence and offence (Section 6.5.) and how they are seen, understood and have developed in Bulgaria, before concluding on what the Bulgarian case study can tell us more generally about the EU's status as a cybersecurity regulator, especially compared to the more prepares states such as the UK and Italy.

6.2. The Bulgarian legal framework pre-NIS transposition law

Scholars have been encouraging the development of cybersecurity measures in Bulgaria for a decade now,[856] pointing out the lack of common principle for inter-institutional cooperation or cross-border cooperation with the EU and NATO in case of a cyberattack.[857] Others have noted that even though it was a member of NATO and the EU, Bulgaria had not learned from or taken advantage of the other member states' cybersecurity knowhow,[858] leaving scope for the EU to fill in this regulatory gap.

Back in 2012, then-President of the Republic, Rosen Plevneliev, stated that Bulgaria had "enough intelligent young people" who could be working in cyber defence. He also added that it would be "great" if NATO opened a cyber defence centre in Bulgaria because it would "position Bulgaria on the war maps of the 21st century as one of the most technologically-developed

[856] Petko Petkov, 'Cybersecurity: Emerging Characteristics and Impact on Defence' IT4SecReports 98 ICT Institute, Bulgarian Academy of Science 21.
[857] Krasimir Staikov Koev, *Increasing Cyber Security and Defense of Communication and Information Structures of the Defense Ministry and the Bulgarian Army* (Military Academy "Georgi Stoykov Rakovski" 2019) 25.
[858] Petkov 20.

countries".[859] His statement was put in rather militaristic terms and reflected the discussions that were happening at the time at international level, where the fear of cyber Pearl Harbor and cyber 9/11 were at the centre of contemporary debate. The following sections will demonstrate the President's limited foresight, as more than a decade later, the reality in Bulgaria is far removed from what he envisaged. Furthermore, as seen in Section 2.2.2.2., cyber threats in general have moved into a different direction, with cyber war having become a less pressing concern for the international community than persistent lower-level cyber incursions.

In late 2012 President Plevneliev spoke again about the importance of cybersecurity for the national security, stating that he was planning for the topic to be discussed at the Advisory Council for National Security.[860] Apparently, this remained in the 'planning' phase as Bulgaria's cybersecurity legislative framework only started developing as a separate body of law in the late-2010s and its importance for national security was disregarded for a long time.

Indeed, six years later, in preparation for the transposition of the EU NIS Directive, and in the course of reviewing the existing regulatory framework, MPs serving on different committees seemed to have contradictory background information on the existing legislation. In their respective first reading reports, the committees debating the draft bill provided a controversial analysis of Bulgaria's legal preparedness. The leading Committee on Homeland Security went as far as stating that "[c]ybersecurity is regulated in a number of laws but not in a systematic manner and does not fully meet the new challenges".[861] The Committee on Defence report reiterated that cybersecurity has been regulated by a number of laws.[862] However, this account is overly simplistic, as none of the existing laws - as will be shown below - discussed cybersecurity explicitly or sufficiently. In other words, nothing in the Bulgarian framework could be comparable to the two Prime-Ministerial decrees in Italy (as seen in Section 5.3. through 5.3.3.), or the vast investigatory powers-related legislation in the UK (as seen in Sections 4.2.1 through

[859] Iva Ivanova, 'Bulgarian hackers should work for NATO, said Plevneliev (Родните хакери да заработят за НАТО, поиска Плевнелиев)' *Newsbg 2 April 2012* (2 April 2012) <https://news.bg/politics/rodnite-hakeri-da-zarabotyat-za-nato-poiska-plevneliev.html> accessed 7 July 2021.
[860] Rosen Plevneliev, *Lecture of President Rosen Plevneliev at the Atlantic Club in Bulgaria on "Current problems and priorities in the national security system of the Republic of Bulgaria" (Лекция на президента Росен Плевнелиев пред Атлантическия клуб в България на тема "Актуални проблеми и приоритети в системата за национална сигурност на Република България")* (Official website of the President 22 November 2012).
[861] Tomislav Donchev, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee on Homeland Security and Public Order 6 June 2018).
[862] Kiril Doichinov, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee on Defense 21 June 2018).

4.2.3). The Committee on Security Services Control provided a more accurate statement: "[t]he current regulatory framework only indirectly reflects the concepts and lacks clearly identified bodies that are responsible for the sectors concerned."[863]

Sections 6.2.1. through 6.2.6. will examine the legal framework before the BCSA entered into force in late 2018. These laws provided the scaffolding upon which the law was built but were insufficient to cover the requirements for businesses of critical importance to the functioning of the state to adopt resilience and risk management mechanisms, or the institutional infrastructure needed to tackle cross-border cyberattacks, covered in the NIS Directive.

6.2.1. Unlawful computer activity

Like the UK and Italy, Bulgaria also introduced provisions on the unlawful use of computer devices when cyber threats were nascent. This, however, happened at a much later stage: while the UK adopted the Computer Misuse Act in 1990 (as seen in Section 4.2.1.1.), and Italy amended the Penal Code in 1993 with Act of Parliament 547/1993 (Section 5.2.1.), in Bulgaria, provisions tackling the topic were only introduced in 2002 as amendments to the Penal Code. What served as a "wake-up call" for the Bulgarian legislature was the increased number of computer crimes such as credit card fraud, scam emails and attacks on public and private bodies' websites.[864]

An amendment to the Code in 2002 introduced a list of newly regulated unlawful computer activity. The new provisions prohibited accessing information systems illegally, assessing classified state information, tampering with computer data, publishing personal data, and implanting malware and viruses.[865] Assessing classified state information and tampering with computer data could lead to imprisonment of between one and eight years applied if, by accessing classified state information, "major consequences" occurred,[866] and with imprisonment

[863] Atanas Temelkov, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee for the control of the Security Services, the application and use of Special Intelligence Tools and access to Data under the Electronic Communications Act 21 June 2018).
[864] Gentian Fetah Kochi, *Computer crimes in Bulgarian and Albanian criminal law (Компютърните престъпления по Българското и Албанското Наказателно право)* (Sofia University Faculty of Law 2016) 24.
[865] Bulgarian Penal Code 1991 Chapter IXA article 319a-e.
[866] Ibid Chapter IXA Article 319a (5).

of between five and eight years and a fine of up to 10 000 BGN (roughly 5 000 EUR), applied if a person who "illegally add[ed], copie[d], use[d], change[d], transport[ed], delete[d], br[oke], worsen[ed], hi[d], destroy[ed] computer data in an information system, or halt[ed] the access to such data",[867] acted "on behalf of or executed a decision of an organised criminal group"[868] or who targeted a critical infrastructure's (CI) information system.[869]

Other relevant provisions include the definition of 'computer virus' introduced in 2007 and last amended in 2017.[870] In 2022 a new provision based on the latter was introduced, criminalising all activities related to installing computer viruses into an information system or a computer network,[871] with imprisonment between five and twelve years and a fine of up to 20 000 BGN (roughly 10 000 EUR) if said information system or computer network belongs to a CI.[872]

These provisions do not explicitly cover malicious computer interference performed or orchestrated by foreigners who are trying to meddle with the CI of the state. As seen, Article 319b 5 (1) makes a hint to 'contracted agents' with regards to organised criminal groups, which could have a transnational nature, but the provision falls short of specifying whether it refers to only national, or also transnational criminal groups. No such specification is found in relation to Article 319g (4) either. Here it is interesting to add that according to Article 5, the Penal Code has extraterritorial applicability and it hence applies also to foreigners who have committed crimes "of a general nature" that can "affect the interests of Bulgaria and its citizens" outside of the territory of Bulgaria.[873] Indeed, the cybersecurity threats analysed in this study are much more complicated than a lonely Bulgarian hacker tinkering with malware.[874] The extraterritorial applicability of Article 5, however, is very broad and – as opposed to other MS such as

[867] Ibid Chapter IXA Article 319b.
[868] Ibid Chapter IXA Article 319b (5) 1.
[869] Ibid Chapter IXA Article 319b (5) 2.
[870] Ibid Article 93 (27) a computer virus is "a computer program that is spread automatically and against the will or without the knowledge of the people using the information systems, and that is intended to bring information systems or computer networks into a state that is unwanted by their users, or for the occurrence of undesirable results".
[871] Ibid Chapter IXA Article 319g (1).
[872] Ibid Chapter IXA Article 319g (4).
[873] Ibid Chapter I article 5
[874] A scenario that became a reality in the summer of 2019 when the National Incomes Agency was hacked. A detailed analysis of the attack and how the relevant laws were applied will be discussed in Chapter 6.5.

Germany, Romania, Finland - provides no list of what exactly these 'interests' entail.[875] Such granularity would be helpful, especially now that a lot of criminal activity has moved online, making it very difficult to follow up on *all* crimes performed both within the territory of Bulgaria and outside. Such granularity would also be helpful in deciphering the actual scope of Articles 319b 5 (1) and 319g (4). If interpreted in a broader manner - with the malicious cyber operation seen as affecting the interests of Bulgaria and its citizens - then both provisions could mean that they are applicable to a foreign person or a foreign non-state actor (who could potentially also be performing the malicious cyber activity on a state government's orders. Chapter II has provided a more detailed account of the role of non-states actors and cyber operations (see Sections 2.4.2. through 2.4.2.2.)). If interpreted more narrowly, however, such cyber operations performed outside the territory of Bulgaria might be considered outside the scope of the Penal Code. Without a well-defined list of crimes affecting the interest of Bulgaria and its citizens, it remains only speculative whether a cyber operation launched from outside the national borders, targeting Bulgarian CI, would be followed up by a criminal investigation.

For the sake of the analysis, consider the following scenario. A foreign national is hired by their government, or a third-country government, to access classified information from state networks (in other words, perform a cyber espionage operation, as described in Section 2.3.2. Also, the international legal aspects of the state-sponsored attacks by non-states actors' scenario were addressed in detail in 2.4.2.1.) As extraterritoriality as a principle applies to the provisions above, this third-country national, if caught and convicted, could be fined and could spend up to eight years in Bulgarian prison. The problem is that he or she are simply contractors, where the real perpetrator is the third-country government that sought to access classified national security information. Naming an individual hacker, when the real aggressor is a nation-state, would not deter the actual mastermind from continuing to perform such operations. Because of the shortcomings of the law, the real aggressor seems unreachable by the Bulgarian prosecutor as only the 'middleman' could bear the legal consequences set in the Penal Code. The only other option for pointing the finger at a state's government is through a diplomatic response – an official accusation of a foreign state, however, must carefully consider the attribution issue and

[875] Anton Girginov, 'Extraterritorial effect of the Penal Code - problems with the legal system (Извънтериториално действие на Наказателния Кодекс - проблеми на правната уредба)' 8 Bar Review (Адвокатски преглед) 10, 14.

the potential consequences of having attributed the attack wrongly by, for instance, having linked the 'middleman' to the wrong state.

In summary, the Penal Code provided some promising provisions on how to (potentially) tackle state-sponsored cyber operations, but because the scope of the Code was not well-defined, these provisions might prove insufficient to tackle current trends in cyberattacks. It is clear more robust legislative measures were needed to cover the gaps. The following sections will examine how some of these gaps were addressed by the Bulgarian legislature prior to the entry into force of the BCSA.

6.2.2. Securitisation in the telecommunications sector

As seen with the other case studies, although not included in the scope of the NIS Directive (as seen in Section 3.3.1.1.A)), the telecommunications sector must be considered with regard to the security agenda because it is the telecommunication companies that provide electronic communications, and they are the very basis of network and information systems - the latter being the core of the NIS Directive.

One of the conditions for Bulgaria's entry into the European Union on 1st January 2007 was the alignment of the national laws to the Union laws. Hence, the securitisation in the telecommunications sector in Bulgaria followed a similar path to other EU Member States, but at a later stage. The Framework Directive on a common regulatory framework for electronic communications networks and services (Framework Directive) of 2002[876] was incorporated into national law via the Electronic Communications Act, adopted in May 2007. The relevant security-related provisions were inserted only in 2011 under Title XV *Security and integrity of electronic communications systems and services, confidentiality of messages and protection of customers' data.* Section I, *Security and integrity of the electronic communications networks* imposes a range of security requirements. Article 243 regulated the need for telecom operators to take the necessary preventive, technical and operational measures for security risk management

[876] Framework Directive 2002.

of the services they provide.[877] Encryption was the only example provided of such measures,[878] but admittedly, the EU regulator failed to provide more detailed list as it is technology-neutral. The following Article 244 posed obligations on the sector to take all technical and organisational measures needed to secure the integrity of their networks.[879] Article 243b then set the requirements for obligatory reporting of incidents by the sector and the Commission on Regulating Communications.[880]

In brief, what was observed as a trend at EU level and the other MS – that the telecoms sector was regulated much earlier and separately from the CI sectors listed under the NIS Directive – was mirrored in Bulgaria. Aligning its national law applicable to the telecoms sector might have meant that Bulgaria fulfilled its commitments to the EU, but the Bulgarian legislator did not go any further. Considering it was a Directive, Bulgaria could have easily introduced more stringent security measures, but it did not. As seen, the UK did not do it either (Section 4.2.1.2.), as opposed to Italy, whose telecoms security framework included also a DPCM on the IT security of the telecommunication services of the public administration adopted in 2002 and an Act of Parliament 155/2005 on International terrorism, addressing Electronic security (Section 5.2.2.). As outside the scope of this thesis, telecoms security will not be further addressed in detail, but to conclude on the role of the EU as an important supranational regulator, the discrepancies between the preparedness levels of the MS were addressed with the European Electronic Communications Code in 2018.[881]

6.2.3. Securitisation in the public domain

The legal framework on security measures for the public domain slowly began developing in 2008 with the E-Government Act. The amendments introducing concepts related to network and information security only came into force on 1 July 2016, undoubtedly because the NIS Directive was adopted a week later. New sections were introduced under Chapter IV *Technical*

[877] Electronic Communications Act 2007 Article 243 (1) and (2).
[878] Ibid Article 243 (2).
[879] Ibid Article 243a.
[880] Ibid Article 243b.
[881] Directive 2018/1972 establishing the European Electronic Communications Code (Recast).

infrastructure, network and information security – Section III *Network and Information Security* and Section IV *Compliance with the requirement for interoperability and network and information security*. The new provisions placed obligations on administrative bodies (without specifying which ones, therefore, presumably all of them) to secure their respective network and information security of information systems.[882] The requirements and security standards to be adopted by these administrative bodies were to be set by a Council of Ministers' Ordinance.[883] In the Bulgarian legislative system, an Ordinance has a similar status to the Prime-Ministerial decree in Italy, e.g. decreto Monti or decreto Gentiloni, examined in Sections 5.3. through 5.3.3. With this, the topic of securing the networks and systems of the administrative bodies was exhausted in the law.

The Ordinance on general requirements for information systems, registers and electronic administrative services, adopted in 2017, was equally vague in terms of guidance and concrete measures. The only article dedicated to information security was article 45 which reads that providers of electronic administrative services must use certificates of authenticity for their official websites through which said electronic services are provided.[884] Provided were also several suggestions as to what domain name security services and algorithms to transform passwords could be used.[885]

Another Ordinance on network and information security (NIS Ordinance N1) was adopted in 2017.[886] The NIS Ordinance N1 signalled a significant improvement compared to the previous tentative steps: it included a whole chapter on information security which included measures for risk management, systems' access, protection against malicious interference and malware, and systems' incident management.[887] Within its scope were, however, were only the administrative bodies. This led to the NIS Ordinance N1 being reappealed very soon by NIS Ordinance N2, adopted in 2019, which will be discussed below.

[882] E-Government Act 2008 article 54.
[883] Ibid Article 55.
[884] The Ordinance on general requirements for information systems, registers and electronic administrative services 2017 Article 45 (1).
[885] Ibid Article 45 (2) (3).
[886] Ordinance on network and information security 2017 (NIS Ordinance N1).
[887] Ibid Article 24 – 52.

Interestingly, as already seen, administrative bodies and public administrations did not in fact end up being covered by the NIS Directive, similarly to the telecom sector. This makes the provisions found in the E-Government Act and the NIS Ordinance N1 a good addition to any other law tackling network and information systems' security, but in no way sufficient to even be considered a predecessor of the NIS Directive's transposition law, as it engages with different sectors. On one hand, it could be argued that this move exposed under-preparedness, as the Bulgarian legislators introduced security obligations for a sector not covered in the EU law at the exact same time this EU law was adopted, instead of focusing on its new obligations. Indeed, there was no legal requirement for the E-Government Act to include any of the security measures for other sectors required by the NIS, as its scope and objectives were different, and because it was not a transposing instrument, but it was still a missed opportunity for the Bulgarian legislators to gain a head start into mapping out security requirements for a broader range of sectors. On the other hand, it could be argued that this move demonstrated ambition where lack of regulation was seen as problematic. The inclusion of security requirements for the public bodies also in a way reflects the debates on the scope of the NIS Directive and the active role Bulgarian representatives had in shaping it. As seen in Section 3.3.1.2.C)ii) Bulgarian MEP Kalfin argued strongly against the exclusion of the public administration sector from the scope of the EU law.[888]

More on the issue of administrative bodies and their role in the cybersecurity value chain will follow in the sections below, as the public administrations were later included among the sectors covered in the NIS transposition law – the BSCA - which made the latter an even more important piece of legislation to analyse, as its scope was clearly extended further than that of the NIS Directive – something that was not observed in Italy or in the UK. Despite therefore the efforts of states with high level of preparedness which acted as obstructors of the EU views (as seen in Section 3.3.1.2.C)ii)), Bulgaria followed what was observed by MEP Kalfin and reinstalled the sector within the scope of the NIS transposition law.

[888] European Parliament, 'Speech by Ivailo Kalfin on High common level of network and information security (debate)'.

6.2.4. Definitions underpinning cybersecurity laws

As observed throughout Chapter II and III, defining cybersecurity-related terminology is tricky as there have been discrepancies among the MS – and it was even trickier before the adoption of the 2013 EU Cybersecurity Strategy and the NIS Directive. Examining the terminology in each MS nonetheless enables an evaluation of the political positions the state was taking, how the threats were defined and its overall perception of cybersecurity. This will ultimately help draw conclusions on the different ways the analysed MS dealt with the topic in the pre-NIS Directive era and to what extent the EU definitions influenced their respective approaches. Like in the other case studies, in Bulgaria, important definitions are found both in the relevant strategies, and – albeit in a very limited way – in legislation.

6.2.4.1. Legislation

A key piece of Bulgarian legislation is once again the Electronic Communications Act 2008. As observed in Section 3.3.1.1.A), a fundamental definition found in the NIS Directive – regarding *network and information systems* – refers the reader to the EU telecommunications body of law. Bulgaria's legislative framework replicates this, providing that it is "an electronic communication network in the sense of §1.15 of the additional provisions in the Electronic Communications Act."[889] The term, introduced as amendment in 2011, is the translation of the one found in the EU Framework Directive 2002 (as quoted in Section 3.3.1.1.A)). This – although a key definition - completed the list of relevant cybersecurity terms found in legally binding documents.

[889] Bulgarian Cybersecurity Act 2018 Additional provisions, **§** 3. 23. "network and information system" is a) an electronic communication network in the sense of § 1, 15 of the additional provisions in the Electronic Communications Act.

6.2.4.2. Strategies

While the case studies' respective cybersecurity strategies are not discussed in detail in this study, they are an integral part of the overall cybersecurity ecosystem and contain important elements for the broader topic of the thesis. Most importantly, in view of Article 7 of the NIS Directive, each MS had to adopt its own NIS Strategy, in other words, its strategic approach to cybersecurity. Bulgaria did this for the first time in 2016, with its "Cyber resilient Bulgaria 2020",[890] and was one of the last MS to do so. Nonetheless, it was considered a "good ground" based on which the Bulgarian policies in the area could be improved.[891] The revamped document was adopted in 2021 as "Cyber resilient Bulgaria 2023".[892] As a comparison, as we saw in Section 4.2, the UK published its first such Strategy back in 2009.

The choice of name and the focus of the Strategy – resilience – was welcomed by Bulgarian academics who argued that focusing on resilience of systems, rather than security (which was the focus of the BCSA) was more realistically achievable. Absolute security in cyberspace, they argued, cannot exist.[893] In this regard, there was a "visible degree of coherence and continuity" between the Bulgarian and the 2013 EU strategies,[894] whose focus on cyber resilience was a number one strategic priority.[895]

The Bulgarian Cybersecurity Strategy 2016, therefore, defined key terms such as cybersecurity, cyberspace, cyber threat, and cybercrime,[896] which were later copy-pasted into the updated 2021 version.[897] As seen, Italy has already defined key cybersecurity terms back in 2013 (Sections 5.3.1.1. and 5.3.1.2.) but the UK had not included such granularity in its approach (see Section 4.2.) This is another element of diverging MS' approaches, and one of major importance. Having coherent definitions of the key terms at EU level – or at least of the different types of cyber

[890] Bulgarian Cybersecurity Strategy "Cyber resilient Bulgaria 2020" 2016.
[891] Petko Stefanov Dimov, *Application of web technologies for the protection of national security (Приложение на уеб технологиите за защита на националната сигурност)* (DioMira 2018) 61.
[892] Bulgarian Cybersecurity Strategy "Cyber resilient Bulgaria 2023" 2021.
[893] Kristina Bosakova, 'Cybersecurity – concepts, policies and strategies' in S. Denchev (ed), *Information and Security* (Za bukvite – O pismenehu 2019) 340.
[894] Venelin Georgiev (ed) *Strategic aspects of the cybersecurity on national and regional level* (Department of National and International Security, New Bulgarian University 2016) 344.
[895] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (7 February 2013) 4.
[896] Bulgarian Cybersecurity Strategy 2016 55.
[897] Bulgarian Cybersecurity Strategy 2021 50.

threats as observed in Sections 2.3. through 2.3.3.2.A) – would also help crystallising potential responses when attributing cyberattacks at EU level. As observed in Sections 3.3.2. through 3.5., however, there are limitations to the EU sanctions regime, meaning that when the EU is not available to provide support to its MS, the latter still have available ways of responding to a malicious cyberattack provided to them by existing international law, as seen in Sections 2.2.2.1. through 2.2.2.2.

Interestingly, however, the Bulgarian Strategies defined neither cyber espionage nor cyber terrorism – key elements, especially the former, in the digital domain nowadays - but defined cyber warfare twice. Definition One states that cyberwar is "any politically-motivated conflict in cyberspace, characterised by cyberattacks against adversarial computer and information systems."[898] Definition Two identifies cyberwarfare as "[m]ilitary actions conducted in cyberspace by IT means and methods. In a broader sense, this is the support of military operations conducted in traditional operational spaces - land, sea, air and space - through actions carried out in cyberspace."[899] It remains unclear why two definitions were adopted, as they seem complementary. Both, however, fall short from mentioning states or non-state actors as the perpetrators of attacks. This is an important element as, as seen in Section 2.4., clearly, not *any individual with* a political motive, targeting adversarial IT systems with a military action in cyberspace, would be triggering a *war*. The Bulgarian framework, however, fell short from drawing this very important distinction. Such an approach was not a unique case, as the UK strategies also did not contain many of these definitions. Italy did include such a definition back in the 2013 Strategy, but in the strategies adopted since, has also been reluctant to point fingers at specific states. This thesis has, in fact, identified the lack of a common definitions at EU level as one of the shortcomings of the EU regulatory and strategic approaches (Section 7.2.2.)

6.2.5. The institutional infrastructure pre-NIS

Out of the three case studies, Bulgaria seems to be the one with the least complex institutional infrastructure. Despite not being as burdensome as in Italy, simplicity in this case is not

[898] Bulgarian Cybersecurity Strategy 2016 56.
[899] Ibid 56.

necessarily a synonym of optimal functionality. While the UK's institutional infrastructure had its shortcomings, Bulgaria's cybersecurity institutional reality was non-existent before 2015. Prior to the BCSA there were three organisations which had some cybersecurity responsibilities: the State Agency for e-Government (Държавна агенция "Електронно управление", ДАЕУ, hereinafter DAEU), which was downgraded in 2022 and whose cybersecurity responsibilities were taken over by the newly established Ministry for Electronic Government,[900] the State Agency for National Security (Държавна агенция "Национална Сигурност", ДАНС, hereinafter DANS) and General Directorate for Fighting Organised Crime in the Ministry of Interior (Главна дирекция "Борба с организираната престъпност" (ГДБОП), hereinafter GDBOP). Their competences were acquired as recently as 2015 via provisions in the relevant laws analysed below.

According to the E-Government Act 2008's now repealed article 7a, the DAEU was going to be the lead agency in the broader area of cybersecurity. The President of the Agency was to be in charge of the state policy on the matter.[901] Criticised as requiring "cosmic" costs for the implementation of the broader e-government policies and measures,[902] it was revealed that nobody took notice of the specific budget invested in the area of cybersecurity.[903] In fact, it appears that the cybersecurity responsibilities of DAEU were given a rather peripheral importance prior to the NIS Directive requiring MS to take action. For instance, the E-Government Act did not specify whether DAEU would have responsibilities in protecting the CI sectors' network and information systems. Since 2022, the leading role in cybersecurity regulation was taken over by the Ministry for Electronic Government, to be discussed below.[904]

Cybersecurity's link to national security also remained unexplored until as recently as 2015. Providing a bit more detail in terms of the area of applicability, according to an amendment in the State Agency for National Security Act 2008, within the powers of the DANS fell the responsibility to protect against destructive effects on communication and information

[900] BCSA 2018 Article 12.
[901] E-Government Act 2008 Article 7a.
[902] Ivan Valentinov Ivanov, *Parliamentary Plenary session* (27 June 2018).
[903] Vladislava Peeva, 'Cyber(in)security for millions (Кибер(не)сигурност за милиони)' (1 August 2019) <https://www.mediapool.bg/kibernesigurnost-za-milioni-news296397.html> accessed 3 January 2024.
[904] BCSA 2018 Article 12.

systems.[905] To further demonstrate the lack of knowledge on how to legally address cyber threats at national level in Bulgaria at the time, there appears to be no further detail as to which exactly are the concerned communication and information systems. There also appears to be no provision-specific debate in plenary when the amendments of the law were discussed and voted through.[906] It is evident that not *all* breaches of communication and information systems would pose a threat to national security. Again, no specification of whether these systems belonged to the CI sectors or not was found. Considering the broader matter of the law – national security – one would assume that the provision in the State Agency for National Security Act referred to the CI sectors' systems and the cyberattacks to be considered were those amounting to a threat against the national security. But no classification of which types of attacks would be considered such was provided (as seen throughout Chapter II there could be different types of attacks that would violate different national and international norms and would thus require different types of response). Leaving such an information gap could only lead to confusion in DANS' personnel regarding their roles and responsibilities as regards cyberattacks. It also shows that cybersecurity was not given a "top-of-the-national-security-agenda" status, and the regulator thought that penning such a vague provision would suffice to address the threat.

An amendment introduced in 2018 provided the much needed "detail". It was clarified that the reference is to communication and information systems "of strategic objects relevant to national security".[907] That same year, the DANS became the body to accredit the security of the communication and information systems within which classified information was to be created, worked on, filed, and transmitted.[908]

The last public authority with responsibilities in the cyber domain was GDBOP. In 2016 amendments were introduced in the Interior Ministry Act 2014, according to which GDBOP was responsible for the organised crime related to computer crimes or crimes committed through computer networks and systems.[909] No further details were added, and the Act was not followed by an Ordinance mapping the exact responsibilities of the institution. In view of its general responsibilities, it is likely that the types of crime GDBOP deals with are not those related to the

[905] State Agency for National Security Act 2008 Article 4 (1) 10.
[906] *Thirty-seventh plenary session of the National Assembly of the Republic of Bulgaria* (11 February 2015).
[907] State Agency for National Security Act 2008 Article 40a (4).
[908] Ibid Article 6 (5).
[909] *Interior Ministry Act 2014* article 39 (2) 3.

CI infrastructure protection, but rather to the cybercrime pillar, focusing on non-politically motivated cyberattacks.

To summarise, an institutional infrastructure has existed in Bulgaria since 2016, but there was little detail on who did what, and it was limited in scope and competences. Missing was also a roadmap for response to cyberattacks, operational procedures and exchange of information between authorities and responsible parties.[910] As Dimov points out, the focus was mainly on network security, with information security given merely a "technological toolkit"[911] - implying that the substance of information security such as protective measures, applicable legislative framework, responsible authorities in case of a breach of information security – were all missing. The lack of clarity of the relevant areas of expertise – which organisation protected the CI sectors, would all operations against the CI sectors amount to a national security threat, which organisation was responsible for performing protective or pro-active cyber defence operations – meant the legislator was confused and did not have enough expertise to further assign clear roles and responsibilities. The Bulgarian reality clearly had little similarities with Italy and the UK (whose institutional infrastructures pre-NIS Directive was analysed in 5.3.1.3. and 4.2.3. respectively). Prominent powers – included in the Italian and British frameworks - for the PM, or for the Defence Minister, or the intelligence agencies remained vague and subject to interpretation, and had to wait the BCSA 2018 to be adopted, evidencing again the key role as a regulator the EU had for those MS with low level of legal preparedness.

6.2.6. Summary

Compared to the other case studies, this section has demonstrated that cybersecurity as a sector was not given importance in Bulgaria until very recently. As a consequence, legislation was sporadic. The gradual securitisation of various domains did bring a better understanding of the topic but was not enough to conclude that Bulgaria had developed a comprehensive cybersecurity legal framework prior to the NIS Directive. None of the abovementioned pieces of legislation tackled the protection of CI sectors from cyberattacks, a key element for any

[910] Dimov 62.
[911] Ibid 63.

legislative framework dealing with cybersecurity. As a comparison, although through secondary legislation, as seen in Sections 5.3. through 5.3.3., Italy had done as much. The UK, on the other hand, despite being much more advanced in terms of the broader cybersecurity legal preparedness, also had not addressed the protection of the CI sectors prior to the NIS Directive, as Section 4.2.4. showed. Nonetheless, Bulgaria and the UK cannot be categorised together, as the UK NIS Regulations, which introduced cybersecurity measures for CI sectors, complemented other existing cybersecurity body of law and a very well-developed strategic approach. This has not been the case in Bulgaria. Also, the three different levels of preparedness were evidenced clearly also by the institutional infrastructure. All these missing or mismatched elements in the three MS provide the scope for the EU to address the gaps and harmonise preparedness with the ultimate goal to avoid fragmentation of the internal market.

6.3. Transposing the NIS Directive into national law

The adoption of the Bulgarian Cybersecurity Act in 2018 brough a fundamental change in the Bulgarian cybersecurity landscape. The following sub-sections will highlight the major changes the law brought into the national legal system.

The BCSA 2018 is the first piece of legislation addressing *sensu stricto* cybersecurity in Bulgaria. Unlike Italy and the UK, whose transposition laws were mostly a copy-pasted version of the NIS Directive, the Bulgarian one was different. Branded "revolutionary" by the Committee on Defence in its first reading report, alongside assertions that cybersecurity was already covered by existing legislation,[912] this document did bring into light a new legal approach to the topic in Bulgaria. The country did not successfully transpose the Directive by the deadline of 9 May 2018. Even the draft bill was introduced to Parliament late, on 30 May 2018. The national law was adopted only in November 2018. However, this is not exceptional, as only around one third of the EU MS had managed to transpose it on time.[913] The level of preparedness across the MS analysed is reflected also in the timeliness of transposing the Directive: the UK,

[912] Doichinov.
[913] Walser, Roman. "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework." Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings. Vol. 11252. Springer, 2018.

despite Brexit, was one of the few countries to transpose the Directive by the deadline, this was not the case also in Italy, where national legislation came into force on 24 June 2018 (as seen in Section 3.3.1.1.A)).

Title I of the BCSA - *General provisions* - is largely scene-setting, defining the scope and attributing various cyber domains to the respective institutions and agencies. According to Article 1, the subject matter of the law is to "define the activities for the organisation, management and control on cybersecurity, including cyber defence and cybercrime, define the measures to achieve a high level of network and information security and outline the competences and functions of the competent authorities in the field of cybersecurity".[914] It becomes clear that Bulgarian legislators have tried to incorporate in one piece of legislation all types of cyber threats possible. This is reminiscent of the approach taken in the non-legally binding 2013 EU Strategy: cover as much as possible of the cyberattacks spectrum in one place. In Bulgaria this was likely a compensating mechanism to the major gap in the field evidenced above, via which it tried to incorporate all relevant cyber issues under the same legislative umbrella.

Title II follows with provisions on NIS which introduce the new requirements for operators of essential services (OES) and digital service providers (DSP), which technically is the part transposing the NIS Directive. The structure of the bill caused concerns during parliamentary debates, as it was pointed out that it was not clear which parts of the law transposed the NIS Directive and which parts were added by the Bulgarian legislators.[915] This indicates again that parliamentarians were largely unfamiliar with both the existing framework and the requirements of the EU law.

[914] BCSA 2018 Article 1 (1) and (2).
[915] Ahmed Ahmedov, *Parliamentary Plenary session* (27 June 2018).

6.3.1. Definitions

The BCSA defines important concepts, including some previously found in the 2016 Strategy, e.g. "cyberattack", "cyber threat", "cyber incident", "cyber defence" and "cyberspace".[916] The wording of the Act and the Strategy differ, but not significantly. The BCSA includes also a definition of "cybersecurity" - something noticeably missing from the NIS Directive.[917] Cybersecurity is thus defined as "a state of the society and the state where, by applying a set of measures and actions, cyberspace is protected from threats against its independent networks and information infrastructure or threats that may disrupt the latter's work".[918] Article 2.2 then specifies that cybersecurity encompassed three elements; network and information security, cybercrime and cyber defence.[919] This wording again mirrors the wording of the 2013 EU Cybersecurity Strategy (Section 3.1.), which separated these three elements in different pillars. This indicated that Bulgaria indeed considered the EU as a leader whose framework should be followed and implemented. However, the three terms clearly differ in terms of what they encompass. Moreover, they do not fully correspond to the EU definition of "cybersecurity" (provided in the Cybersecurity Strategy 2013 (as acknowledged in Section 3.2.1.) and later included in a much more consisted version in the EU Cybersecurity Act 2019 as seen in Section 3.3.1.1.B).) This highlights the discrepancies in MS' cybersecurity approaches and further demonstrates the need for an EU-level line of command. These discrepancies appeared also during the transposition process across the MS when identifying the operators of essential services (OES), the national competent authorities (NCA), the single points of contact (SPOC), the Computer Security Incident Response Team (CSIRT) – issues which will be addressed below.

[916] BCSA 2018 Additional provisions, § 3 10-17.
[917] A definition of "cybersecurity" was included in the EU Cybersecurity Act 2019, in Article 2(1). It states that cybersecurity "means all activities necessary to protect network and information systems, their users, and affected persons from cyber threats". The message EU legislators are sending is clear – while with the NIS Directive MS were reluctant to put forward a piece of legislation on a topic that can easily be seen as national competence, with the EU Cybersecurity Act the picture has changed.
[918] BCSA 2018 Article 2.1.
[919] Ibid Article 2.2.

6.3.2. The new institutional infrastructure

The BCSA sets up a brand-new cybersecurity institutional design in Bulgaria. While incorporating diverse (existing and non-existing) normative frameworks into one law was a step forward, the need for newly regulated institutions and other stakeholders to improve their cooperation was essential.[920] Duties were shared by several already mentioned bodies. DAEU was assigned the area of NIS,[921] but after the amendments in 2022 the e-Government Ministry took over its role;[922] the Ministry of Defence was assigned the area of cyber defence and hybrid threats;[923] the Ministry of Interior was assigned cybercrime;[924] and the DANS was assigned the protection of the communication and information systems of strategic sites and activities against cyber interference.[925] A similar fragmented but all-encompassing approach was embraced also in Italy with DPCM 2013 (but then repolished with subsequent legislative measures as observed in Sections 5.3.1.3. and 5.4.2. respectively).

6.3.2.1. The Cybersecurity Council

Together with the abovementioned new responsibilities assigned to existing institutions, Article 7 of the BCSA establishes a new body: the Cybersecurity Council (hereinafter CC).[926] It took a further year for the authorities to institute the CC – it was officially established in late 2019.[927] This was not a requirement of the NIS Directive, but a national initiative.

The CC is an overarching body, dealing with the broader area of cybersecurity, mirroring the broad nature of the BCSA. It is institutionalised within the Council of Ministers, the body in charge of cybersecurity at political level.[928] The Council is chaired by the Minister for e-

[920] Dimitrina Polimirova and others, 'Cybersecurity and Opportunities for Application of Innovative Technologies in the Public Administration in Bulgaria' National Lab for Computer Virology, Bulgarian Academy of Sciences73.
[921] BCSA 2018 ex-Article 12.
[922] Ibid Article 12.
[923] Ibid Article 13.
[924] Ibid Article 14.
[925] Ibid Article 15.
[926] Ibid Article 7 (2).
[927] Rules regulating the organisation and activity of the Cybersecurity Council 2019.
[928] BCSA 2018 Article 7.1 and 2.

Government (as per a 2022 amendment)[929] and consists of key ministers and officials, including the Interior Minister, the Defence Minister, the Minister of Foreign Affairs, all Ministers in the lead of CI sectors, the President for the Intelligence State Agency, the President of the DAEU, the Secretary of the Council of Ministers' Security Council, and a representative of the President of the Republic, among others.[930] This makes it a high-level political body.

The Council's remit is of a coordinating and advisory nature, ranging from analysing cyber threats and countermeasures, to drafting the national strategies on the matter, informing the State Security Council of the state of play in cyberspace or advising on the national plan on managing cyber crises.[931] While not explicitly addressed, it could be also expected that the CC would be consulted on a possible attribution case if a foreign-sponsored cyberattack is considered. The CC is hence similar in structure and responsibilities to the Italian NSC, the Cybersecurity Unit, responsible for handling cyber crises, among other tasks (as seen in Section 5.3.1.3.A)).

The BCSA does not, however, provide details on the configuration according to which the CC is to be assembled or when its meetings would be needed. This information came a year later, with the adoption of the 'Rules regulating the organisation and activity of the Cybersecurity Council', according to which the CC would meet regularly - at least once a year – or hold extraordinary meetings if summoned by its Chair or if at least ¼ of its members required a meeting.[932] The reasons for holding the latter have not been set out in the 'Rules' and remain therefore speculative. The CC has its own page on the Advisory Board Portal,[933] where similar advisory bodies are also represented, and where information on the annual programme and indicative dates for the regular meetings should be found, according to article 26 of the 'Rules'.[934] In August 2023, the page did not provide any such information, when there should have been at least three or four regular meetings by that date. Furthermore, some of the page's actual content, divided into sub-headings such as work programme, work programme reports, strategic goals, continued to be unpopulated.

[929] Ibid Article 9.2.
[930] Ibid Article 9.3.
[931] Ibid Article 10.
[932] Rules regulating the organisation and activity of the Cybersecurity Council 2019 Article 6.
[933] Advisory Board Portal of the Council of Ministers, 'Cybersecurity Council' <http://saveti.government.bg/web/cc_1901/1> .
[934] Rules regulating the organisation and activity of the Cybersecurity Council 2019 Article 26 (1), (2) 3 and 4.

It is interesting to mention that, back in 2021, when this Chapter was first drafted, when trying to access the page of the Advisory Board Portal, a warning popped up saying that the website is using "outdated security configuration which may expose" information such as passwords or other personal data. In August 2023, the website is no longer "outdated", but clicking on the various menu options caused the page to get blocked and the message "[t]his site can't provide a secure connection" to appear.[935] The security level of the Advisory Board Portal of the Council of Ministers should be exemplary of the way the Government approaches cybersecurity; such gaps clearly demonstrate the insufficient level of cybersecurity know-how and the fact that there continues to be a gap between the adopting the law and enforcing the law.

6.3.2.2. National competent authorities and single points of contact

As per requirements observed in 3.3.1.1.A), the NIS Directive requires the MS to designate national competent authorities (hereinafter NCA) and single points of contact (hereinafter SPOC) to monitor the correct application of the Directive in the MS and to facilitate information exchange and achieve better cooperation at Union level.[936] In Bulgaria, the DAEU was initially chosen as the main NCA for all administrative bodies, as well as SPOC.[937] After the establishment of the Ministry for E-Government in 2022, it took over the two roles.[938] With regards to each of the CI sectors covered in the Directive, an NCA was created within the respective Ministry.[939] This fragmented approach was also the preferred choice in Italy and the UK, as one of the few elements all three case studies had in common (as seen in Sections 4.2.4.2.A) for the UK and 5.4.2.1. for Italy). This fragmentation, however, hides the risk of uneven implementation of obligations and circumvention of responsibilities in case of breaches of security. Cyberattacks are usually multi-layered, difficult to constrain within the existing categories, not focusing on specific sectors, and a decentralised approach would be an additional burden for the better implementation of legislative measures.

[935] Advisory Board Portal of the Council of Ministers.
[936] NIS Directive 2016 Article 1 and 8 respectively.
[937] BCSA 2018 former Articles 16.2 and 17 respectively.
[938] Ibid Articles 16.2 and 17 respectively.
[939] Ibid Article 16(1).

6.3.2.3. Operators of essential services (OES) and administrative bodies

The BCSA introduces the obligation for identification of OES and DSP and the necessary risk management requirements deriving from the NIS Directive.[940] In line with the latter, the OES for the seven CI sectors had to be identified. In Bulgaria 185 entities were identified as such (compared to 470 British and 553 Italian entities see Sections 4.2.4.2.B) and 5.3.2.2.).[941]

Prior to the Directive, since 2012, Bulgaria had listed nineteen sectors as CI:[942] those seven listed in the NIS Directive were also found in the Bulgarian framework. Other sectors included information and communication technologies (electronic communications networks and information and communications infrastructure), postal services, environment, food and agriculture, economy, sports equipment, education and technology, tourism, defence, disasters protection and cultural heritage.[943] The BCSA, however, limited the cybersecurity requirements to only those sectors identified in the NIS Directive, therefore not expanding the scope to the other critical sectors. This will have to be done, however, as NIS2 Directive covers many more sectors compared to the original NIS, and many of these new sectors correspond to those identified in Bulgaria in 2012: postal services; waste management; manufacturing, production and distribution of chemicals; food; manufacturing; digital providers, research (see Section 3.3.1.1.C)). Research has not managed to identify whether it was Bulgarian representatives at EU level that contributed to shaping the new critical sectors' framework based on the national one, but it demonstrates the EU and Bulgaria have been moving in similar directions.

Where the BCSA went beyond any EU requirement was with regards to administrative bodies, public legal entities and organisations - not classified as OES - providing administrative services via electronic ways.[944] This is, however, not surprising, as public administrations did fall within the scope of the initial proposal for the NIS Directive. Hence, it is not an 'originality' attempt by the Bulgarian lawmakers to include public legal entities in the transposition law. Moreover, as

[940] Ibid Article 23 OES and 25 DSP.
[941] European Commission, *Report on assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems* 27.
[942] Ordinance on the way, order and competent authorities for identifying critical infrastructure sectors and assessing the risk applicable to them 2012.
[943] Ibid Annex I.
[944] BCSA 2018 Article 4 Scope.

seen in Section 3.3.1.2.C), back when the NIS Directive was debated in the European Parliament, a Bulgarian MEP, Ivaylo Kalfin, in his role of shadow rapporteur of the Opinion of the Committee on Industry, Research and Energy (ITRE) on the NIS directive, argued that it was a great mistake to leave the public sector out of the Directive.[945] While this is speculative – Mr Kalfin did not return to the Bulgarian Parliament after being an MEP - it could be argued that him voicing his concerns might have influenced Bulgarian legislators, or reflected their pre-existing concerns. Either way, the result is that the Bulgarian law encourages a higher number of sectors to comply with the EU security requirements. This will certainly bring a higher level of complexity on the implementation and technical side but is nonetheless a valuable addition to the Act.

6.3.2.4. CSIRT

Appointing or establishing the CSIRT is the last piece in the NIS institutional requirements puzzle (see Section 3.3.1.1.A)). The nature of the CSIRT has been defined as the "nucleus", the "nervous system" of any cybersecurity system.[946] Considering the role of the body assigned by the EU law within the CSIRT network and its importance for the overall cross-border level of incident reporting and mutual cooperation, this comparison seems very accurate.

The Bulgarian CSIRT was initially established within the DAEU,[947] later replaced by the Ministry of E-Government.[948] Even though as per NIS Directive's Annex I, all national CSIRTs need to be operable, reachable and responding to incidents 24/7, the Bulgarian CSIRT's contact hours, as of August 2023, are still 08:00-20:00, Monday to Friday.[949] Also, the job of the national CSIRT is limited to providing support and advice to the sectoral CSIRTs, established

[945] European Parliament, 'Speech by Ivailo Kalfin on High common level of network and information security (debate)'.
[946] Colonel Ass. Prof. Ivan Chakarov, 'Directions on cyber protection in management systems (Направления за киберзащита в системите за управление)' Nacionalna Sigurnost (Национална сигурност) 9, 11.
[947] BCSA 2018 ex-Article 19 (1).
[948] Ibid Article 19 (1).
[949] National CSIRT, <https://www.govcert.bg/en/%d0%ba%d0%be%d0%bd%d1%82%d0%b0%d0%ba%d1%82%d0%b8/> accessed 16 August 2023.

within all the different sectorial competent authorities.[950] These sectoral CSIRTs need to be operable 24/7, have an efficient system for handling incident reports, enough personnel and proper infrastructure to guarantee ongoing operability.[951] As the NIS Directive requires entities to notify incidents either the competent authorities or the national CSIRTs,[952] in Bulgaria it is these sectoral CSIRTs that have to be notified of incidents by the administrative bodies, OES or DSP. The UK's approach was similar to the Bulgarian one, with incidents reports to the designated competent authorities, although without creating the sectoral CSIRTs within the latter (Section 4.2.4.2.C)). Italy instead, put the national CSIRT at the heart of its approach to transposition, assigning to it the responsibility of receiving incident notifications (Section 5.3.2.3.).

The timeframe for reporting in the three states is another interesting issue: whilst Italy kept to the NIS Directive's subject-to-interpretations "without undue delay" (as seen in Section 5.4.2.3.A)), the UK was more restrictive: "without undue delay and in any event no later than 72 hours" (as seen in Section 4.2.4.2.A)). Bulgaria, however, was the harshest, yet most ambitions: it only gave entities 2 hours for reporting after having become aware of the incident.[953] This short timeframe demonstrates that it did not have the necessary knowledge of the threat landscape and how some cyberattacks work in reality. Even running an analysis of infected/affected systems or networks, unauthorised assets access, or data leaks, can consume a lot of time – how are entities expected to provide a report of the issue and how is the sectorial CSIRT supposed to conclude by this very early report what the actual problem is and whether it could potentially have a cross-border effect? Once again, from the provisions transpires the unpreparedness seen in Bulgaria and the significant knowledge gap. On the same issues, also Italy had a significantly complicated incident reporting mechanism (as seen in Section 5.4.2.3.A)), which also highlights the importance of knowledge sharing and solid EU leadership in overcoming discrepancies such as these ones on critical issues such as incident response.

[950] BCSA 2018 Article 19.
[951] Ibid Article 18 (2) 3.
[952] NIS Directive 2016 Article 14 3.
[953] BCSA 2018 Article 21 4, 5.

6.3.3. NIS Ordinance N2

Since the BCSA provides no details on the technicalities of achieving network and information security, this gap was filled with NIS Ordinance N2 (which repealed NIS Ordinance N1). NIS Ordinance N2 has a much wider scope compared to N1: it applies to administrative bodies, OES, DSP and any other organisation providing public services and functions that has not been identified as OES, but that provides administrative services via electronic means.[954] In terms of content, it is the "technical guide" accompanying the BCSA by adding much needed granularity. It provides a very detailed roadmap of what technical and organisational measures should be taken in terms of how to manage NIS (e.g. with well-developed security policy, a roadmap of all information documentation, classification of the information, risk management, third-party security),[955] protection (segregation of systems, access management, remote work security, hardware and software protection, malware protection, NIS incidents management and reporting),[956] resilience (archiving information, continuity plans)[957] and controls (audits, checks).[958] This document is therefore a significant piece of the regulatory puzzle despite not having the status of a "law".

6.3.4. Summary

To sum, the BCSA played a key role in shaping the Bulgarian legal framework to cybersecurity. It was an ambitious law: it eliminated the legal fragmentation and provided scaffolding for existent institutions by mapping their newly assigned responsibilities to tackle cyber threats. It expanded the scope by imposing cybersecurity obligations to the public administrations, but also included cyber defence and cybercrime as subject matter – an unusual move, as these two areas have traditionally been regulated separately at EU level. Perhaps unsurprisingly, then, the provisions of the law addressing these two areas provided little detail, particularly on how to

[954] Ordinance on Network and Information Security 2019 Article 1. (1) 1.-5.
[955] Ibid Chapter II Section I NIS Management, Article 3 – 12.
[956] Ibid Chapter II Section II Protection, Articles 13 – 31.
[957] Ibid Chapter II Section III Resilience, Articles 32 – 34.
[958] Ibid Chapter III Controls, Articles 35 – 37.

respond to a cyberattack threatening national security. Despite therefore the EU's efforts to eliminate fragmentation, and to achieve a better level of preparedness across all MS, clearly the NIS Directive was insufficient. It is up to the Bulgarian policymakers to learn from the other states with higher level of preparedness and not make similar mistakes as incorporating too many issues in the NIS2 transposition law.

6.4. Implementing the BCSA 2018: the attack against the National Incomes Agency 2019

Nearly a year after the adoption of the BCSA, in early summer of 2019, the Bulgarian National Incomes Agency (Национална Агенция по приходите, НАП, hereinafter NAP) came under attack and the personal data of around 5 million Bulgarians was accessed.[959] The data was leaked to the media via an email containing the – harsh, but seemingly not entirely inaccurate – words: "[y]our Government is demented. Your cybersecurity is a parody".[960] The NAP was fined 5.1 million leva (roughly 2.5 million euro) by the Commission for Personal Data Protection for having breached the security obligations for data controllers to adopt the necessary and proportionate technical and organisational measures to protect the personal data they handle, a requirement found in Article 32[961] of the GDPR.[962]

Even though originating from the territory of Bulgaria, and therefore not representing the state-sponsored attacks this thesis is focusing on, the hack is important for assessing the Bulgarian approach to cybersecurity for several reasons. First, both law enforcement and media only superficially referenced the BCSA in relation to the hack. Also, a significant gap was left because what did not follow was a detailed analysis or parliamentary debate, focusing on the

[959] Peeva.
[960] Ibid.
[961] GDPR 2016 Article 32, Security of processing 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
[962] 'The Commission for Personal Data Protection explained why the NAP was fined 5.1 million leva (Комисията за защита на лични данни обясни защо глобява НАП с 5.1 млн. лева)' *Dirbg 29 August 2019* <https://dnes.dir.bg/obshtestvo/komisiyata-za-zashtita-na-lichni-danni-obyasni-zashto-globyava-nap-s-5-1-mln-leva> accessed 3 July 2021.

cybersecurity aspects of protecting personal data, on the existing legislative framework and its potential cracks in enforcement, on the profound lack of practical and technical knowhow, on the deep lack of knowledge on what cybersecurity constitutes and what the consequences of not having an approach to mitigate and respond to cyberattacks are. In other words, there was no 'lessons learnt' acknowledgement by the political elite or the NAP itself, at least not publicly. On the website of the Cybersecurity Council, established roughly one month after the attack, there seems to be no sign of a meeting related to the event. Moreover, in the aftermath of the attack, Vice-PM Donchev admitted that the Government was investing very little in cybersecurity and stated that "cyber war is ongoing", in reference to the NAP hack.[963] The comment is surprising, as well as being inaccurate. To be classified as "cyber war", according to the two definitions of the term found in the 2016 Cybersecurity Strategy discussed in Section 6.2.4.2., the attack should have been politically motivated and/or a military action conducted in cyberspace. The NAP hack was neither. The Bulgarian level of preparedness thus transpires also from comments like this one: arguments surrounding the imminent occurrence of cyber war have long been overcome (as seen throughout Chapter II, and more specifically Sections 2.2.2.2. and 2.3.3. through 2.3.3.2.A)).

Second, the prosecution decided to file charges against the perpetrator, Kristian Boikov, for terrorism under article 108a of the Penal Code which addresses actions "aimed at creating fear and confusion in the population",[964] instead of Article 319 on unlawfully accessing information systems and publishing personal data, analysed above. Stoichkov has argued that a potential reason for the lack of developments in the case – four years into its filing it has still not been seen in court, with the Sofia City Court, where it was meant to be heard, returning it back to the Prosecutor General in April 2023 for "substantial mistakes" in the original filing[965] - was that

[963] 'Tomislav Donchev: A cyberattack from the inside shakes the government, from the outside - shakes the state (Томислав Дончев: Кибератака отвътре клати правителството, отвън - клати държавата)' (*Novini.bg*, 20 July 2019) <https://novini.bg/bylgariya/politika/548365> accessed 12 September 2023.
[964] Peeva.
[965] 'The court returned the terrorism case for the NAP data breach to the prosecutor's office (Съдът върна на прокуратурата делото за тероризъм покрай теча на данни от НАП)' (*Lex News*, 5 April 2023) <https://news.lex.bg/%D1%81%D1%8A%D0%B4%D1%8A%D1%82-%D0%B2%D1%8A%D1%80%D0%BD%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D0%BA%D1%83%D1%80%D0%B0%D1%82%D1%83%D1%80%D0%B0%D1%82%D0%B0-%D0%B4%D0%B5%D0%BB%D0%BE%D1%82%D0%BE-%D0%B7/>

proving there was a "terrorist" element was rather difficult.[966] Evidently, the hack had no terrorist element and the fact that the authorities misinterpreted it in such a way once again demonstrates profound misunderstanding of key cybersecurity concepts.

A third and final point worth making about the NAP hack is that the NAP, being a public administration of key importance providing its services via electronic means, falls within the scope of the BCSA, and thus is required to adopt certain cybersecurity risk management measures. Clearly, the hack was a case of failed implementation and enforcement of the law. The data breach not only reflected the low level of security awareness of the public institutions, but also compromised the integrity of their work.[967] The event serves as a further example of the lack of fulfilment of the adoption of cybersecurity requirements for key sectors in Bulgaria. While the law continues to be wrongly implemented, or even disregarded and circumvented, such attacks will keep happening. This again highlights the scope for the EU to act in the field of cybersecurity, thereby harmonising the level of preparedness across the MS. Whilst the NAP hack was a targeted and contained attack and it did not spread cross-border, this simply is not always the case (as observed throughout Chapter II). The EU's role as a cybersecurity regulator emerges as a solution to the MS with low level of preparedness as it contributes towards raising that level.

6.5. Cyber defence and offence

6.5.1. Cyber defence

In terms of cyber defence, there is a big difference between how Bulgaria has dealt with the topic compared to the other states analysed in this thesis (for the UK see Sections 4.2.1.3. through 4.2.1.3.i) and for Italy see Sections 5.6. through 5.6.2.). The National Security Strategy 2018 acknowledged the rise of cyber threats against Bulgaria.[968] Taking a more reserved approach

[966] Ognyan Stoichkov, 'Special Intelligence and Cyber security (Специални разузнавателни средства и киберсигурност)' Security & Defense (Сигурност и отбрана) 137, 139.
[967] Ibid, 139.
[968] National Security Strategy 2018 2.

compared to the UK, both this document and the two cybersecurity Strategies stopped short of naming foreign states as perpetrators in cyberspace, while at the same time acknowledging that there are indeed states that do so.[969] Bulgaria, like the UK and Italy, also has acknowledged that cyberspace is the 5th domain of war, although indirectly – by citing NATO's views on the matter.[970]

Against this reality, it comes as surprising that the BCSA encompasses also a 'defence' pillar. Article 13 sets the requirements for the Defence Minister: the focus is on building cyber capabilities for defence and organising trainings and coordination with NATO and the EU.[971] Article 13 further states that the Defence Minister is responsible for the state policy on "defence and **active counteraction** [emphasis added] to cyberattacks and hybrid interference on defence and army systems",[972] but there are no details on what "active counteraction" might constitute: there is no actual mapping of how to "actively counteract" to a cyberattack, nor there is an Ordinance that explains how to do so.

What is absent, for example, is Bulgaria exercising its rights deriving from Article 222 of the TFEU or Article 42.7 TEU, as discussed in Section 3.3.1. What could have been helpful is a provision such as "[i]f victim of a [foreign-sponsored] cyberattack against Bulgaria's sovereignty or against the integrity of CI sectors' network and information systems, thereby causing major consequences for the state, including massive destruction or death, the Defence Minister shall summon the Cybersecurity Council which shall decide on the appropriate way to act, including with countermeasures, in accordance with international law, or evoke the Solidarity Clause or Mutual Defence Clause, in accordance with EU law." Such a provision could have brought some added value to the text in terms of the role of the institutions in not only defending and responding (in the sense of restoring the status quo) to attacks, but defending Bulgarian sovereignty in cyberspace with concrete measures that will have an impact.

Hence, while it might have seemed a good idea to the legislators to include cyber defence, the added value of these provisions in practical terms is limited, especially if there is not much in the Act pinpointing the response roadmap. This could be due to Bulgarian lawmakers' unwillingness

[969] Bulgarian Cybersecurity Strategy 2016 7, Bulgarian Cybersecurity Strategy 2021 8, and National Security Strategy 2018 7.
[970] Bulgarian Cybersecurity Strategy 2016 10.
[971] BCSA 2018 Article 13.
[972] Ibid Article 13 (1).

to impose an unnecessarily rigid framework. However, in this case, the topic of cyber defence should have been left out – the same way it was left out from the NIS Directive (and, in general, from the overall EU regulatory approach to cybersecurity as seen in Section 3.4.). Assigning a Ministry responsible for tackling cyberattacks threatening the national security without drawing a roadmap for how to legally do so is at the very least, insufficient. As a comparison, the UK's approach to cyber defence – and offense – is framed under 'equipment interference' and 'interception' terminology, which have had a legal basis in the UK for almost 30 years (as seen in Sections 4.2.1.3. through 4.2.1.3.i)), but its NIS implementation law does not address it (see Section 4.2.4. through 4.2.5.) Italy, although having a completely different framework to the UK, has also considered the inclusion of the defence pillar in the NIS transposition law unnecessary (as seen in 5.4. through 5.4.3. and 5.6. through 5.6.2.).

6.5.2. Cyber offence

Cyber offense (or "softer" ways of framing it e.g. equipment interference in the UK framework) is not a topic covered in the BCSA. The reasons for this are speculative – not enough resources (financial, technical and/or human) could be a possible suggestion. Alternatively, the Bulgarian political agenda might just not have prioritised cyber offensive capabilities. Admittedly, developing offensive cyber capabilities would make Bulgaria a much more attractive target in cyberspace, as evidenced by the way the UK is being targeted.

In a broader sense, however, the lack of developing cyber offence capabilities suggests a clear divide between those MS pulling the train towards power-projection and developing relevant laws applicable to cyberspace and those being in the wagons, expecting others to lead. Either way, there is an obvious difference how Bulgaria has approached the issue - develop the minimum of capabilities required by the EU - compared to the UK, which has explicitly admitted of performing offensive cyber operations on adversaries,[973] and to a lesser extent, Italy, whose Cybersecurity Agency was set up in 2021, incorporating the Cybersecurity Unit and the CSIRT

[973] Dan Sabbagh, 'Britain has offensive cyberwar capability, top general admits' *The Guardian 25 September 2020* <https://www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits> accessed 3 July 2021.

(as seen in Section 5.5.2.). This makes for another issue on which Bulgaria is lagging behind, not only legally, but also operationally and technically thereby highlighting again the scope for the EU act to iron out the discrepancies between the MS.

6.6. Conclusion

In a short piece taken from his monograph Fancy Bear Goes Phishing, Scott Shapiro wrote that "[i]n the 1980s, there was no better place than Bulgaria for virus lovers" and that the country was "one of the hottest hi-tech zones on the planet".[974] Shapiro also noted, however, that "security was not a priority or even a necessity" back in the 1980s.[975] Bulgaria quickly became a country producing many viruses that were not only also sophisticated, but also destructive. As a comparison, Shapiro claimed, few Americans were familiar with computer viruses at the time.[976]

But the cold-war grandeur of the Bulgarian technological realm is long forgotten. The virus-developer giant has become a cybersecurity dwarf. Admittedly, cybersecurity is a very niche and small part of the technological realm, but prior to the transposition of the NIS Directive, Bulgaria's overall cybersecurity knowhow – institutional, technical and legal - was embryonic. The lack of such knowhow was probably among the reasons why in the 1980s creating computer viruses became so popular in Bulgaria: when the law says nothing against it, it is very easy to exploit underexplored areas.

Examining the pre-NIS Directive state-of-play demonstrated the gaps in the legal preparedness and consecutive institutional challenges: who did what and how in the field of cybersecurity was not clearly defined. The lack of sources also speaks to the level of preparedness: the topic of securing the online domain from cyber threats was never a top-of-the-agenda political issue and, as a consequence, there was very limited debate on its relevance, on the effectiveness of the strategic approach, on the concerning issue of being one of the most unprepared EU countries. The EU's role in filling these regulatory gaps was hence crucial if Bulgaria wanted to improve its

[974] Scott J Shapiro, 'On the trail of the Dark Avenger: the most dangerous virus writer in the world' *The Guardian* (9 May 2023) <https://www.theguardian.com/news/2023/may/09/on-the-trail-of-the-dark-avenger-the-most-dangerous-virus-writer-in-the-world> accessed 30 August 2023.
[975] Ibid.
[976] Ibid.

cybersecurity legal (and not only) preparedness. The Bulgarian case study further evidenced that without a supranational body to lead the way and shape its regulatory agenda, it would have remained an unprepared state, becoming fertile soil for attackers. The EU's role as a key regulator on cybersecurity has therefore been of key importance for the states with low level of preparedness, as seen in Sections 3.3.1.2. through 3.3.1.3.

Chapter VII: CONCLUSION

7.1. Overview

This final Chapter concludes this thesis by answering the research question and sub-questions posed in the introduction, and by summarising the main findings of the work, as well as their original contributions to knowledge.

Sections 7.2. through 7.4. will be based on the substantial Chapters (II through VI) of this thesis. A brief overview of the main discussions in Chapters II and III will be provided in Sections 7.2.1. and 7.3.1. respectively, before these Chapters' findings – and their relation to the research questions – will be highlighted in Sections 7.2.2. and 7.3.2. respectively. The three case study Chapters analysing the MS will be addressed together in Section 7.4., to more easily enable the highlighting of the similarities and differences that research into them revealed. The gaps in the MS' legal frameworks and what they tell about the EU's role as a cybersecurity regulator identified throughout Chapters IV through VI will be analysed in Section 7.4. Ultimately, this Chapter will conclude with Section 7.5. by considering the final research sub-question as set out in Section 1.2.: can the EU claim the role of a cybersecurity regulator?

7.2. The theoretical background: analysing the EU regulatory approach to cybersecurity 'inside-out'

7.2.1. Overview

Chapter II provided the theoretical background to the reminder of the project. It began with an outline of debates and regulatory advances at international level, to set the scene within which the EU approach has been developing. The Chapter provided the context of why regulating cybersecurity and cyberspace has been so difficult. The international community's decision-makers and scholars struggled for years to agree on how to interpret existing international norms

in relation to cyberspace, how to define state-sponsored cyberattacks, how and whether real-life attacks violated existing principles of international law such as violation of sovereignty or non-intervention and what the lawful response to such attacks could be.

The Chapter thus allowed for the assessment of the EU regulatory regime 'inside-out', a benchmark against which the EU's approach could be compared to. The analysis in Chapter II was hence the first step towards evaluating the effectiveness of the EU regulatory regime: without knowing what debates were taking place outside of the EU and what other states' positions and interpretations of malicious state-sponsored cyberattacks were, it would have been difficult to assess the regulatory efforts of the EU. Furthermore, Chapter II enabled comparing the EU's approach against the international background so as to demonstrate how the latter impacted the former; in other words, Chapter II made it possible to consider the international cyber-agenda as a possible 'external' influence on the EU.

7.2.2. Summary of Findings

The analysis in Chapter II lead to several important findings. First, the 2020 EU Cybersecurity Strategy emphasised the need to develop an official EU position on the applicability of international law to cyberspace.[977] The EU has since actively participated in discussions at UN level: in its Statement about international law at the UN Open-Ended Working Group on ICT in March 2023, the EU acknowledged that "states should apply international law to cyber activities" and that there were "examples of states violating international law via cyber means"[978] (without further elaborating on which states). It further emphasised the "need for further study on how and when the principles of humanity, necessity, proportionality and distinction apply" to the use of ICT by States.[979] Despite, therefore, not having an official position on international law's applicability to cyberspace, the EU did appear to be mandated by its MS to deliver statements

[977] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* 20.
[978] Delegation of the European Union to the United Nations in New York, *EU Statement – UN Open-Ended Working Group on ICT: International Law* (24 May 2023).
[979] Delegation of the European Union to the United Nations in New York, *EU Statement – UN Open-Ended Working Group on ICT: International Law* (8 March 2023).

like this. As Delerue and Géry observed, the EU could evidence how the MS' approaches (of those MS that have adopted their views on how international law applies to cyberspace)[980] were not challenging the capacity to cooperate collectively – in and outside of the EU.[981] Delerue further stated that there was a "significant degree of convergence" among the MS' approaches to the applicability of international law to cyber operations.[982] This, however, provides for an overly simplistic account as, as this thesis and more specifically Sections 3.3.1.2. through 3.3.1.3. have evidenced, there has been very little convergence between the MS especially during the development of the network and information security (NIS) and cyber diplomacy fields. Delerue's observation implied that the interpretation of international laws' applicability was not a contentious issue among the MS. If that were entirely true, the EU would have already provided its views on whether certain cyber operations violate international law and how, and what the lawful response to these operations could be – for instance, in terms of self-defence, countermeasures or retorsions. This has not yet been the case.

Second, on defining cyber operations concretely, interestingly, the EU seems to have put limited attention on defining the spectrum of cyberattacks (as defined in Sections 2.3. through 2.3.4.). Identifying whether a specific operation was a cyber espionage or an international cybercrime operation, for instance, has never been a priority for EU regulators. However, not doing so has caused limitations specifically in the cyber diplomacy and cyber defence fields (se seen in Sections 3.3.2. through 3.5.) thereby undermining both their development and relevance for the overall EU cybersecurity regulatory agenda. More recently, an EU infographic presented the main threats: ransomware, DDOS, malware, supply chain attacks and disinformation.[983] But classifying cyberattacks like this missed the point – whether they were politically motivated (state or non-state actors-led) was not reflected. As acknowledged in Section 3.4., the fact that cybersecurity and other key cyber terms were interpreted differently across the MS (as further demonstrated in Sections 4.2.1. and 4.2.4.1. for the UK, Sections 5.3.1.1. and 5.4.1. for Italy, and

[980] As of summer 2023 ten MS have adopted an approach how international law applies to cyberspace: Czech Republic (2020), Estonia (2019, 2021), Finland (2020), France (2019, 2021), Germany (2021, 2021), Italy (2021), Netherlands (2019, 2021), Poland (2022), Romania (2021), Sweden (2022).

[981] François Delerue and Aude Géry (eds), *International Law and Cybersecurity Governance* (EU Cyber Direct 2022) 18.

[982] François Delerue, 'Toward an EU position on the application of international law in cyberspace' (2023) EU Cyber Direct 3.

[983] Council of the EU, 'Infographic - Top cyber threats in the EU' (2022) <https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/> accessed 15 January 2023.

6.2.4. and 6.3.1. for Bulgaria) had its consequences mainly because how the threat was interpreted would influence what response could be justified.[984] An observation from the dawn of the developments of the EU regulatory regime (2015), yet, eight years later, it has not been taken on board. Hence, if the EU wants to demonstrate coherence and understanding of the applicability of international law to cyber operations and advance its own EU-level position on it, it is recommended that it adopts definitions on the different types of cyberattacks, for example based on the succinct criteria set out in Chapter II, which identified four main types of state-sponsored cyberattacks: international cybercrime, cyber espionage, cyber *use of force* and cyber armed attack (Sections 2.3. through 2.3.4.). This would become the basis upon which the EU official position on state-sponsored cyber operations and the role of international law would be built. In addition, it would open the way for the EU to be more assertive in attributing attacks to foreign states *and* become a more confident cybersecurity regulator.

Third, an interlinked issue arose from the lack of clear-cut definitions of cyberattacks at EU level: the EU has also given limited attention to assessing whether an attack – e.g. the WannaCry, NotPetya, SolarWinds, COVID attacks on the health sector – has violated any international law principles such as the territorial sovereignty of the MS, or the principle of non-intervention. However, discussions by EU scholars and decision-makers about whether any of the abovementioned attacks violated any international law principles have never been as extensive as the (mainly US-led) discussions which surrounded the DNC hack for instance (as seen throughout Chapter II). But when an operation is not defined, a lawful response to it is also undefinable: Sections 2.2.2.1. through 2.2.2.2. have explored in detail the available responses to states fallen victims to cyberattacks, but these can only be applied if an operation has been clearly defined as an international wrongful act and, if possible, what international principles specifically have been violated. Thus, in terms of developing possible lawful responses to state-on-state cyber operations such as self-defence or countermeasures, the EU has also lagged behind. This calls for the development of an EU cyber defence posture. However, while initially addressed as a key pillar in the 2013 Cybersecurity Strategy, and despite occasional efforts to resuscitate it (as seen in Section 3.4.) regulatory measures in the cyber defence area never developed and the focus has never been on the interpretation of how MS collectively or the EU

[984] European Parliament and Directorate-General for Internal Policies, *Cybersecurity in the European Union and Beyond Exploring the Threats and Policy Responses* (2015) 15.

itself would respond lawfully to a state-sponsored operation: interpreting how international law principles such as the right to self-defence apply to such cyberattacks had always fallen out of the scope of the EU cyber defence approach. Resilience, not defence, has remained the key goal of the EU approach to cybersecurity. This, however, clearly undermines the contribution the EU can have in developing the applicability of international law to state-on-state cyber operations and could indirectly impact its ambitious for becoming a cybersecurity regulator.

To sum, the level of maturity of the EU approach on the applicability on international law is therefore low, a view shared also by Delerue.[985] The EU approach does not exist in a vacuum – its regulatory approach must follow international developments if it wants a framework fit for purpose. How the EU sees international law does not appear to be a priority on the policy and regulatory agenda, but looking at cybersecurity more holistically, it is recommended that the EU engages in further work on this topic. The EU cannot claim the role of a coherent cybersecurity regulator if it is concerned neither about the source of the attack, nor about the response. The international developments followed in Chapter II therefore could serve as guidance, as a 'handbook' for the EU to consider when developing its regulatory approach to the applicability of international law to state-sponsored cyber operations.

7.3. The MS as protagonists: analysing the EU regulatory approach to cybersecurity 'bottom-up'

7.3.1. Overview

Chapter III of the thesis considered the EU regime, providing specific focus on the 'bottom-up' approach, by focusing on the role of the MS and their representatives in Brussels in shaping the EU's regulatory regime. In 2013, the first Cybersecurity Strategy mapped out the future cybersecurity developments splitting them into three standalone pillars – NIS, law enforcement and defence. With time, the NIS pillar developed into a significant regulatory focus: at the time when the international community was discussing whether new laws needed to be specifically

[985] Delerue, 'Toward an EU position on the application of international law in cyberspace' 4.

adopted to address cyberthreats, the EU did not hesitate and put forward its proposal for NIS Directive with the aim of safeguarding the internal market from the impact of cyber operations. The regulatory approach's core therefore laid in the continuous economic prosperity of the EU, by removing the hurdles and threats that might interfere with it. Security subsequently also became a key element, but it was not the focus. It was merely the *means* via which the EU was trying to protect its economy. To the developing NIS pillar, cyber diplomacy was added in 2017 as an approach: the EU was trying to address cyber threats from a different angle and was slowly advancing its *collective cybersecurity* agenda.

The Chapter put the MS in the spotlight and it analysed their contribution to the EU regulatory approach. The developments of the latter were hence seen from the prism of the MS. The analysis observed how the MS (in the face of MEPs, government representatives, (cyber)security agencies' representatives) actually differed a lot in their views on cybersecurity and how their interpretations of the cyberworld led them to disagree with each other and at times even position themselves against the EU. The Chapter analyses therefore the horizontal dimension of this contestation of power and mistrust (between the MS) and the vertical dimension (between the MS and the EU) and how these shaped the regulatory measures as they are today. The EU clearly wanted to lead the way, but so did some MS with an already high level of cybersecurity legal and technical preparedness, such as the UK. Other states such as Bulgaria, which had low level of legal preparedness, relied on the supranational body to be the locomotive so they could, as it were, hop on the wagons. British and Bulgarian representatives in Brussels proved very active – representing opposing views, reflecting the already existing cybersecurity preparedness or the lack thereof respectively. Nonetheless, with both its NIS and cyber diplomacy regulatory steps (called "securitising moves" as per Barry Buzan, Ole Wæver and Jaap de Wilde's securitising theory), the EU was slowly but steadily signalling its ambitions to become a cybersecurity regulator.

7.3.2. Summary of Findings

The aim of Chapter III was to evaluate the emergence of the EU as a potential prominent cybersecurity regulator, and, specifically, to consider the evolving challenges and limitations of achieving this task. The research produced a number of key findings.

First, Chapter III discovered that the biggest hurdle to the EU's ambitions to become a cybersecurity regulator did not lie outside of the EU, but inside. Continuous state-sponsored attacks (such as the WannaCry ransomware, the NotPetya attack, the SolarWinds hack) have had little impact on the trajectory of the EU's legal approach. The fact that like-minded states such as the US and the UK, even when it was still a member state, have attributed attacks to Russia for instance (e.g. WannaCry) have not prompted the EU to actually attribute them as well. Further, despite cybersecurity gaining prominence during the first months of the COVID pandemic, the latter seems to have not been a key element in the development of the EU 2020 Cybersecurity Strategy[986] and did not push the EU to have a stronger voice in calling out perpetrators.

Some MS have had a much bigger impact on the EU developments of its security legislation. Thus, it is more the internal pressure exercised by its own MS, rather than external pressure, that have influenced the EU's cybersecurity legislative frameworks' trajectory. It is the MS that have hindered a better integration in the NIS framework, and lack of agreement on potential EU-level attribution in the cyber diplomacy framework, that have shaped the EU's strategic and legal approaches. As of summer 2023, despite MS having adjusted more to the idea of the EU being in the driver's seat on the subject of cybersecurity, the cyber diplomacy pillar continues to be underdeveloped thereby indirectly undermining the credibility in the EU regulatory approach.

Second, it needs to also be emphasised that the mere adoption of an EU cybersecurity-related laws ("securitising moves") does not "create" a solid legislative framework, but it is the implementation and enforcement of those measures that counts – a perennial problem in law, not limited to cybersecurity. Here, again, all problems identified point to the MS and their continuous efforts to make the EU regulatory framework viable. Being a cross-border issue, MS needed to acknowledge that more integration and better cooperation is the way forward. MS with low level of preparedness could – and can still - benefit from the more prepared states'

[986] Carrapico and Farrand, 1123.

experience and learn from them how to better enforce the laws, how to encourage and monitor compliance efficiently. Unequal capabilities would not be as big of a hurdle if there were more trust - though, admittedly, if there were more trust, capabilities would not be as unequal. Trust would enable more sensitive information sharing, which again, can only be beneficial for those MS with low level of preparedness because it would also entail knowledge sharing. Without trust there cannot be knowledge sharing, and without knowledge, legal and technical knowledge capabilities cannot develop further, creating a vicious cycle.

To overcome this, the way forward could be to create a cycle of trust, where the less prepared states are helped mastering the peculiarities of cybersecurity at the necessary level. Easily achievable on paper, implementing this recommendation on bridging the gap between the MS's and the EU's cybersecurity objectives would be difficult, as (the ten-year-old EU regulatory cybersecurity) 'history' shows that some MS simply cannot overcome their national concerns to serve the EU's priorities in the field of cybersecurity (as viewed in Sections 3.3.1.2. through 3.4.1.).

7.4. The case studies: the UK, Italy and Bulgaria

7.4.1. Overview

The next three Chapters, analysing the three case studies, embraced a 'top-down' approach, by considering how the EU framework was implemented in the three MS chosen for analysis. This allowed for a better understanding of MS's actions during the negotiation process on the EU regulatory measures, but it also evidenced *why* exactly there was a need for EU regulatory measures. MS's preparedness has been grouped into three levels – high, medium and low level of preparedness. Three MS have been chosen to represent each group – the UK, Italy and Bulgaria respectively.

First, prior to the adoption of the NIS Directive, the three MS had very different elements in their 'cybersecurity'-regulatory puzzles: the UK's framework (analysed in Sections 4.2. through 4.2.3.) was composed of computer misuse laws, and laws on equipment interference (EI) and interception of communications on devices located abroad. Cybersecurity and foreign-sponsored

cyber threats were first acknowledged in 2008 with the National Security Strategy, and the first Cybersecurity Strategy, published in 2009, acknowledged that "the most sophisticated threat" in cyberspace came from states. The 2010 National Security Strategy further identified malicious state-sponsored attacks against the UK and "large scale cyber crime" as a Tier One threat to national security.[987] Key concepts such as cybersecurity, cybercrime, computer network exploitation, active cyber defence and cyber threats were defined later on, with the 2016-2021 Cybersecurity Strategy.[988]

Italy's 'cybersecurity'-regulatory puzzle (analysed in Sections 5.2. through 5.3.3.) had fewer components: it had some 'unlawful computer activity'-related provisions in the Penal Code and two administrative acts – the Monti and Gentiloni decrees - on CI protection. The first National Strategic Framework for Cybersecurity of 2013 acknowledged that some states were already capable of penetrating other states' networks,[989] and also defined cybercrime, cyber espionage, cyber terrorism and cyber warfare.

Bulgaria 'cybersecurity'-regulatory puzzle (analysed in Sections 6.2. through 6.2.6.) had only two components: it had 'unlawful computer activity'-related provisions in the Penal Code and a Cybersecurity Strategy adopted in 2016 which defined key terms such as cybersecurity, cyberspace, cyber threat, and cybercrime.

Second, later on, when the EU had already adopted its 2013 Cybersecurity Strategy and when some MS had already taken some legislative measures – but before the NIS Directive has come into force in 2016 - the legal preparedness level was also reflected in the institutional infrastructure of who did what in cybersecurity in the different MS. In the UK, it was the GCHQ performing all things cyber and, as of 2016, the National Cyber Security Centre (NCSC) (with the GCHQ still being its mother organisation) operating on the defence and CI protection side and the National Cyber Force (NCF), as of 2020, operating on the offensive side (but still under the GCHQ umbrella) (as seen in Sections 4.2.3.). In Italy, instead, the picture was rather fragmented, with many bodies – the PM, the PM's military council, the Interministerial Committee for the Security of the Republic, the Cybersecurity Unit – all assigned cybersecurity

[987] Government 27.
[988] HM Government, *National Cyber Security Strategy 2016 - 2021* 74.
[989] Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *National Strategic Framework for Cybersecurity (Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico)* 15. Translation taken from the English version of the document.

responsibilities (as seen in Sections 5.3.1.3. through 5.3.2.1.). In Bulgaria, because of the lack of legal measures on the matter, no body or intelligence agency had been assigned *sensu stricto* any cybersecurity responsibilities, though some intelligence agencies - the State Agency for National Security and the General Directorate for Fighting Organised Crime in the Ministry of Interior had remotely related responsibilities (as seen in Section 6.2.5.).

This brief overview reflects broadly the levels of legal preparedness in cybersecurity across the EU MS: some (e.g. the UK) were leading the way with a very mature legal and strategic approaches, some (e.g. Italy) had done some work towards the better understanding of the cyber threats phenomenon, but others (e.g. Bulgaria) had done very little and seemed very unprepared – legally, strategically and, consequently, operationally.

Against this reality across its MS, the EU had to adopt a law to harmonise these huge discrepancies if it wanted to be prepared to face the threats coming from cyberspace.

7.4.2. Summary of Findings

7.4.2.1. Pre-NIS Directive findings

The comparative approach across Chapters IV through VI lead to several findings. First, the primary element the three case studies had in common was that online crimes developed first within criminal law: what is known today as cybercrime or illegal access to or interference with devices and systems. But similarities only went this far. Whilst the UK adopted a new law back in 1990 – the Computer Misuse Act, Italy and Bulgaria merely amended their respective Penal Codes, in 1993 and 2002 respectively. This 20-year lag in addressing a criminal matter demonstrated how little attention was paid to cybersecurity in Bulgaria. By the time Bulgaria had taken its first baby steps, the UK's framework was already multilayered, with existing legislation providing the legal basis for EI (or offensive cyber) abroad (namely section 7 of the ISA 1994, which, however, only became the legal basis for EI in 2001, as per amendment made to the law by section 116 of the Anti-terrorism, Crime and Security Act 2001), as seen in Section 4.2.1.3.C)i)).

Second, despite different levels of preparedness, all three MS had to wait for the NIS Directive's respective transposition laws to introduce legally binding measures on CI protection. That said, here Italy takes the leadership position with the Monti and Gentiloni decrees (Sections 5.3. through 5.3.3.), which focused precisely on CI protection from cyberattacks. Despite being administrative acts, they still had added value as they laid the ground for further work and for the development of a cyber-culture and understanding in Italy. Italy, therefore had a head start with the preparatory work it had done. Interestingly, although having a very well-developed legal approach and operational capacities, the UK framework lacked a law on CI sectors' protection. This was evidenced with the WannaCry ransomware, which hit the UK NHS more than other public or private bodies across the EU (as seen in Section 4.2.2.). At the time of the attack – spring 2017 – the NIS transposition law was still in the works. The attack evidenced the gap in the UK regulatory framework as regards protecting CI sectors from cyberattacks and, more importantly, demonstrated the added value of the NIS Directive for the national legal frameworks.

To sum, these observations evidenced the profound differences between the three MS chosen as case studies. An EU in the driver's seat would entail adhering to the EU views and perceptions of how cybersecurity needed to be addressed, in some cases slowing down or changing the direction of individual MS's approaches – an avenue states such as the UK did not want to take willingly (as observed in Sections 3.3.1.2. through 3.3.1.3.). The larger and more prepared MS had valid arguments against too much integration in this regulatory field. The comparative study also put into context the UK's trust issues and concerns as regards mandatory information sharing among the MS (seen in Sections 3.3.1.2.B)i) and 3.3.1.2.B)ii)). Yet, whilst trust issues were not groundless, the bigger concern was that with cybersecurity being a part of national security, unpreparedness in any member state meant potential consequences for the highly prepared states too due to the borderless nature of cyberattacks. This meant that *not* having an EU approach which would encourage cooperation, joint action and common understanding of the threats, could impact *all* MS negatively, regardless of their individual preparedness. The comparative analysis thus showed the benefits and the drawbacks as regards an EU-level cybersecurity regulatory approach, but it also demonstrated why the benefits outweighed the drawbacks.

7.4.2.2. Post-NIS Directive findings

Summarising the comparative analysis conducted on the post-NIS Directive developments lead to the following key findings.

First, the need for a harmonisation of the legal frameworks was evident, but to what extent was it achieved? The NIS Directive's purpose to create a harmonised approaches among the MS as regards the vulnerability of the CI sectors to cyberattacks was somewhat achieved, at least on paper. The role the NIS Directive played in the examined national frameworks was, however, very different. In the case of states with high level of preparedness such as the UK, it was simply another piece in the cyber regulatory puzzle. On the other side of the spectrum, where the states with low level of preparedness such as Bulgaria were found, the NIS Directive laid the long-overdue basis for a cybersecurity regulatory framework. In the case of MS like Italy, it was a much-needed tool to crystalise or consolidate existing rules and to align them with the broader EU goals for CI protection. The EU regulatory efforts aiming at harmonising existing frameworks were thus essential.

Second, although the EU approach has bridged the regulatory gaps between the MS to a large extent, the comparative analysis concluded that after ten years of continuous EU efforts for more integration, the MS kept moving at their own pace and, seemingly, in different cyberspaces (metaphorically speaking). Post-Brexit, the UK has not been advancing further regulatory measures in the field of CI protection from cyberattacks. Once liberated from the EU regulatory chains, the UK could once again pursue its own national security objectives. The NIS2 Directive, upon transposition by the MS, will bring even stronger cybersecurity awareness and resilience of the CI sectors, whilst the UK's review of its NIS Regulations, which has a much smaller scope, will likely not bring the same result. Italy, on the other hand, has been developing its approach much faster than the EU – and, surprisingly, the UK. Its Cybersecurity Perimeter is a promising regulatory framework, that, in the absence of the UK, could potentially put Italy on the list of the states with high level of preparedness. On the other hand, Bulgaria, as per its tradition in the field, is waiting for the EU to push further so it can advance its national framework.

Whilst the EU has never precluded the MS to pursue their own national views (the *directive* nature of the key legislative measures demonstrated this) and the development of national

approaches is welcomed in the sense that it is the national level of preparedness that influences the EU's *the most* (as seen throughout Chapter III), for the EU to become a solid cybersecurity regulator, MS need to move along the same line – or, at least, in the same cyberspace (again, metaphorically speaking). Having MS with different levels of preparedness will always remain the reality (and not only in cybersecurity), but it is important that discrepancies are not as huge as they were prior to the adoption of the NIS Directive. The EU can push further its regulatory agenda only when its own MS have embraced it and have benefited from it to the extent that cross-border cyberattacks have very little impact on the internal market.

To conclude on the relevance and the effectiveness of the EU regulatory regime to the NIS pillar, and what the MS's comparative analysis has demonstrated about it, it is evident that the EU has solidified its regulatory agenda to the extent that its role as a leader, despite the initial contestation of power, has now been endorsed by its MS. This makes the EU a solid NIS regulator (although imperfect, as per Christou's definitions in Section 3.2.1). Considering the nature of the topic in general, where so much of MS's national security is at stake, being an "imperfect regulator" is still better than not being a regulator at all. But while the NIS pillar has been successfully developed, what has not followed at the same pace, has been the cyber diplomacy approach, the shortcoming of which and its impact of the overall *cybersecurity* regulatory agenda of the EU is explored in next Section 7.5.

7.5. The EU cybersecurity regulatory regime: shortcomings and the way forward

This final section will address some overarching cybersecurity issues and how the EU and the MS addressed them.

7.5.1. Cyber diplomacy's shortcomings: attribution

As concluded in Section 7.4.2.2. the EU has solidified its position as a NIS regulatory authority. But shortcomings to its cyber diplomacy persist thereby undermining its ambitious to become a strong *cybersecurity* regulator.

To better exemplify the hurdles in the cyber diplomacy domain – and its weak spot: attribution - the thesis has used the cyberattacks on the health sector during the first months of COVID (among other examples) as a case study (Section 3.5.). The health sector was one of the seven sectors covered in the NIS Directive, but with COVID successful attacks on the health sector in the EU spiked. This is because many health institutions covered by the EU law had not effectively implemented the appropriate cybersecurity measures. But malicious actors also kept performing these attacks because there was no actual deterrent, there was no actual moment where the EU officially attributed some of the attacks to foreign states. This again refers the discussion to the capabilities of the individual MS.

As seen in Section 4.3.5.1., the UK, even when still a member state, never felt that it had to wait for the EU to attribute cyberattacks (such as WannaCry, NotPetya, the DNC hack, attacks on the UK energy sector) to foreign states. Italy and Bulgaria have not, to this date, attributed any, despite Italy having an official position on the applicability of international law to cyber operations. "Italy deems that attribution is a national sovereign prerogative and so is the decision to make it public or not", states the Italian Position Paper.[990] This suggests that it is rather unlikely that Italy takes the UK's seat on the table of the MS leading and shaping the EU approach to cyber operations. Having a developed regulatory framework is not enough. For Italy to become a cyber leader like the UK, it needs to be bolder on attribution. That said, the different positions on attribution show also why there has seemingly been sluggish progress of the EU cyber diplomacy approach. Since the EU does not have its own intelligence gathering competences and capabilities (as seen in Section 3.3.2.1.), it relies on the MS's. But an EU action *and* a MS action on the same issue are not mutually exclusive.[991] Hence if there is no EU-level action, it means that the MS did not see eye-to-eye on that particular attack, further confirming their different capabilities and giving precedence of national security objectives over the EU's.

Another reason for the lack of progress on the EU cyber diplomacy agenda could be – indirectly - Brexit. It is clear that because of Brexit, the EU has lost a major cyber player, despite the UK continuously blocking the EU's more ambitious regulatory agenda (seen in Sections 3.3.1.2. through 3.3.1.3.). Knowledge and practical experience are key for mitigating cyber threats, and losing access to the British intelligence gathering capabilities meant losing access to information

[990] Ministero degli Affari Esteri e della Cooperazione Internazionale 5.
[991] Council of the EU, *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox* (8 June 2023) 7.

potentially not retrievable by any of the other MS. Even if suspicions are very strong, the lack of intelligence demonstrating who was the perpetrator would be the key concern - and MS would be reluctant to pursue an EU-level response to avoid that attribution backfires. Hence, whilst very speculative, the lack of progress on EU cyber diplomacy could be also indirectly linked to Brexit.

To sum, developing MS's national approaches is very important as in cyberspace one cannot predict what will happen tomorrow. At the same time, MS need to also work on the EU cyber diplomacy approach. These are not mutually exclusive, they are complementary. MS should not shy away from focusing on cyber-cooperation within the EU whilst advancing their won cybersecurity agendas and objectives because if after a successful attack the perpetrators are not called out, they will be emboldened to continue performing such attacks. This thesis hence continues to highlight that for the overall cybersecurity approach to be fully effective, the cyber diplomacy approach needs to further advance too: so far the cyber diplomacy toolbox's implementation has no lived up to the expectations due to the MS giving precedence of their national interests. Whilst attribution in itself is not a deterrent,[992] if done collectively, it sends a stronger message, it signals a unified EU voice. If not done at all – the message is also clear – the EU does not speak with a unified voice and shies away from taking an official position.

7.5.2. Has the EU become a cybersecurity regulator?

This final section will provide a wrap-up analysis of all findings so far, with the aim of concluding whether the EU has achieved its ambitions to become a cybersecurity regulator.

Regulating cybersecurity is more complex than just the development of the different pillars that make up cybersecurity: NIS, law enforcement, cyber defence and cyber diplomacy. The EU has been consolidating its NIS regulatory approach with some significant amount of legislation on the CI sectors protection from cyberattacks, but this does not imply that it has become either a coherent or a solid *cybersecurity* regulator (as observed in 7.4.2.2.). Fragmentation might have been the preferred choice for regulation, as regulating a "smaller" field is easier than regulating

[992] Eichensehr, 553.

cyberspace, but the big picture should always be considered. So far, the NIS pillar has been developing with a significant speed and much faster than cyber diplomacy (cyber defence is not even mentioned as in such embryonic state) but having a more comprehensive approach to interpreting cyberattacks is key. The EU cannot have an effective cybersecurity regulatory regime that only pursues the development of the NIS pillar (despite having successfully done so as observed in Sections 7.3. through 7.4.2.2.), because the latter is not enough to deter malicious foreign sponsored attacks. To add to Carrapico & Barrinha conclusions on the coherence of the EU approach to cybersecurity,[993] it could be added that being a coherent regulator would also entail equal efforts in the other sub-fields of cybersecurity. The EU cannot be a coherent *cybersecurity* regulator if only its NIS framework advances and the other pillars do not. If the EU wants to be a *cybersecurity* regulator, it needs to put some significant work into further developing its cyber diplomacy *and* cyber defence approaches through the adoption of more "securitising moves" (as suggested in Sections 3.3.2.1. through 3.4.1.). Developing a common foreign policy on cyber operations (and the related aspects of developing an official position to the applicability of international law to cyber operations) has been problematic because of the problematic area of EU foreign policy regulation in general (as observed in Section 3.3.2.). Hence, the EU might simply decide not to put any additional efforts to its development. This would not undermine the relevance of its NIS framework, but it would mean that the EU would not be able to call itself 'a *cybersecurity* regulator'.

To sum, the shortcomings of the existing EU regime, heavily emphasising on the NIS pillar, make it imperfect to the extent that 'exporting' its *cybersecurity* regime would appear difficult. It is more likely that some states take what they consider best of it and develop it in view of their national interests - which, itself is a successful export. The shortcomings of any legislative framework will always exist. Thus, if the EU wants to have an impact *internationally,* it should push for more integration in all cyber pillars. Developing only of the NIS pillar is sufficient only for the internal dimension of the EU regulatory efforts in cybersecurity.

[993] Carrapico and Barrinha.

Research hence concludes, and this thesis reinforces, that whilst the EU has been solidifying its cybersecurity body of law, it cannot be argued that the Brussels effect[994] applies to the EU's overall cybersecurity agenda as yet. Whist it can claim the role of a NIS regulator, there is still a long way to go for the EU to claim a *cybersecurity* regulatory power status. It could be argued that the EU has the potential of achieving this, if it continues to persist with the securitisation processes in all cybersecurity pillars.

[994] The Brussels effect is a notion, advanced by Prof. Anu Bradford. Focusing on the economic dimension, she argues that EU norms in areas such as data protection, environment, consumer protection, among others, have become global standards. For more details view Anu Bradford, The Brussels Effect: How the European Union Rules the World, OUP 2020.

BIBLIOGRAPHY

Krasikov DV and Lipkina NN, *Sovereignty in Cyberspace: A Scholarly and Practical Discussion* (Advances in Social Science, Education and Humanities Research 2020)

Commission E, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union* (13 September 2017)

——, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (13 September 2017)

Government HM, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (2010)

Parliament E and Policies D-GfI, *Cybersecurity in the European Union and Beyond Exploring the Threats and Policy Responses* (2015)

Armstrong D, Farrell T and Lambert H, *International law and international relations* (2nd edn, CUP 2012)

Brownlie I, *International law and the use of force by States* (Oxford, Clarendon Press 1963)

Buchan R, *Cyber espionage and international law* (Oxford, UK, Hart Publishing 2018)

Buzan B, Wæver O and Wilde Jd, *Security : A New Framework for Analysis* (Lynne Rienner Publishers 1998)

Chen L-c, *An introduction to contemporary international law: a policy-oriented perspective* (2nd edn, New Haven: Yale University Press 2000)

Christou G, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* (Palgrave Macmillan 2016)

Delerue F, *Does International Law Matter in Cyberspace?* (CUP 2020)

Dimov PS, *Application of web technologies for the protection of national security (Приложение на уеб технологиите за защита на националната сигурност)* (DioMira 2018)

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012)

Gori U, *Cyber Warfare 2017. Information, Cyber and Hybrid Warfare: contents, differences, applications (Cyber Warfare 2017. Information, Cyber e Hybrid Warfare: contenuti, differenze, applicazioni)* (Franco Angeli 13 September 2018)

Guzzetta G and Marini FS, *Lineamenti di diritto pubblico* (Giappichelli - Torino 2014)

Hodgson QE, Shokh Y and Balk J, *Many Hands in the Cookie Jar: Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response* (RAND Corporation 2022)

Kochi GF, *Computer crimes in Bulgarian and Albanian criminal law (Компютърните престъпления по Българското и Албанското Наказателно право)* (Sofia University Faculty of Law 2016)

Politi F, *Diritto Pubblico* (Giappichelli – Torino 2010)

Prucher J, *Brave New Words: The Oxford Dictionary of Science Fiction* (OUP 2007)

Rid T, *Cyber War Will Not Take Place* (OUP 2013)

Romaniuk S and Manjikian M, *Routledge Companion to Global Cyber-Security Strategy* (2020)

Sanger DE, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown Publishing Group, Division of Random House Inc 2012)

Stürchler N, *The threat of force in international law* (Cambridge: Cambridge University Press 2007)

Sylvia de Mars, *EU law in the UK* (OUP 2020)

Ziccardi G, *Cyber Law in Italy, 3rd edition* (Kluwer Law International e-Book January 14 2020)

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (1986) (International Court of Justice)

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement (1986) (International Court of Justice)
Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) (International Court of Justice)
Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (ICJ Reports 2005)
Privacy International and Greennet & Others v.s (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters [2016] (Investigatory Powers Tribunal)
Delerue F, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' (13th International Conference on Cyber Conflict (CyCon))
Kosseff J, 'Retorsion as a Response to Ongoing Malign Cyber Operations' (12th International Conference on Cyber Conflict (CyCon) 2020)
Schmitt MN, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' (Proceeding of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy)
Shukla M, Johnson SD and Jones P, 'Does the NIS implementation strategy effectively address cyber security risks in the UK?' (2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security))
Biscop S and Andersson JJ, 'Introduction' in *The EU and the European security strategy: Forging a global Europe* (Routledge 2008)
Bosakova K, 'Cybersecurity – concepts, policies and strategies' in Denchev S (ed), *Information and Security* (Za bukvite – O pismenehu 2019)
Brenner SW, '25 - History of computer crime' in Leeuw KD and Bergstra J (eds), *The History of Information Security* (Elsevier Science B.V. 2007)
Hardy K and Williams G, 'What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism' in Chen TM, Jarvis L and Macdonald S (eds), *Cyberterrorism Understanding, Assessment, and Response* (Springer 2014)
Herrmann D, 'Cyber Espionage and Cyber Defence' in Reuter C (ed), *Information technology for peace and security: IT applications and infrastructures in conflict, crises, war and peace*, vol 36 (Routledge 2020)
Lavorgna A, 'Brexit and Cyberspace: Implications for Cybersecurity' in Berthélémy CNa (ed), *Brexit and Internal Security Political and Legal Concerns in the Context of the Future UK-EU Relationship* (Palgrave Macmillan 2019)
Lindsay JR, 'Cyber Espionage' in Cornish P (ed), *The Oxford Handbook of Cyber Security* (Oxford Academic, OUP 2021)
Porcedda MG, 'Brexit, Cybercrime and Cyber security: From 'Block Opt-Out' to 'Creative Opt-Ins' in the AFSJ and the Internal Market?' in Berthélémy CNa (ed), *Brexit and Internal Security Political and Legal Concerns in the Context of the Future UK-EU Relationship* (Palgrave Macmillan 2019)
Sorell T, 'Privacy, bulk collection and "operational utility"' in *National Security Intelligence and Ethics* (1 edn, Routledge 2021)
Wæver O, 'Aberystwyth, Paris, Copenhagen. The Europeanness of new "schools" of security theory in an American field1' in Tickner A and Blaney DL (eds), *Thinking International Relations Differently* (Taylor & Francis Group 2012)
Watts S, 'Cyber Law Development and the United States Law of War Manual' in Osula A-M and Rõigas H (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE 2016)
Vestito F, *Cyber Command Panel* (CyCon 2019)
Carrapico H, Niehuss A and Berthélémy C (eds), *Brexit and Internal Security: Political and Legal Concerns on the Future UK-EU Relationship* (Palgrave MacMillan 2019)

Cassese A, Gaeta P and Jones JRWD (eds), *The Rome statute of the international criminal court: a commentary*, vol 1A (OUP 2002)
Delerue F and Géry A (eds), *International Law and Cybersecurity Governance* (EU Cyber Direct 2022)
Fleck D (ed) *The handbook of international humanitarian law* (2nd edn, OUP 2008)
Georgiev V (ed) *Strategic aspects of the cybersecurity on national and regional level* (Department of National and International Security, New Bulgarian University 2016)
Meyer MA (ed) *Armed conflict and the new law : aspects of 1977 Geneva protocols and the 1981 weapons convention* (London : British Institute of International and Comparative Law 1989)
Schindler D and Toman J (eds), *The laws of armed conflicts. A collection of conventions, resolutions and other documents* (Geneva, Henry Dunant Institute 1973)
Schmitt MN (ed) *Tallinn Manual on the International Law applicable to Cyber Warfare* (CUP 2013)
—— (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2 edn, CUP 2017)
Wolfrum R (ed) *The Max Planck encyclopedia of public international law*, vol VI (OUP 2013)
—— (ed) *The Max Planck encyclopedia of public international law*, vol II (OUP 2013)
—— (ed) *The Max Planck encyclopedia of public international law*, vol X (OUP 2013)
Interior Ministry Act 2014
Thirty-seventh plenary session of the National Assembly of the Republic of Bulgaria (11 February 2015)
1976-1978 DPC, *Data Protection Committee: Evidence and Papers* (The National Archives 1975-1979)
Ahmedov A, *Parliamentary Plenary session* (27 June 2018)
Angelini M, *Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness* (CIS Sapienza 2013)
Banca d'Italia and IVASS, *Cybersecurity: contribution of Banca d'Italia and IVASS (Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass)* (August 2018)
Cabinet Office, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space* (June 2009)
——, *The National Security Strategy of the United Kingdom: Update 2009. Security for the Next Generation* (June 2009)
——, *The National Security Strategy of the United Kingdom. Security in an interdependent world* (March 2008)
Cabinet Office National Security Secretariat, *Cyber Security: Critical National Infrastructure inquiry, Written evidence for the Joint Committee on the National Security Strategy* (17 January 2018)
Colatin SDT, *National Cybersecurity Organisation: ITALY* (NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2020)
Commission E, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (7 February 2013)
Council of Europe's European Committee on Crime Problems, *Computer-related crime* (1990)
Council of Europe, *Convenition on Cybercrime* (2001)
Council of the EU, *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox* (8 June 2023)
——, *Action Plan to Combat Organised Crime (97/C 251/01)* (15 August 1997)
——, *(CFSP) Decision on restrictive measures against cyber-attacks threatening the Union or its Member States* (17 May 2019)
——, *EU Cyber Defence Policy Framework* (18 November 2014)
——, *EU Cyber Defence Policy Framework (2018 update)* (19 November 2018)
——, *Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"* (27 May 2011)
——, *European Security Strategy. A secure Europe in a better world* (2009)

Council of the European Union, *Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.* (5 March 2021)
David Anderson Q.C., *Report of The Bulk Powers Review* (August 2016)
Defence Mo, *White Paper for International Security and Defence* (July 2015)
Department of Defense, *Strategy for Operating in Cyberspace* (July 2011)
——, *Law of War Manual* (June 2015)
Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (November 1999)
Digital/Culture/Media/Sport Df, *Proposal for legislation to improve the UK's cyber resilience* (Updated 30 November 2022)
Doichinov K, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee on Defense 21 June 2018)
ENISA, *Cyber espionage. ENISA Threat Landscape* (From January 2019 to April 2020)
European Defence Agency, *Fact Sheet on Cyber Defence* (10 February 2015)
European Parliament, *Resolution on Estonia (P6_TA(2007)0215)* (24 May 2007)
European Parliament Committee on Foreign Affairs, *Report on Cyber Security and Defence* (17 October 2012)
European Parliament Committee on Industry Research and Energy, *Draft Report on the Proposal for NIS2 Directive* (3 May 2021)
European Parliamentary Research Service, *Understanding the EU's approach to cyber diplomacy and cyber defence* (May 2020)
Foreign Commonwealth & Development Office, *Policy paper on Application of international law to states' conduct in cyberspace: UK statement* (3 June 2021)
Goverment H, *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world* (November 2011)
Hathaway M and others, *ITALY CYBER READINESS AT A GLANCE* (Potomac Institute for Policy Studies November 2016)
HM Government, *National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK* (December 2022)
——, *The future relationship between the United Kingdom and the European Union* (July 2018)
——, *National Cyber Security Strategy 2016 - 2021* (November 2016)
Home Office, *DRAFT Equipment Interference Code of Practice* (February 2017)
——, *Investigatory Powers Act 2016. Consultation: Codes of Practice* (February 2017)
——, *Equipment Interference Code of Practice* (January 2016)
——, *Operational Case for Bulk Powers* (March 2016)
——, *Investigatory Powers Bill Factsheet - Bulk Interception* (October 2015)
House of Commons Committee of Public Accounts, *Cyber-attack on the NHS. Thirty-Second Report of Session 2017–19* (28 March 2018)
Interception of Communications Commissioner's Office (IOCCO), *Report of the Interception of Communications Commissioner. Annual Report for 2016* (2017)
International Commitee of the Red Cross, *Protocol Additional to the Geneva Conventions* (1949)
International Criminal Court, *Rome Statute of the International Criminal Court* (1998)
International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001)
Ivanov IV, *Parliamentary Plenary session* (27 June 2018)
Koev KS, *Increasing Cyber Security and Defense of Communication and Information Structures of the Defense Ministry and the Bulgarian Army* (Military Academy "Georgi Stoykov Rakovski" 2019)

Ministero degli Affari Esteri e della Cooperazione Internazionale, *Italian Position Paper on 'International Law and Cyberspace'* (November 2021)
No.186 TLC, *Criminal Law. Computer Misuse* (1989)
Organisation for Economic Co-operation Development, *Computer-related Crime: Analysis of Legal Policy* (Organisation for Economic Co-operation and Development 1986)
Parliamentary Committee on Defence, *Study on the security and defence of cyberspace* (20 Dicember 2017)
Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers), *Written statement on the information security policies (Relazione sulla politica dell'informazione per la sicurezza)* (2009)
——, *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2011)
——, *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2012)
——, *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2017)
——, *Written statement on the information security policies (Relazione sulla Politica dell'Informazione per la Sicurezza)* (2019)
——, *National Strategic Framework for Cybersecurity (Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico)* (December 2013)
——, *National Strategic Framework for Cyberspace Security* (Presidenza dei Consiglio dei Ministri, Dicembre 2013)
——, *The Italian Cybersecurity Action Plan* (March 2017)
Report of the Study Group co-organised by the University of Bologna University of Milan and University of Westminster, *International Law and Cyberspace* (February 2021)
Republic PCftSot, *Report on cyber threats relevant to the national security, Doc. XXXIV n. 4* (2010)
Temelkov A, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee for the control of the Security Services, the application and use of Special Intelligence Tools and access to Data under the Electronic Communications Act 21 June 2018)
The Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure Contents* (19 November 2018)
The Law Commission, *Working Paper No. 110 on Computer Misuse* (1988)
The Senate of the Parliament of the Czech Republic, *Resolution of the Senate on the Proposal for NIS Directive* (16 May 2013)
The United States Department of Justice, *Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector* (24 March 2016)
United Kingdom Mission to the United Nations, *Statement to the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law to States' Conduct in Cyberspace* (GOV.UK 3 June 2021)
United Nations, *Voting on Resolution A/RES/73/27 on Developments in the field of information and telecommunications in the context of international security* (5 December 2018)
——, *Voting on Resolution A/RES/73/266 on Advancing responsible State behaviour in cyberspace in the context of international security* (22 December 2018)
——, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (A/CONF.144/28/Rev.1 edn, 1990)
United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security* (10 March 2021)

——, *Group of Governmental Experts on Advancing Responsible*

State Behaviour in Cyberspace in the Context of International Security (14 July 2021)
——, *Declaration on Principles of International Law Concerning Friendly Relations And Co-Operation Among States in Accordance with The Charter Of The United Nations (GAR 2625)* (1970)
——, *Developments in the field of information and telecommunications in the context of international security* (2013)
——, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015)
'Cybersecurity – the Heart of the EU Security. Interview with Despina Spanou' 7:1 European Cybersecurity Journal
Aggestam L and Johansson M, 'The Leadership Paradox in EU Foreign Policy' (2017) 55:6 JCMS 1203
Barrinha A and Renard T, 'Cyber-diplomacy: the making of an international society in the digital age' (2017) 3:4-5 Global Affairs 353
Bendiek A, 'The European Union's Foreign Policy Toolbox in International Cyber Diplomacy' (December 2018) 2:3 Cyber, Intelligence, and Security 57
——, 'A Paradigm Shift in the EU's Common Foreign and Security Policy: From Trans-formation to Resilience' (October 2017) SWP Research Paper
Bendiek A, Bossong R and Schulze M, 'The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges' (2017, November) Stiftung Wissenschaft und Politik (SWP) - German Institute for International and Security Affairs
Bendiek A and Kettemann MC, 'Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy' (February 2021) SWP 1
Bendiek A and Schulze M, 'Attribution: A Major Challenge for EU Cyber Sanctions An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW' SWP Research Paper 11
Boeke S, 'National cyber crisis management: Different European approaches' (2017) 31 Governance 449
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
Bruno B, 'Cybersecurity between legislation, national interests and the market (Cybersecurity tra legislazioni, interessi nazionali e mercato)' (2020) 14 Federalismiit 10
Carrapico H and Barrinha A, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55:6 JCMS 1254
——, 'European Union cyber security as an emerging research and policy field' (2018) 19:3 European Politics & Society 299
Carrapico H and Farrand B, 'Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy' (2020) 42:8 Journal of European Integration 1111
——, ''Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers' 67 Crime, Law and Social Change 245
Chakarov CAPI, 'Directions on cyber protection in management systems (Направления за киберзащита в системите за управление)' Nacionalna Sigurnost (Национална сигурност)
Chitarro A and Setola R, 'Nuova Direttiva per la protezione cibernetica e la sicurezza informatica (New Directive on cybersecurity and information security)' II Sicurezza e Giustizia
Christou G, 'The collective securitisation of cyberspace in the European Union' (2019) 42:2 West European Politics 278
——, 'The challenges of cybercrime governance in the European Union' [Routledge] 19 European Politics and Society 355

Corn GP and Taylor R, ‘Concluding Observations on Sovereignty in Cyberspace. Sovereignty in the age of cyber’ (2017) 111 AJIL Unbound 282
Crootof R, ‘International cybertorts: Expanding state accountability in cyberspace’ (2018) 103 Cornell law review 565
Cross MaKD, ‘An EU Homeland Security? Sovereignty vs. Supranational Order’ (2007) 16:1 79
Delerue F, ‘Reinterpretation or Contestation of International Law in Cyberspace?’ (2019) 52 Israel law review 295
——, ‘Toward an EU position on the application of international law in cyberspace’ (2023) EU Cyber Direct
Eichensehr KE, ‘The Law and Politics of Cyberattack Attribution’ (2020) 67 UCLA Law Review 520
Fafinski S, ‘Access Denied: Computer Misuse in an Era of Technological Change’ (2006) 70:5 The Journal of Criminal Law 424
——, ‘The UK legislative position on cybercrime: a 20-year retrospective’ (2009) 13:4 Journal of Internet Law 3
Floyd R, ‘Collective securitisation in the EU: normative dimensions’ (2019) 42:2 West European Politics 391
Girginov A, ‘Extraterritorial effect of the Penal Code - problems with the legal system (Извънтериториално действие на Наказателния Кодекс - проблеми на правната уредба)’ 8 Bar Review (Адвокатски преглед) 10
Gordon S and Ford R, ‘On the definition and classification of cybercrime’ (2006) 2 Journal in Computer Virology 13
Greca FTL, ‘The regulatory approach to cybercrime (L'approccio normativo alla criminalità informatica)’ [2003] ADIR, L'altro diritto
Grotto M, ‘Council of Europe Convention on cyber crime and its ratification in the Italian legal system’ (2010) 2 Sistema Penal & Violência 1
Guitton C, ‘Cyber insecurity as a national threat: overreaction from Germany, France and the UK?’ (2013) 22:1 European Security 21
Hill C, ‘The Capability-Expectations Gap, or Conceptualizing Europe's International Role’ (1993) 31:3 JCMS 305
Jensen ET and Watts S, ‘A cyber duty of due diligence: Gentle civilizer or crude destabilizer?’ (2017) 95 Texas Law Review 1555
Johnson DE and Schmitt MN, ‘Responding to Proxy Cyber Operations Under International Law’ (2021) 6:4 The Cyber Defense Review 15
Kelemen M and Smith W, ‘Community and its 'virtual' promises: a critique of cyberlibertarian rhetoric’ (2001) 4 Information, Communication & Society 370
Kilovaty I, ‘World Wide Web of Exploitations – the Case of Peacetime Cyber Espionage Operations Under International Law:: Towards a Contextual Approach’ (2017) 18 Science and Technology Law Review
Konstantopoulos IL and Nomikos JM, ‘Brexit and intelligence: connecting the dots’ 16 Journal of Intelligence History 100
Kulikova A, ‘Cyber norms: technical extensions and technological challenges’ (2021) 6 Journal of Cyber Policy 340
Laura K D, ‘Criminal Law: Anglo-American Privacy And Surveillance’ 96 Journal of Criminal Law and Criminology 1059
Lewis JA, ‘Cyber War and Ukraine’ [2022] Center for Strategic and International Studies (CSIS)
Li X, ‘Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime ’ 9 International Journal of Cyber Criminology 185
Lotrionte C, ‘Countering state-sponsored cyber economic espionage under international law’ (2015) 40 North Carolina Journal of International Law and Commercial Regulation 443

——, ‘Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law’ (2018) 3 The Cyber Defense Review 73
Lucarelli S, ‘The EU as a securitising agent? Testing the model, advancing the literature’ (2019) 42:2 West European Politics 413
Mačák K, ‘Unblurring the lines: military cyber operations and international law’ (2021) 6 Journal of Cyber Policy 411
Macewan N, ‘The Computer Misuse Act 1990: lessons from its past and predictions for its future’ (December 2008) Criminal Law Review 955
Markopoulou D, Papakonstantinou V and Hert Pd, ‘The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation’ (2019) 35 Computer Law & Security Review 105336
Maschmeyer L, ‘The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations’ (2021) 46 International Security 51
McGraw G, ‘Cyber War is Inevitable (Unless We Build Security In)’ (2013) 36 Journal of Strategic Studies 109
Milanovic M and Schmitt MN, ‘Cyber Attacks and Cyber (Mis)information Operations during a Pandemic’ (2020) 11 Journal of National Security Law & Policy
Neville-Jones P and Phillips M, ‘Where Next for UK Cyber-Security?’ (December 2012) 157 RUSI JOURNAL 32
Osawa J, ‘The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?’ (2017) 24 Asia-Pacific Review 113
Petkov P, ‘Cybersecurity: Emerging Characteristics and Impact on Defence’ IT4SecReports 98 ICT Institute, Bulgarian Academy of Science
Polimirova D and others, ‘Cybersecurity and Opportunities for Application of Innovative Technologies in the Public Administration in Bulgaria’ National Lab for Computer Virology, Bulgarian Academy of Sciences
Rid T, ‘Cyber War Will Not Take Place’ (2012) 35 JStrategic Stud 5
Romano BN, ‘Il rischio di “attacchi” ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di “buona amministrazione” (The risk of "attacks" on computer systems between relevant cases, data protection and requirements for "good administration")’ (2021) 3 Rivista di Ateneo dell’Università degli Studi di Roma “Foro Italico” 545
Roscini M, ‘Cyber Operations as Nuclear Counterproliferation Measures’ (2014) 19 Journal of Conflict and Security Law 133
Rossa S, ‘Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy’ (2022) 14 Italian Journal of Public Law 426
Sallavaci O, ‘Combating Cyber Dependent Crimes: The Legal Framework in the UK’ (2017) Communications in Computer and Information Science 53
Scaccia G, ‘Intelligence and state secrecy in law no. 133 of 2012 (Intelligence e segreto di Stato nella legge n. 133 del 2012)’ Editoriale Scientifica
Schafer B, ‘Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill’ (Wiesbaden) 40 Datenschutz und Datensicherheit - DuD 592
Schmitt MN, ‘"Below the threshold" cyber operations: the countermeasures response option and international law’ (2014) 54 Virginia Journal of International Law 697
——, ‘Grey Zones in the International Law of Cyberspace’ (2017) 42 The Yale Journal of International Law Online 1
Schmitt MN, ‘The Law of Cyber Warfare: *Quo Vadis?*’ (2014) 25 StanL& Pol'y Rev 269
Schmitt MN and Vihul L, ‘Respect for Sovereignty in Cyberspace’ (2017) 95 Texas Law Review 1639

Schmitz-Berndt S and Chiara PG, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) 3 International Cybersecurity Law Review 289
Scott PF, 'General warrants, thematic warrants, bulk warrants: property interference for national security purposes' 68:2 (2017) Northern Ireland Legal Quarterly 99
Setola R, 'Istituito il 'Nucleo per la Sicurezza Cibernetica' (Establishment of the Cybersecuirty Unit)' II Sicurezza e Giustizia
——, 'Il Quadro Strategico Nazionale per la Cybersecurity (The National Strategic Framework for Cybersecurity)' I Sicurezza e Giustizia 26
Setola R and Assenza G, 'Ricepimento della Direttiva NIS sulla cyber-security delle reti (Transposition of the NIS Directive)' IV Sicurezza e Giustizia
Sliwinski KF, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35:3 Contemporary Security Policy 468
Spataro A, 'Security policies and fundamental rights (Politiche della sicurezza e diritti fondamentali)' Speciale Questine Giustizia: Terrorismo internazionale Politiche della sicurezza Diritti fondamentali
Sperling J and Webber M, 'The European Union: security governance and collective securitisation' (2019) 42:2 West European Politics 228
——, 'NATO and the Ukraine crisis: Collective securitization' (2017) 2:1 European Journal of International Security 19
Stevens T and O'Brien K, 'Brexit and Cyber Security' 164 The RUSI Journal 22
Stoichkov O, 'Special Intelligence and Cyber security (Специални разузнавателни средства и киберсигурност)' Security & Defense (Сигурност и отбрана) 137
Sweeney S and Winn N, 'Do or die? The UK, the EU, and internal/external security

cooperation after Brexit' European Political Science 237
Walden I and Michels J, 'Going it alone? UK cybersecurity regulation post-Brexit' 2 International Cybersecurity Law Review 1
Wall DS, 'Policing Cybercrime in the EU: Shall I Stay Or Shall I Go?' [2016] 78 British Society of Criminology Newsletter 1
Woods L, 'United Kingdom: Draft Investigatory Powers Bill' 2:1 (2016) European Data Protection Law Review 103
'The Commission for Personal Data Protection explained why the NAP was fined 5.1 million leva (Комисията за защита на лични данни обясни защо глобява НАП с 5.1 млн. лева)' *Dirbg 29 August 2019* <https://dnes.dir.bg/obshtestvo/komisiyata-za-zashtita-na-lichni-danni-obyasni-zashto-globyava-nap-s-5-1-mln-leva> accessed 3 July 2021
'The snoopers' charter of warrants and watchers' *The Economist* (23 January 2016)
Clarke V, 'Brexit 'will not impact' UK-EU co-operation on cybersecurity' *The Irish Times* <https://www.irishtimes.com/business/technology/brexit-will-not-impact-uk-eu-co-operation-on-cybersecurity-1.3682697> accessed 31 July 2022
Ivanova I, 'Bulgarian hackers should work for NATO, said Plevneliev (Родните хакери да заработят за НАТО, поиска Плевнелиев)' *Newsbg 2 April 2012* (2 April 2012) <https://news.bg/politics/rodnite-hakeri-da-zarabotyat-za-nato-poiska-plevneliev.html> accessed 7 July 2021
Mensurati M and Tonacci F, 'Russian hackers in the servers of Italian Ministry of Defence (trs)' *La Repubblica* (17 February 2016) <www.repubblica.it/cronaca/2016/02/17/news/hacker_russi_ministero_difesa_italiano-155988416/> accessed 21 January 2017
Sabbagh D, 'Britain has offensive cyberwar capability, top general admits' *The Guardian 25 September 2020* <https://www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits> accessed 3 July 2021

Shapiro SJ, 'On the trail of the Dark Avenger: the most dangerous virus writer in the world' *The Guardian* (9 May 2023) <https://www.theguardian.com/news/2023/may/09/on-the-trail-of-the-dark-avenger-the-most-dangerous-virus-writer-in-the-world> accessed 30 August 2023
Council of the EU, *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union* (10 May 2022)
——, *Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation* (15 April 2021)
——, *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack* (22 October 2020)
——, *EU imposes the first ever sanctions against cyber-attacks* (30 July 2020)
Delegation of the European Union to the United Nations in New York, *EU Statement – UN Open-Ended Working Group on ICT: International Law* (8 March 2023)
——, *EU Statement – UN Open-Ended Working Group on ICT: International Law* (24 May 2023)
Donchev T, *Parliamentary debate on the First reading Report on the Bulgarian Cybersecurity Bill* (Committee on Homeland Security and Public Order 6 June 2018)
Plevneliev R, *Lecture of President Rosen Plevneliev at the Atlantic Club in Bulgaria on "Current problems and priorities in the national security system of the Republic of Bulgaria" (Лекция на президента Росен Плевнелиев пред Атлантическия клуб в България на тема "Актуални проблеми и приоритети в системата за национална сигурност на Република България")* (Official website of the President 22 November 2012)
The White House Office of the Press Secretary, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment* (29 December 2016)
United Nations, *Pay More Attention To Cyberwarfare, Verification, Secretary-General Advises In Remarks To Advisory Board On Disarmament Affairs* (18 February 2009)
Baldoni R and Nicola RD, *White paper on the Future of Cybersecurity in Italy (Il Futuro della Cyber Security in Italia)* (October 2015)
Baldoni R, Nicola RD and Prinetto P, *The Future of Cybersecurity in Italy: Strategic Project Areas (Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici)* (Laboratorio Nazionale di Cybersecurity; CINI - Consorzio Interuniversitario Nazionale per l'Informatica, January 2018)
Dublin European Council, *Presidency Conclusions* (13-14 December 1996)
European Commission, *Staff Working Document; Impact Assessment on the NIS2 Directive {COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final} Part 1/3* (16 December 2020)
——, *A Digital Agenda for Europe* (19 May 2010)
——, *Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673 final)* (22 November 2010)
——, *Report on assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems* (28 October 2019)
——, *Proposal for a Council Decision in the Field of Information Security* (1990)
——, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century: White Paper* (1993)
——, *Staff Working Document; Impact Assessment on the NIS Directive {COM(2013) 48 final} {SWD(2013) 32 final}* (February 2013)
——, *Communication on Network and Information Security: Proposal for A European Policy Approach COM(2001)298 final* (June 2001)
——, *Communication on A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" {SEC(2006) 656}* (May 2006)

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (7 February 2013)
——, *The EU's Cybersecurity Strategy for the Digital Decade* (16 December 2020)
European Parliament, *Report on the 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* (4 November 2021)
——, *Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (12 September 2013)
European Parliament Directorate General for Internal Policies, *Cybersecurity in the European Union and Beyond Exploring the Threats and Policy Responses* (2015)
House of Deputies, *Parliamentary debate Sitting n. 734 1 February 2017*
——, *National cybersecurity, experts hearing (Sicurezza nazionale cibernetica, audizione di esperti)* (16 Ottobre 2019)
——, *Joint hearing of the Constitutional Affairs and Defence Committees, 7 March 2017* (XVII Legislature)
——, *Joint hearing of the Constitutional Affairs and Defence Committees, 14 June 2017* (XVII Legislature)
——, *Bulletin of the parliamentary committees, Special Committee for the Examination of Government Acts* (XVIII Legislature, 8 May 2018)
——, *Bulletin of the parliamentary committees, Special Committee for the Examination of Government Acts* (XVIII Legislature, 18 April 2018)
NCCIC and FBI, *Grizzly Steppe - Russian Malicious Cyber Activity* (29 December 2016)
Secretary of State for Digital Culture Media and Sport, *Post-Implementation Review of the Network and Information Systems Regulations 2018* (May 2020)
Senato della Repubblica (Senate) and Camera dei Deputati (House of Deputies), *Schema di decreto legislativo recante attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, Atto del Governo n.10 (Outline of Legislative decree 65/2018 transposing the NIS Directive)*
UK Parliament Public Bill Committee, *Investigatory Powers Bill. Written evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc and Yahoo Inc (IPB 21)* (Session 2015-16)
18 U.S. Code § 1030 - Fraud and related activity in connection with computers
Act of Parliament 109/2021
Act of Parliament 124/2007
Act of Parliament 155/2005
Bulgarian Cybersecurity Act 2018
Bulgarian Cybersecurity Strategy "Cyber resilient Bulgaria 2020" 2016
Bulgarian Cybersecurity Strategy "Cyber resilient Bulgaria 2023" 2021
Bulgarian Penal Code 1991
Canadian Criminal Code 1985
The Data Protection Act 1984
Decree law 105/2019
Decree law 174/2015
Directive 2018/1972 establishing the European Electronic Communications Code (Recast)
Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive 2016)
Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)
Directive on a common regulatory framework for electronic communications networks and services (2002) (Framework Directive)
DM Interior Ministry 9 January 2008

DPCM 8 August 2019
DPCM 14 April 2021 Incident notification
DPCM 14 June 2021 Cybersecurity Agency
DPCM 16 January 2002
DPCM 30 July 2020 Entities
DPCM (PM Decree) 17 February 2017
DPCM (PM Decree) 24 January 2013
E-Government Act 2008
Electronic Communications Act 2007
European Communities Act 1972
European Union (Withdrawal) Act 2018
General Data Protection Regulation 2016
German Criminal Code 1998
HC Deb 03 March 1977, vol 927, col 589
HC Deb 12 April 2016, vol 608, col 129
HC Deb 15 March 2016, vol 607, col 890
HC Deb 21 April 2016, vol 608, col 441
HC Deb 23 February 2017, vol 621, col 38WS
HC Deb, 19 May 2021, cW
HL Deb 04 June 1991 vol 529 col 535
Intelligence Services Act 1994
Interinstitutional Agreement on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) (January 2018)
Investigatory Powers Act 2016
Italian Penal Code
Legislative decree 65/2018
Legislative decree 259/2003
National Security Strategy 2018
The NIS (Amendment etc.) (EU Exit) Regulations 2019
NIS Regulations 2018
Ordinance on Network and Information Security 2019
Ordinance on the way, order and competent authorities for identifying critical infrastructure sectors and assessing the risk applicable to them 2012
Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union (NIS Directive Proposal) 2013
Proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents 2023 (EU Cyber Solidatity Act)
Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)
Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (2019) (Cybersecurity Act)
Regulation of Investigatory Powers Act 2000
Rules regulating the organisation and activity of the Cybersecurity Council 2019
Russian Criminal Code 1996
State Agency for National Security Act 2008
The Telecoms Act 1984

Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (April 2021)
Treaty on the European Union
Treaty on the Functioning of the EU
UK Computer Misuse Act 1990
UK Terrorism Act 2000
UN Charter 1945
Serious Crime Act
Political declaration setting out the framework for the future relationship between the EU and the UK (November 2019)
Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities 2017 ("Cyber Diplomacy Toolbox")
'CERT Pubblica Amministrazione' <https://www.cert-pa.it/> accessed 12 August 2020
'The cybersecurity perimeter: Italy's cyber defense (Perimetro di sicurezza cibernetica: la cyber difesa dell'Italia)' (*Cyber Trends*) <https://www.cybertrends.it/perimetro-di-sicurezza-cibernetica-la-cyber-difesa-dellitalia/> accessed 19 November 2023
'National Protective Security Authority Official Website' <https://www.npsa.gov.uk/about-npsa> accessed 15 January 2024
'Official National Security Secretariat website' <https://www.gov.uk/government/organisations/national-security/about> accessed 21 December 2023
'Official NCF website' <https://www.gov.uk/government/organisations/national-cyber-force> accessed 21 December 2023
'Snowden Revelations' (*Lawfare*) <www.lawfareblog.com/snowden-revelations> accessed 10 March 2017
'Warnings over growing IS cyber-threat' (*BBC News*, 3 June 2015) <www.bbc.co.uk/news/technology-32982609> accessed 21 January 2017
'The court returned the terrorism case for the NAP data breach to the prosecutor's office (Съдът върна на прокуратурата делото за тероризъм покрай теча на данни от НАП)' (*Lex News*, 5 April 2023) <https://news.lex.bg/%D1%81%D1%8A%D0%B4%D1%8A%D1%82-%D0%B2%D1%8A%D1%80%D0%BD%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D0%BA%D1%83%D1%80%D0%B0%D1%82%D1%83%D1%80%D0%B0%D1%82%D0%B0-%D0%B4%D0%B5%D0%BB%D0%BE%D1%82%D0%BE-%D0%B7/>
'Russia 'was behind German parliament hack'' (*BBC News*, 13 May 2016) <www.bbc.co.uk/news/technology-36284447> accessed 21 January 2017
'Massive ransomware infection hits computers in 99 countries' (*BBC News*, 13 May 2017) <https://www.bbc.com/news/technology-39901382> accessed 21 December 2023
'Coronavirus: Cyber-attacks hit hospital construction companies' (*BBC News*, 13 May 2020) <https://www.bbc.com/news/technology-52646808> accessed 15 January 2024
'NHS was repeatedly warned of cyber-attack, says Fallon' (*BBC News*, 14 May 2017) <https://www.bbc.com/news/uk-39912825> accessed 21 December 2023
'Tomislav Donchev: A cyberattack from the inside shakes the government, from the outside - shakes the state (Томислав Дончев: Кибератака отвътре клати правителството, отвън - клати държавата)' (*Novini.bg*, 20 July 2019) <https://novini.bg/bylgariya/politika/548365> accessed 12 September 2023
'Cybersecurity: Italy's steps ahead (Cybersecurity: ecco i passi avanti dell'Italia)' (*Sicurezza Nazionale*, 21 December 2018) <https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-ecco-i-passi-avanti-dell-italia.html> accessed 18 November 2023

‘The hacking of the solarwinds platform: the Cyber Security Unit is summoned (Hackeraggio della piattaforma solarwinds: riunito il Nucleo per la Sicurezza Cibernetica)’ (*Italian CSIRT*, 24 December 2020) <https://www.csirt.gov.it/contenuti/hackeraggio-della-piattaforma-solarwinds-riunito-il-nucleo-per-la-sicurezza-cibernetica-ne01-201224-csirt-ita> accessed 18 Novembre 2023
‘U.S. homeland chief: cyber 9/11 could happen "imminently"’ (*Reuters*, 24 January 2013) <https://www.reuters.com/article/idUSBRE90N1A4/> accessed 29 December 2023
‘Microsoft Digital Defense Report ’ (October 2021) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738> accessed 22 December 2023
Ackerman S and Thielman S, ‘US officially accuses Russia of hacking DNC and interfering with election’ (*The Guardian*, 8 October 2016) <https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election> accessed 21 January 2024
Advisory Board Portal of the Council of Ministers, ‘Cybersecurity Council’ <http://saveti.government.bg/web/cc_1901/1>
Agency NC, ‘Nunzia Ciardi: The digital revolution has enormous potential. But be careful about privacy: the internet does not forget (Nunzia Ciardi: La Rivoluzione digitale ha potenzialità enormi. Ma attenti alla privacy: la rete non dimentica)’ (24 Maggio 2023) <https://www.acn.gov.it/notizie/contenuti/nunzia-ciardi-la-rivoluzione-digitale-ha-potenzialita-enormi-ma-attenti-alla-privacy-la-rete-non-dimentica> accessed 25 Novemner 2023
al SMe, ‘Cybersecurity: the role of engineers and the possible synergies between Government, Industry and University (Cyber Security: il ruolo degli Ingegneri e le possibili sinergie tra Governo, Industria e Università)’ (*Radio Radicale*, 6 December 2019) <https://www.radioradicale.it/scheda/592274/cyber-security-il-ruolo-degli-ingegneri-e-le-possibili-sinergie-tra-governo-industria> accessed 28 November 2023
Albanian Government, ‘Videomessage of Prime Minister Edi Rama’ (7 September 2022) <https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/> accessed 15 January 2024
Alperovitch D and Ward I, ‘How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks? ’ (*Lawfare*, 12 March 2021) <https://www.lawfaremedia.org/article/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks> accessed 24 January 2024
ANSA R, ‘The Occhionero siblinges, between masonry and finance (I fratelli Occhionero, tra massoneria e alta finanza)’ (*ANSA*, 12 December 2017) <https://www.ansa.it/sito/notizie/cronaca/2017/01/10/chi-i-sono-i-fratelli-occhionero-gli-spioni-tra-massoneria-e-alta-finanza_d4a65eeb-3cd1-4b59-a223-92555cc77728.html> accessed 28 November 2023
Arimatsu L and O’Connell ME, ‘Cyber Security and International Law’ (*Chatham House*, 2012) <www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf> accessed 26 November 2016
Arkhipov I and Andrianova A, ‘Putin Vents at U.S. for ‘Hysteria’ Over Hacking Blamed on Russia’ (*Bloomberg*, 12 October 2016) <www.bloomberg.com/news/articles/2016-10-12/russia-denies-u-s-allegations-of-hacking-attacks-on-elections> accessed 20 January 2024
Ashford W, ‘UK committed to working with EU cyber security partners’ (21 February 2019) <https://www.computerweekly.com/news/252458102/UK-committed-to-working-with-EU-cyber-security-partners> accessed 15 January 2024
Assessment UIC, ‘Assessing Russian Activities and Intentions in Recent US Elections’ (6 January 2017) <https://s3.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf> accessed 24 January 2024
Barlow JP, ‘A Declaration of the Independence of Cyberspace’ <http://editions-hache.com/essais/pdf/barlow1.pdf> accessed 15 January 2024

Boccellato P, 'Interview with Prof. Annita Sciacovelli: Italy needs a public and private cyber intelligence strategy based on the Israeli model' (19 July 2021) <https://www.cybersecitalia.it/cybersecurity-annita-sciacovelli-in-italia-serve-una-strategia-di-cyber-intelligence-pubblica-e-privata-basata-sul-modello-israeliano/12835/> accessed 25 November 2023
Carrer G, 'Crisis in the Middle East at the center of the Cybersecurity Unit meeting (Crisi in Medio Oriente al centro della riunione del Nucleo per la cybersicurezza)' (*Formiche.net*, 21 Ottobre 2023) <https://formiche.net/2023/10/nucleo-per-la-cybersicurezza-medio-oriente/> accessed 18 November 2023
Chatterjee BB, 'International law and cyber warfare: an agenda for future research' (*Lancaster: Lancaster University*, 2014) <www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/security-lancaster/tallinn_report_final[1].pdf> accessed 6 December 2016
Chesney R, 'Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?' (15 April 2021) <https://www.lawfaremedia.org/article/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross> accessed 25 January 2024
Cimpanu C, 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak' (*ZDNET*, 13 March 2020) <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> accessed 15 January 2024
Clasen A, 'EU countries' reservations persist on Cyber Solidarity Act' (*EURACTIV*, 24 November 2023) <https://www.euractiv.com/section/cybersecurity/news/eu-countries-reservations-persist-on-cyber-solidarity-act/> accessed 15 January 2023
Corera G, 'How and why MI5 kept phone data spy programme secret' (*BBC News*, 5 November 2015) <https://www.bbc.com/news/uk-politics-34731735> accessed 21 December 2023
Council of the EU, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic' (30 April 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/> accessed 15 January 2023
——, 'Infographic - Top cyber threats in the EU' (2022) <https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/> accessed 15 January 2023
Cybersecurity & Infrastructure Security Agency, 'HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm' (31 May 2018) <https://www.cisa.gov/news-events/alerts/2018/05/29/hidden-cobra-joanap-backdoor-trojan-and-brambul-server-message-block> accessed 24 January 2024
Cyen, 'Speech by Marina Kaljurand on Sanctions in cyberspace: the EU and the US diplomatic approaches' (27 May 2021) <https://www.youtube.com/watch?v=Ti7AjuUNCfE> accessed 15 January 2023
Defence UMo, 'New cyber reserve unit created' (*GOV.UK*, 29 September 2013) <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit> accessed 31 January 2024
Defense Mo, 'The role of engineers for cybersecurity - Speech by General Leverano, then Defence Deputy Chief of Staff' (6 December 2019) <http://www.difesa.it/SMD_/Staff/Sottocapo/Messaggi/Pagine/cyber_security_convegno_Napoli.aspx> accessed 28 November 2023
Department for Digital C and Sport M, 'Telecoms security: proposal for new regulations and code of practice' (August 2022) <https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice> accessed 20 December 2023
European Commission, 'State-of-play of the transposition of the NIS Directive' (7 June 2022) <https://digital-strategy.ec.europa.eu/en/policies/nis-transposition> accessed 28 November 2023

——, ‘Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme’ (27 Novembre 2019) <https://ec.europa.eu/commission/presscorner/detail/it/speech_19_6408> accessed 15 January 2024
European Parliament, ‘Speech by Nicola Danti on High common level of security of network and information systems across the Union (debate)’ (5 July 2016) <https://www.europarl.europa.eu/doceo/document/CRE-8-2016-07-05-ITM-013_EN.html> accessed 15 January 2024
——, ‘Speeches by Mylène Troszczynski and Eva Paunova on High common level of security of network and information systems across the Union (debate)’ (5 July 2016) <https://www.europarl.europa.eu/doceo/document/CRE-8-2016-07-05-ITM-013_EN.html> accessed 6 January 2024
——, ‘Speech by Ivailo Kalfin on High common level of network and information security (debate)’ (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-INT-3-904-000_EN.html?redirect> accessed 15 January 2024
——, ‘Speech by Neelie Kroes on High common level of network and information security (debate)’ (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 15 January 2024
——, ‘Speech by Vicky Ford on High common level of network and information security (debate)’ (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 6 January 2024
——, ‘Speeches by Vicky Ford and Malcolm Harbour on High common level of network and information security (debate)’ (12 March 2014) <https://www.europarl.europa.eu/doceo/document/CRE-7-2014-03-12-ITM-015_EN.html> accessed 6 January 2024
——, ‘Speech by Peter Kouroumbashev on cybersecurity - debates in ITRE Committee’ (22 March 2018) <https://www.youtube.com/watch?v=3265VcpSI14&t=3s> accessed 15 January 2024
European Parliament Legislative Observatory, ‘High common level of network and information security across the Union. NIS Directive 2013/0027(COD) (Summary of debate in Council)’ (*Legislative Observatory*, 5 December 2013) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1327607&t=e&l=en> accessed 28 December 2023
——, ‘High common level of network and information security across the Union. NIS Directive 2013/0027(COD) (Summary of debate in Council)’ (6 June 2013) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1274749&t=e&l=en> accessed 28 December 2023
Foreign & Commonwealth Office, ‘Foreign Office Minister condemns North Korean actor for WannaCry attacks’ (19 December 2017) <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks> accessed 24 January 2024
Foreign Commonwealth and Development Office, ‘UK exposes Russian spy agency behind cyber incidents’ (24 March 2022) <https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents> accessed 22 December 2023
——, ‘Russia's FSB malign activity: factsheet’ (*GOV.UK*, Updated: 7 December 2023) <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet> accessed 22 December 2023
Foschini G, ‘Russian hackers, blitz against the Air Force in search of F-35's secrets (trs)’ (*La Repubblica*, 14 January 2017) <www.repubblica.it/cronaca/2017/01/14/news/hacker_russi_aeronautica-155988414/> accessed 15 January 2024

Fouquet H, 'Paris Hospitals Target of Failed Cyber-Attack, Authority Says' (*Bloomberg*, 23 March 2020) <https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says> accessed 15 January 2024
Fox C and Kelion L, 'Coronavirus: Russian spies target Covid-19 vaccine research' (16 July 2020) <https://www.bbc.com/news/technology-53429506> accessed 24 January 2024
GCHQ, 'National Cyber Force transforms country's cyber capabilities to protect the UK' (19 November 2020) <https://www.gchq.gov.uk/news/national-cyber-force> accessed 31 January 2024
Goodman R, 'International Law and the US Response to Russian Election Interference' (5 January 2017) <https://www.justsecurity.org/35999/international-law-response-russian-election-interference/> accessed 24 January 2024
Hollinger P, 'Cyber attackers target G20 documents' (*Financial Times*, 7 March 2011) <www.ft.com/content/83dc8ce4-48f4-11e0-af8c-00144feab49a> accessed 21 January 2017
INTCEN) EIACE, 'Fact Sheet' (19 April 2012) <https://www.asktheeu.org/en/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf> accessed 30 January 2024
International Committee of the Red Cross, 'Norms for responsible State behavior on cyber operations should build on international law' (11 February 2020) <https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law> accessed 15 January 2024
Jones T, 'William Gibson: beyond cyberspace' (*The Guardian*, 22 September 2011) <www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace> accessed 15 January 2024
Kabelka L, 'EU's cyber incident reporting mechanism does not work, agency chief warns' (*EURACTIV*, 27 April 2022) <https://www.euractiv.com/section/cybersecurity/news/eus-cyber-incident-reporting-mechanism-does-not-work-agency-chief-warns/> accessed 28 December 2023
Kaspersky, 'Cyber threat real-time map' <https://cybermap.kaspersky.com/> accessed 15 January 2024
Kilovaty I, 'The Democratic National Committee Hack: Information as Interference' (*Just Security*, 1 August 2016) <www.justsecurity.org/32206/democratic-national-committee-hack-information-interference/> accessed 5 December 2023
Landler M and Markoff J, 'Digital Fears Emerge After Data Siege in Estonia' (*The New York Times*, 29 May 2007) <www.nytimes.com/2007/05/29/technology/29estonia.html> accessed 15 January 2024
Mačák K, Gisel L and Rodenhäuser T, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?' (*Just Security*, 27 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 24 January 2023
MacAskill E, 'MI5 chief: UK and EU intelligence sharing 'never more important'' (*The Guardian*, 13 May 2018) <https://www.theguardian.com/uk-news/2018/may/13/uk-and-european-intelligence-more-vital-than-ever-warns-m15-head> accessed 24 December 2023
Mele S, 'National Cybersecurity perimeter: Prime Ministerial Decree 131/2020 is taking shape (Perimetro di Sicurezza Nazionale Cibernetica: ecco come prende forma con il DPCM 131/2020)' (*Altalex*, 3 November 2020) <https://www.altalex.com/documents/2020/11/03/perimetro-di-sicurezza-nazionale-cibernetica-ecco-come-prende-forma-con-il-dpcm-131-2020> accessed 19 November 2023
Mr Hahn (on behalf of the European Commission), 'European Parliament Questions to the European Commission: SolarWinds hack' (13 April 2021) <https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.pdf> accessed 24 January 2024
Müller M and Harnisch S, 'With a little help from my friends? Cyber assistance and Ukraine's successful cyber defence' (*European Repository of Cyber Incidents*, February 2023) <https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Opinion_piece_Feb_2023_A_little_help_ab5769f036.pdf?updated_at=2023-02-27T12:13:16.994Z> accessed 10 April 2023

National CSIRT, <https://www.govcert.bg/en/%d0%ba%d0%be%d0%bd%d1%82%d0%b0%d0%ba%d1%82%d0%b8/> accessed 16 August 2023
National Cyber Security Centre, 'Official website' <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>
——, 'Reckless campaign of cyber attacks by Russian military intelligence service exposed' (3 October 2018) <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> accessed 22 December 2023
——, 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' (14 February 2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 24 January 2024
——, 'Russian state-sponsored cyber actors targeting network infrastructure devices' (15 April 2018) <https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices> accessed 22 December 2023
——, 'UK and US call out Russia for SolarWinds compromise' (15 April 2021) <https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise> accessed 22 December 2023
——, 'Advisory: APT29 targets COVID-19 vaccine development' (16 July 2020) <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> accessed 24 January 2024
——, 'UK supports US charges against North Korean cyber actors' (17 February 2021) <https://www.ncsc.gov.uk/news/uk-supports-us-charges-against-north-korean-cyber-actors> accessed 22 December 2023
NATO CCD COE, 'National Positions' <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions> accessed 15 January 2024
Office of Public Affairs U.S. Department of Justice, 'Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers' (30 January 2019) <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north> accessed 24 January 2024
Patrikakis C, Masikos M and Zouraraki O, 'Distributed Denial of Service Attacks' (December 2004) <https://web.archive.org/web/20190826143507/https:/www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html> accessed 20 December 2023
Peeva V, 'Cyber(in)security for millions (Кибер(не)сигурност за милиони)' (1 August 2019) <https://www.mediapool.bg/kibernesigurnost-za-milioni-news296397.html> accessed 3 January 2024
Perlroth N, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back' (*The New York Times*, 23 October 2012) <www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html> accessed 21 January 2024
Peters A, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I' (*EJIL:Talk!*, 1 November 2013) <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/> accessed 6 December 2016
Polityuk P, 'Ukraine investigates suspected cyber attack on Kiev power grid' (*Reuters*, 20 December 2016) <www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF> accessed 15 January 2024
——, 'Ukraine to probe suspected Russian cyber attack on grid' (*Reuters*, 31 December 2015) <www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231> accessed 15 January 2024
QED, 'Speech by Jakub Boratynski at the 5th Annual QED Conference on Cybersecurity' (22 June 2017) <https://www.youtube.com/watch?v=Ayc8Jef_Rds> accessed 15 January 2024

Republic REitC, ‘Embassy Comment on the accusation that Russia has performed cyberattacks on the territory of the Czech Republic’ (20 April 2020) <https://www.facebook.com/AmbRusCz/posts/2440514632835902> accessed 22 January 2023
Rocchi W, ‘Cybersecurity in the healthcare sector, medical equipment and confidential data at risk: the scenario (Cyber security nel settore sanitario, a rischio apparecchiature mediche e dati riservati: lo scenario)’ (*Network Digital 360*, 5 Maggio 2020) <https://www.cybersecurity360.it/nuove-minacce/cyber-security-nel-settore-sanitario-a-rischio-apparecchiature-mediche-e-dati-riservati-lo-scenario/> accessed 15 January 2024
Sanger DE and Perlroth N, ‘Cyberattacks Against U.S. Corporations Are on the Rise’ (*The New York Times*, 12 May 2013) <www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html> accessed 29 December 2023
Schmitt MN, ‘Five Myths in the Debate about Cyber War’ (*Just Security*, 23 September 2013) <www.justsecurity.org/918/myths-debate-cyber-war/> accessed 6 December 2016
——, ‘Normative Voids and Asymmetry in Cyberspace’ (*Just Security*, 29 December 2014) <www.justsecurity.org/18685/normative-voids-asymmetry-cyberspace/> accessed 6 December 2016
Smith B, ‘A moment of reckoning: the need for a strong and global cybersecurity response’ (17 December 2020) <https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/> accessed 24 January 2024
Soesanto S, ‘After a Year of Silence, Are EU Cyber Sanctions Dead?’ (26 October 2021) <https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead> accessed 15 January 2024
Sol. P, ‘Coronavirus, hackers attack on Spallanzani in Rome. The Prosecutor's Office investigates (Coronavirus, attacco hacker allo Spallanzani di Roma. Indaga la Procura)’ (*Il Sole 24 Ore*, 1 April 2020) <https://www.ilsole24ore.com/art/coronavirus-attacco-hacker-spallanzani-roma-indaga-procura-roma-ADtLHTH?refresh_ce=1> accessed 28 November 2023
Sport UDfDCMa, ‘The NIS Regulations 2018’ (20 April 2018) <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 28 November 2023
Stolton S, ‘Von der Leyen: Chinese cyberattacks on EU hospitals ‘can’t be tolerated’’ (23 June 2020) <https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/> accessed 22 January 2024
Stupp C, ‘Commission should ‘walk the walk’ on cybersecurity, German chief says’ (*EURACTIV*, 9 April 2018) <https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/> accessed 9 January 2024
——, ‘French cybersecurity chief warns against ‘step back into the past’’ (*EURACTIV*, 25 April 2018) <https://www.euractiv.com/section/cybersecurity/news/french-cybersecurity-chief-warns-against-step-back-into-the-past/> accessed 15 January 2024
——, ‘Commission wants member states to trust each other more on cybersecurity’ (*EURACTIV*, 26 April 2016) <https://www.euractiv.com/section/digital/news/commission-wants-member-states-to-trust-each-other-more-on-cybersecurity/> accessed 23 December 2023
Sudworth J, ‘New 'cyber attacks' hit S Korea’ (*BBC News*, 9 July 2009) <http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm> accessed 21 January 2017
Templeton E and Dewar DRS, ‘The post-Brexit EU-UK relationship; an opportunity or challenge for cyber security?’ (*Geneva Centre for Security Policy*, 17 September 2021) <https://www.gcsp.ch/global-insights/post-brexit-eu-uk-relationship-opportunity-or-challenge-cyber-security> accessed 20 December 2023
The White House, ‘FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government’ (15 April 2021) <https://www.whitehouse.gov/briefing-room/statements-

releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> accessed 24 January 2024
The White House Office of the Press Secretary, 'Remarks by the President in Year-End Press Conference' (19 December 2014) <www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference> accessed 15 January 2024
Tocci N, 'On foreign policy, EU has to speak up — even if it's not with one voice' (1 October 2020) <https://www.politico.eu/article/eu-foreign-policy-vision-belarus-sanctions/> accessed 8 January 2024
Traynor I, 'Russia accused of unleashing cyberwar to disable Estonia' (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 22 January 2024
U.S. Embassy in the Czech Republic, 'The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector' (17 April 2020) <https://cz.usembassy.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/> accessed 15 January 2024
Vallance C, 'Ukraine cyber-attacks 'could happen to UK'' (*BBC News*, 29 February 2016) <www.bbc.co.uk/news/technology-35686493> accessed 15 January 2024
Watts S, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*Just Security*, 14 October 2016) <www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/> accessed 6 December 2016
Wright O, 'Isis plotting cyber warfare to kill people in UK, claims George Osborne' (*The Independent*, 17 November 2015) <www.independent.co.uk/news/uk/politics/paris-terror-attack-uk-government-to-invest-2bn-in-cyber-force-to-combat-online-terror-threats-a6737071.html> accessed 21 January 2017
Zetter K, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (*Wired*, 3 March 2016) <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> accessed 25 January 2024
Zinets N, 'Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'' (*Reuters*, 29 December 2016) <www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC> accessed 15 January 2023