European Law and Cyberspace

Ramses A. Wessel
Professor of European Law, University of Groningen, The Netherlands

Draft chapter – to be published in N. Tsagourias and R. Buchan (Eds.), *International Law and Cyberspace*, Cheltenham/Northhampton: Edward Elgar Publishing, 2021 (forthcoming)

1. INTRODUCTION: DEFINING EU CYBERSECURITY LAW

Does anything like cybersecurity law exist as part of European Union law? Cybersecurity is not mentioned as such in the EU Treaties as an area to be dealt with by the European Union. This should not come as a surprise. After all, while security reasons where behind the creation of the original European Communities in the 1950s, the main means were economic in nature. Nevertheless, after a number of earlier policy initiatives,[1] cybersecurity is now high on the EU's agenda in particular since the adoption of the 2013 Cybersecurity Strategy (updated in 2017[2]) and the 2015 Council conclusions on cyber-diplomacy.[3] The Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of a Directive on a common level of security of network and information systems.[4] More recently, in 2019, the EU adopted the EU Cybersecurity Act,[5] which aims to streamline various policies and relabelled the European Union Agency for Network and Information Security (ENISA) to the European Agency for Cybersecurity, while holding on to the original abbreviation.[6] The fact that the European Union justified and clarified its legal activities in this area in a 110-points preamble to the EU Cybersecurity Act points to an awareness that this is not obvious area to deal with from a legal perspective. At the same time, the proliferation of policy documents continues. On 24 July 2020, the European Commission published the latest addition to the collection of EU strategies, the new EU Security Union Strategy (SUS),[7] with, again, a strong emphasis on critical infrastructure protection and

[1] See for the early emergence of a European Union policy on cybercrime from a comparative perspective: F. Mendez, 'The European Union and Cybercrime: Insights from Comparative Federalism', *Journal of European Public Policy*, 2005, pp. 509-527; as well as R.A. Wessel, Cybersecurity in the European Union: Resilience through Regulation, in Elena Conde Pérez, Zhaklin V. Yaneva, Marzia Scopelliti (Eds.), *Routledge Handbook of EU Security Law and Policy* (Routledge, 2019), 283-300. The present contribution further builds on that latter publication as well as on the chapter 'Towards EU Cybersecurity Law: Regulating a New Policy Field' in the 2015 edition of this Research Handbook and can be seen as updates of these earlier publications.

[2] European Commission, 'State of the Union 2017 – Cyber-security: Commission scales up EU's response to cyber-attacks', Press release (Brussels, 19 September 2017).

[3] Respectively European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (Brussels, 7 February 2013), http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf; and *A Digital Single Market Strategy for Europe*, COM(2015) 192 final (Brussels, 6 May 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ EU L 151/15, 7.6.2019.

[6] https://www.enisa.europa.eu.

[7] EU Security Union Strategy, COM(2020) 605 final, Brussels, 24.7.2020; https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf.

resilience and plans for a new a Joint Cyber Unit to provide structured and coordinated operational cooperation.

Despite the absence of a clear and concrete legal basis for the EU to act in this area, and despite the Union's traditional focus on other policy areas, the range of initiatives shows that "cybersecurity is now among one of the EU's most important priorities, with cyber security elements having been integrated transversally within other EU policies."[8] The reasons are obvious: over the past years the number of cyber-attacks on states and critical infrastructure have been constantly growing,[9] and by its nature cyber security needs cross-border cooperation.[10] The EU measures aim to build resilience, fight cybercrime, build cyberdefence, develop industrial and technical resources and elaborate a diplomatic strategy for cyberspace.[11] Indeed, 'resilience' is a key-word in the EU's 2016 Global Strategy,[12] and this strategy seems more clearly aimed at responding to threats than at promoting values, as was the case in the 2013 Security Strategy. Cybersecurity is now presented as a key-element in the EU's security and resilience policies,[13] albeit that the Union's role is largely limited to 'coordinate', 'support', or 'assist' its Member States in this area due to the lack of express competences. That the Union is aware of this, is underlined in the 2019 Cybersecurity Act: "This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law."[14] Clearly showing the tension between the existence of national competences and the need for the EU to act, it adds the following:

"Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates

[8] Helena Carrapico and André Barrinha, 'European Union cyber security as an emerging research and policy field' (2018), 19 *European Politics and Society* 3, 299-303, at 300. See for a recent overview of the initiatives also Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights', in M. Christen et al. (eds.), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology* (Springer, 2020), 97-113 at 109; Faye F. Wang, 'Legislative Developments in Cybersecurity in the EU' (2020), 1 *Amicus Curiae* 2, 233-59; Agnes Kasper and Alexander Antonov, 'Towards Conceptualizing EU Cybersecurity Law' (2019) *ZEI Discussion Paper* C253; as well as George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan, 2016).

[9] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; as well as Kasper and Antonov, 'Towards Conceptualizing EU Cybersecurity Law'; Annegret Bendiek, *European Cyber Security Policy* (2012) *SWP Research Paper* 13; as well as J. Odermatt, 'The European Union as a Cybersecurity Actor', in Steven Blockmans and Panos Koutrakos (Eds.), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar Publishing, 2018). See earlier also the report by Neil Robinson et al., *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*, European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy, Sep. 2013.

[10] Cf. already the remarks by the European Commission in 2011 that cybercrime is "by its very nature cross-border" and hence "proper cross-border arrangements" are required. Commission Communication on Critical Information Infrastructure - results and next steps: the path to global security network, 3.12.2011, COM (2011) 163 final.

[11] Annegret Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy: From Trans-formation to Resilience', *SWP Research Paper*, October 2017.

[12] See *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, 2016; https://europa.eu/globalstrategy/en

[13] The term 'cyber' appears 23 times in the EU's Global Strategy. See more in general also George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan, 2016).

[14] EU Cybersecurity Act 2019, Art. 1(2).

effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance."[15]

These words underline the need for the European Union to adapt its security strategy to new threats.[16] Perhaps ironically this has to be done in a period in which traditional EU defence cooperation finally seems to be progressing. After decades of attempts to establish a defence cooperation alongside the EU's other policies, the careful introduction of the Common Security and Defence Policy (CSDP) in the 1992 Maastricht Treaty and its further adaptations through subsequent treaty revisions,[17] we now witness new and far-reaching initiatives, including the implementation of the notion of permanent structured cooperation (PESCO), new structures and frameworks, enhanced oversight and coordination mechanisms as well as financing tools to trigger joint defence research and development.[18]

The fact that the EU does not have an express competence to take measures to improve cybersecurity has led it to either use legal competences it has in other areas, or adopt soft-law and coordination measures (see section 3). This piecemeal approach has made it difficult to understand what exactly is covered by cybersecurity and, on that basis, to allocate tasks and responsibilities.[19] As underlined by Fuster and Jasmontaite "Definitions used to refer to cybersecurity by various actors, including EU Member States, bodies and institutions, typically represent different perspectives, which can potentially be at odds with each other."[20] And, central to the present chapter is the idea that "The lack of clarity about this core concept raises questions about coherence and consistency of already adopted and newly proposed legislative acts in the field of cybersecurity."[21]

The definition of cybersecurity that was included in the 2013 Cybersecurity Strategy of the European Union (EUCSS) has a broad scope:[22]

"*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."

A narrower definition was provided in the context of the 2019 Cybersecurity Act:

---

[15] EU Cybersecurity Act 2019, preamble, point 5.
[16] Bendiek, *European Cyber Security Policy*, at 5.
[17] See for a recent overview Ramses A. Wessel and Joris Larik (eds), *EU External Relations Law: Text, Cases and Materials* (Hart Publishing, 2020), Chapter 12.
[18] See further on these initiatives the PESCO Factsheet: https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en; as well as Steven Blockmans, 'The EU's modular approach to defence integration: An inclusive, ambitious and legally binding PESCO?' (2018), 55 *Common Market Law Review* 6, 1785-1826.
[19] Cf. Odermatt, 'The European Union as a Cybersecurity Actor'; as well as Krystof F. Sliwinski, 'Moving Beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35(3) *Contemporary Security Policy* 468, 470: "There is no coherent European understanding of what the notion of cyber-security should include. Consequently, conceptualization differences are more than likely to produce different approaches to respective national capabilities catalogues. Such inconsistencies, when reinforced by national security narratives and traditional sovereignty claims, are more than likely to leave the EU toothless in the future."; and Federica Di Camillo and Valérie Miranda, 'Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward', Working Paper No. 11, IAI 26 September 2011.
[20] Fuster and Jasmontaite, *op.cit.*, at 104.
[21] Kasper and Antonov, *op.cit.*
[22] Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013 ('EUCSS').

"'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats."

This relates to ensuring the resilience of networks to potential attacks and the capacity to respond to such attacks.

Yet, cyberspace policies usually also include 'cybercrime'. Indeed, both the broader notion of 'cybersecurity' and the criminal activities falling under 'cybercrime' form part of the EU's policies.[23] In the 2013 EU Strategy it is described as follows:

"*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)."

Hence, while *cybersecurity* refers to the range of safeguards and actions that can be used to protect the cyber domain, *cybercrime* reflects to the actual criminal activities, thus following the descriptions laid down in the Council of Europe Convention on cybercrime.[24] Debates on activities in cyberspace also refer to many more phenomena. Where cybercrime involves offences against property rights of non-state actors (e.g., phishing), *cyber espionage* concerns breaches in the databases of state or non-state enterprises by foreign government agencies, and *cyber war* involves state attempts to attack another state via electronic networks.[25] Given the Union's activities under the heading of its Common Security and Defence Policy (CSDP), it is striking that the latter is hardly mentioned in the EU's documents on cybersecurity. Indeed, allegedly for reasons of Member State sovereignty in the military field, the term *cyberdefence* lacks a clear definition in the EU context.[26]

The aim of the present chapter is to provide an introduction into the ways in which the European Union aims to play a role in the regulation of cybersecurity, both in relation to its own Member States as in contributions to global law-making and governance. Section 2 starts with presenting the internal objectives of the Union as well as its global ambitions in this area. This is followed by an analysis of existing legal competences in Section 3. Section 4 will draw some conclusions.

---

[23] See for a discussion on definitional questions also Elaine Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' (2014, *European Journal of Risk Regulation*, 46-60: "Conceptually, cybercrime may be defined both narrowly, to include offences against computer data and systems but also more broadly, to include offences committed with the help of computer data and systems. By contrast, cyber-security usually relates to four major societal threats- crime, cyberwar, cyber terrorism and espionage" (at 47).

[24] Convention on Cybercrime, CETS No. 185, Council of Europe, signed 23 November 2001 in Budapest, entry into force 1 July 2004.

[25] See the chapters by […., elsewhere in this volume]. Cf. Annegret Bendiek and Andrew L. Porter, 'European Cyber Security Policy within a Global Multistakeholder Structure' (2013), *European Foreign Affairs Review* 2, 155–180, at 158. This article also provides a good overview of the wide scope of the actual problems caused by a lack of cybersecurity.

[26] George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan, 2016) 6: "Cyber defence is not defined within the EU documents given the sensitivity among member states on this issue, and the reluctance of certain member states to participate given their own cyber defence strategies."

2. EU GLOBAL AND INTERNAL OBJECTIVES OF CYBERSECURITY

As noted above, with the adoption of the 2016 *Global Strategy for the European Union's Foreign and Security Policy* the EU stressed the importance of 'resilience'.[27] In fact, the term is used more than 30 times in the 60-page Global Strategy, turning 'resilience' into a key objective of the EU security strategy. While the term as such is not defined by the Global Strategy, the context makes clear that the main ambition is to resist and overcome threats to the EU's security and democratic values:[28] "The Strategy nurtures the ambition of strategic autonomy for the European Union. This is necessary to promote the common interests of our citizens, as well as our principles and values."[29] Yet, the idea of autonomy should not be read as to isolate the EU. On the contrary: "Together with its partners, the EU will [also] promote resilience in its surrounding regions".[30] And, this is done in cooperation with international partners. Thus, the EU Cyber Defence Policy Framework, for instance, clearly refers to cooperation with other international organizations, including NATO.[31] In addition, cybersecurity and cyber-defence cooperation between the EU and NATO has been intensified since 2015, formalised in the July 2016 Warsaw Declaration, and reinforced with concrete implementation proposals at the joint meeting of the EU and NATO foreign ministers in December 2016.[32] More generally, the Union has engaged in a number of strategic partnerships with third countries, also as part of its strategy to 'mainstream' cyber issues in the EU's external relations.[33]

In joining the large group of global governmental and non-governmental actors active in the governance and regulation of cybersecurity,[34] the European Union commits again to its traditional role

---

[27] See also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 6.

[28] As phrased by the Global Strategy at p. 21, it is about: "the swift recovery of Members States in the event of attacks". See also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 6: "Resilience is generally understood as 'a capacity to resist and regenerate', as well as be 'crisis-proof'. The concept acknowledges that there are practical limits to the normative goal of external transformation as outlined in article 21 paragraph 2 of the TEU. Resilience therefore aims to enable the EU both to maintain its existing values and norms and to pursue its own interests."

[29] EU Global Strategy, at 4.

[30] EU Global Strategy, at 23.

[31] Cyber Defence Policy Framework, Brussels, 19 November 2018 14413/18; https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.. See further also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18.

[32] Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18; and Bruno Lété and Daiga Dege, *NATO Cybersecurity: A Roadmap to Resilience*, Policy Brief 3, 2017 (Washington: The German Marshall Fund of the United States, July 2017).

[33] Thomas Renard, 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain', *European Politics and Society*, 2018, 321-337. Renard lists the following dialogues in the framework of strategic partnerships: Brazil (Dialogue on international cyber policy; Information society dialogue); Canada (EU-US-Canada Expert Meeting on Critical Infrastructure Protection China Cyber taskforce; Dialogue on IT, telecommunications and informatisation); India (Political dialogue on cyber-security; Information society dialogue); Japan (Cyber dialogue; Dialogue on ICT policy); Mexico (Working Group on telecommunications; Dialogue on public security and law enforcement); Russia (Information society dialogue South Africa Information society dialogue); South Korea (Cyber dialogue; Information society dialogue); USA (Working Group on Cyber-security and Cyber-crime (WGCC); Cyber dialogue; Information society dialogue; EU-US-Canada Expert Meeting on Critical Infrastructure Protection).

[34] In a recent study we came to a list of international institutions that at least includes the European Union, the Council of Europe, the United Nations, the International Telecommunications Union (ITU), the African Union, Microsoft, the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), NATO, Net Mundial, the G7, the Internet Governance Forum, the Electrical and Electronic Engineers (IEEE), the International Electro-technical Commission (IEC), ICANN, the Asia-Pacific Economic Cooperation (APEC), the Organization for Security and Co-operation in Europe (OSCE), the OECD, the G8, Interpol, the organization of American States (OAS), the Arab League and Gulf Cooperation Council, the International Multilateral Partnership Against Cyber Threats, the G20, the Shanghai Cooperation Organisation, the World Trade Organization (WTO), the World Intellectual Property Organization (WIPO), and UNESCO. See Tatiana

as a normative actor, in line with its brief in Articles 3(5) and 21 of the Treaty on European Union.[35] While the EU is sometimes successful in getting its standards accepted by many other countries – as exemplified by the European General Data Protection Regulation (GDPR)[36] – developing its own rules and standards may also contribute to the current fragmentation in actors, definitions and norms characterizing the current global regime in this field.[37]

In any case, any possible contribution to the global regulation of cybersecurity very much depends on the internal activities the EU is engaged in. In order to understand the EU's ambitions and plans related to cybersecurity, it is useful to quote the respective paragraph in the Global Strategy in full:

"The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. *It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations*, and further developing platforms for cooperation."[38]

Cybersecurity is thus presented as a 'cross-sectional' policy task, and should be a dimension of different EU policy areas related to both internal and external security and civilian as well as military cooperation.[39]

More concrete ambitions can be found in the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*,[40] that addresses different dimensions of cybersecurity, including network and information security (NIS), cybercrime, and cyberdefence. The general starting point is the following: *"For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online"*.[41] The Cybersecurity Strategy can be seen as a continuation of the internal and external policies that have been developed by the EU in the area of NIS[42] – and in the framework of the EU-US Working Group on Cyber-Security and Cyber-Crime (WGCC).[43] The European Commission announced plans to update the Cybersecurity Strategy in 2020.[44] Part of the Cybersecurity Strategy is related to linking core EU values that exist in the 'physical world' to the

---

Nascimento Heim and Ramses A. Wessel, 'The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms', in Lucía Millán Moro (dir.) and Gloria Fernández Arribas (ed.), *Ciberataques y Ciberseguridad en la Escena Internacional* (Aranzadi Thomas Reuters, 2020), 146-173.

[35] Wessel and Larik, 'The EU as a Global Actor', in Ramses A. Wessel and Joris Larik (Eds.), *EU External Relations Law: Text, Cases and Materials* (Hart, 2020, 2nd ed.) 1-28.

[36] Giovanni Buttarelli., 'The EU GDPR as a clarion call for a new global digital gold standard', 6 *International Data Privacy Law* (2016), 77–78. See more generally, Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP, 2020).

[37] See Nascimento Heim and Wessel, 'The Global Regulation of Cybersecurity'.

[38] Global Strategy, at 21-22; emphasis added.

[39] Cf. also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18.

[40] See above.

[41] EU Cybersecurity Strategy, at 1.

[42] *Inter alia* resulting in the 2001 Commission Communication on 'Network and Information Security: Proposal for a European Policy Approach' (COM(2001)298) and the 2006 'Strategy for a Secure Information Society' (COM(2006)251).

[43] EU-U.S. Summit 20 November 2010, Lisbon - Joint Statement, European Commission - MEMO/10/597 20/11/2010. See also Maria Grazie Porcedda, 'Transatlantic Approaches to cyber-security and cybercrime', in Patryk Pawlak (Ed.), *The EU-US Security and Justice Agenda in Action*, EUISS Chaillot Paper, No. 127, 30 December 2011; as well as Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking'.

[44] https://ec.europa.eu/digital-single-market/en/cyber-security

'digital world': promoting fundamental rights, freedom of expression, personal data and privacy; access for all; democratic and efficient multi-stakeholder governance and a shared responsibility to ensure security. Other elements relate to other policy areas of the EU, including the internal market or defence policy. As an express legal basis cannot be found in the EU Treaties, the Strategy acknowledges that "it is predominantly the task of the Member States to deal with security challenges in cyberspace."[45] It lists five strategic priorities: achieving cyber resilience; drastically reducing cybercrime; developing cyberdefence policy and capabilities related to the Common Security and Defence Policy; develop the industrial and technological resources for cybersecurity; and establish a coherent international cyberspace policy for the European Union and promote core EU values.

Relying on a total of 27 Member States to take the necessary measures, however, again risks fragmentation. Primarily to overcome this risk, the European Agenda on Security (EAS) was adopted, as "an effective and coordinated response at European level",[46] providing a strategic framework for EU initiatives in the field of cybersecurity. Specific policies in relation to CSDP had already been formulated in the EU Cyber Defence Policy Framework,[47] to further integrate cybersecurity and defence into CSDP. The focus on these policies is on enhancing cyber-resilience of CSDP missions and operations through for instance standardised procedures and technical capabilities in both civilian and military missions and operations.

More recently, the Commission laid down the EU ambitions in a comprehensive 'cybersecurity package': *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.[48] This policy document – sometimes referred to as the 2017 Joint Communication or the Second Cybersecurity Strategy – further analyses the way forward and introduces a large number of new policy initiatives and actions by the EU, but also calls upon Member States to, *inter alia*, ensure full and effective implementation of the NIS Directive; apply the same rules to public administrations, given the role they play in society and the economy as a whole; provide cybersecurity-related training in public administration; prioritise cyber-awareness in information campaigns and including cybersecurity as part of academic and vocational training curricula; and use initiatives on the 'Permanent Structured Cooperation' (PESCO) and the European Defence Fund to support the development of cyber defence projects.

Overall, the conclusion is that the European Union is very active in developing policies related to all dimensions of cybersecurity, mainly by drafting policy frameworks and guidelines to enhance and synchronise Member State initiatives. The topic is clearly high on the agenda and the EU's ambition is to play a central coordinating role in this area. Indeed, with one main goal in mind: resilience through policy-making and regulation. These policies are more internal than external.[49] This implies, as also rightfully concluded by Odermatt, that "Unlike some other states, the EU has not sought to develop any kind of hard or offensive cyber power. The EU's approach to cyberdefence is guided by the logic of protection."[50] The fact that external competences often depend on the existence (and/or use) of internal

[45] Cf. also Emmanuel Darmois and Geneviève Schméder, 'Cybersecurity: a case for a European approach', SiT Paper SiT/WP/11/16; http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf.

[46] Communication from the Commission to the European Parliament, the Council, European Economic and Social Committee and the Committee of the Regions, European Agenda on Security, COM (2015) 185 final.

[47] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

[48] Joint Communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Brussels, 13.9.2017, JOIN(2017) 450 final.

[49] The Cybersecurity Strategy even clearly states that "The EU does not call for the creation of new international legal instruments for cyber issues" (at 15).

[50] Odermatt, 'The European Union as a Cybersecurity Actor'.

competences,[51] has indeed limited the Union's legal powers as a global actor in this field.[52] This is not to say that the Union is completely passive in its external relations with regard to cybersecurity initiatives. It does see itself as "a global digital player", that aims at mainstreaming 'digital issues' in its foreign policy (see also section 3 below).[53] The question remains, however, to what extent the EU has the legal competence to realise its internal as well as external ambitions.

3. EU COMPETENCES RELATED TO CYBERSECURITY

"The EU is well placed to address cybersecurity, given the scope of its policies and the tools, structures and capabilities at its disposal. While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity".[54]

Irrespective of this statement by the European Commission, the question is whether also in a legal sense, the EU is "well placed" to address cybersecurity.[55] Given the inherent cross-border nature of cybersecurity, the complete absence of the issue in the EU treaties is striking and was not even part of the 2009 treaty update. One reason may be that cooperation by the EU Member States or a transfer of competences to the EU may not be sufficient, precisely because of the larger, global scope of the challenge and the involvement of multiple actors.[56] Yet, given the EU's ambitions described in the previous section, concrete legal bases to at least also formally regulate cybersecurity need to be found. After all, the European Union, like other international organization, fully depends on an attribution of competences, not only for its internal activities, but also for engaging in cooperation with other states and international institutions. [57] And in the absence of express powers, these will need to be found in relation to other policy sectors. This was also emphasised by the European Parliament:

---

[51] Cf. Wessel and Larik, *EU External Relations Law*, Chapter 3.

[52] See Renard, 'EU Cyber Partnerships, at 326: "But just like in many other policy areas, the EU aims to assert itself in the global arena through 'soft power' assets and diplomatic skills"

[53] See Europe as a Global Digital Player; https://ec.europa.eu/digital-single-market/en/content/europe-global-digital-player

[54] 2017 Joint Communication to the European Parliament and the Council.

[55] The Union's activities partly build on the EU's engagement with the regulation of the Internet in a broader sense – with co-regulation as an important dimension. See for instance Franz C. Mayer, 'Europe and the Internet: The Old World and the New Medium' (2000), *European Journal of International Law*, 2000, pp. 149-169. See also Christopher T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge: Cambridge University Press, 2011.

[56] Cf. Jan Kleijssen and Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options' (2016), *Netherlands Yearbook of International Law*, 147-173. Indeed, as mentioned by the authors, the Council of Europe in particular has been used to draft (even more broadly accepted) instruments, such as the 2001 Budapest Convention on Cybercrime (ETS No. 185) as well as a large number of treaties on international co-operation in criminal matters, including in particular the European Convention on Mutual Assistance in Criminal Matters (ETS No. 030), its Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 099), and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182). Cf. also Bendiek and Porter, 'European Cyber Security Policy'.

[57] Cf. also Art. 5(2) TEU: "Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States." Indeed, the 'principle of conferral' may further complicate things and leaves the Union with two options: it either connects cybersecurity to existing competences in other fields, or it uses soft law instruments to stimulate Member States and other relevant actors to implement parts of its strategies. See on the various competence problems in relation to the cooperation of the EU with other international organizations: Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations* (Edward Elgar, 2019).

"conflicts and crises in Europe and around are happening in both physical and cyber space, and underlines that cyber security and cyber defence must therefore be integrated as the core elements of the CSDP and fully mainstreamed throughout all the EU's internal and external policies."[58]

Whereas this is understandable, it also entails a risk of fragmentation and inconsistency when different EU (and member states') institutions, as well as private actors (industry, service providers, etc.) are involved, all with their own policy preferences and procedures. It is questionable whether the demands for consistency and effectiveness (Articles 13 and 21 TEU) can be met. Cybersecurity forms an excellent example of an area in which the different policy fields of the Union need to be combined (a requirement for *horizontal* consistency), and where measures need to be taken at the level of both the EU and the Member States (calling for *vertical* consistency). This possible fragmentation thus raises the question to what extent the above-mentioned ambitions aimed at ensuring 'resilience through regulation' can actually be attained, both internally and in the framework of the EU's external relations.

In an institutional sense, a number of initiatives have been taken to create specialised bodies, but again in specific fields only.[59] Thus, a special EU Cybercrime Centre (EC3) was established[60] and located at one of the EU's agencies, Europol in The Hague.[61] EC3 officially commenced its activities on 1 January 2013 with a mandate to tackle the following areas of cybercrime:

a. That committed by organised groups to generate large criminal profits such as online fraud
b. That which causes serious harm to the victim such as online child sexual exploitation
c. That which affects critical infrastructure and information systems in the European Union.

EC3 thus aims to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners in the pursuit of an EU free from cybercrime. It publishes the yearly Internet Organised Crime Threat Assessment (IOCTA) on key findings and emerging threats and developments in cybercrime.[62] Yet, for the development of actual legislation, it is necessary for the European Commission and the European External Action Service (EEAS) to be involved. For that reason EC3 liaison offices have been placed at those institutions and to other relevant agencies, including ENISA, the EU Cybersecurity Agency.[63] This latter agency is located in Greece and has by now become the main body in this field and it also works to improve cooperation between Member States to implement emergency response plans, conduct regular emergency drills, and develop systems to guard against attacks on critical infrastructure.[64]

Overall, however, it is questionable whether this somewhat loose institutional framework will allow the Union to regulate the field of cybersecurity in any comprehensive fashion. The following sub-sections will provide some examples of legal bases used to tackle different dimensions of cybersecurity.

---

[58] See also: European Parliament, European Parliament Resolution of 23 November 2016 on the Implementation of the Common Security and Defence Policy, 2016/2067(INI) (Strasbourg, 23 November 2016), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0440&language=EN

[59] See on the institutional developments also Jukka Ruohonen, Sami Hyrynsalmi, an Ville Leppänen, 'An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus' (2016), *Government Information Quarterly* 33, 746-756.

[60] Council conclusions on the establishment of a European Cybercrime Centre, 3172nd Justice and Home Affairs Council meeting Luxembourg, 7 and 8 June 2012.

[61] See https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[62] See https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

[63] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ L 77, 13.3.2004.

[64] https://www.enisa.europa.eu/

(a) The Single Digital Market

In terms of EU competences, a number of measures with an economic dimension fall under initiatives in the framework of the so-called 'Single Digital Market' (DSM). The Digital Single Market strategy was adopted on the 6 May 2015. It includes 16 specific initiatives which have been delivered by the Commission by January 2017.[65] The EU refers to an obvious economic element, which relates to the completion of the DSM: citizens need trust and confidence to engage in new connected technologies and to use e-commerce facilities.[66]

Indeed, the extensive internal market competences of the Union do provide some hooks for cybersecurity measures related to the functioning of the free movement or competition rules. This, for instance allows the Union to harmonise national rules with a view to the functioning of the internal market. A concrete example is formed by using the 'internal market harmonisation' provisions in Article 114 TFEU, as was done to find a the legal basis for the Directive on Security of Network and Information Systems ('NIS Directive').[67] The NIS Directive forms the first piece of EU-wide legislation on cybersecurity, aimed at boosting the overall level of cybersecurity in the EU. Member States had to transpose the Directive into their national laws by 9 May 2018.[68] The Commission argued that under Article 114 TFEU, the EU can adopt "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",[69] and security of network and information systems is seen as essential for the functioning of the internal market. The Directive presents the 'internal market' rationale as follows:

"Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. […] Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market."[70]

---

[65] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, Brussels, 6.5.2015, COM(2015) 192 final.

[66] See much earlier already the Electronic Commerce Directive, adopted in 2000, which introduced an Internal Market framework for electronic commerce, providing legal certainty for business and consumers alike. It established harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

[67] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, 1 ('NIS Directive'). See also Johan David Michels and Ian Walden, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?' (2020), *European Law Review*,; Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation', *Computer Law & Security Review* (2019), 105336.

[68] See https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[69] 'NIS Directive', Explanatory memorandum.

[70] Preamble of the NIS Directive, points 1 and 3.

The Directive thus aims at setting a high common level of network and information security across the EU in a number of ways: 1. By requiring Member States to be adequately prepared for cyber threats. This involves the establishment of national NIS Strategies and national Computer Security Incident Response Teams (CSIRTs); and 2. by promoting cooperation between the Member States, e.g. through requirements for security and notification. The NIS Directive thus aims at securing resilience in certain critical sectors, including energy, health, transport and banking.[71] The involvement of the private sector – including a system for certification and labelling to achieve a functioning single market in cybersecurity – returns in the 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.[72] Enhancing trust in the internal market is also pursued by the Regulation on electronic identification and trust services for electronic transactions in the EU internal market.[73] This Regulation is also based on Article 114 TFEU, which concerns the adoption of rules to remove existing barriers to the functioning of the internal market.

In general, these initiatives only seem to form the start of a range of new measures. The 2017 Mid-Term Review of the Single Digital Market process[74] listed a large number of contributing threats and reveals the complications the EU is facing, also in terms of competences: "Cyberattacks are on the increase and tackling them faces the problem that while cyber-attacks are often cross-border, law enforcement competences are strictly national. […] This requires effective EU level response and crisis management, building upon dedicated cyber policies and wider instruments for European solidarity and mutual assistance."

(b) Cybercrime

Another policy area in which the EU has been relatively active when it comes to the regulation of cybersecurity is 'cybercrime'. The 2005 Framework Decision on attacks against information systems is probably one of the first legal instruments adopted by the Union in relation to cybersecurity.[75] The main objective of that Decision was to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems. With a view to the integration of the former Police and Judicial Cooperation in Criminal Matters (PJCC) in the Union's Area of Freedom, Security and Justice (AFSJ), in August 2013 this Decision was replaced by the Directive on attacks against information systems (the 'Cybercrime Directive').[76] The legal basis of this Directive is Article 83(1) TFEU, which underlines that it forms part of the judicial cooperation in criminal matters, currently laid down in that part of the Treaty. In fact, this is one of the areas where one may find a competence of the EU to legislate in the area of cybercrime (despite the fact that the term is not used as such). Article 83(1) TFEU provides:

---

[71] Cf. also Odermatt, 'The European Union as a Cybersecurity Actor'.

[72] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the European Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016) COM (2016) 410 final.

[73] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; OJ L 257, 28.8.2014, p. 73-114.

[74] Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy, *A Connected Digital Single Market for All*, Brussels, 10.5.2017, COM(2017) 228 final.

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

[76] See above.

"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 resulting from the nature or impact of such offences or from a special need to combat them on a common basis.
These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime."

The Cybercrime Directive establishes minimum rules on the definition of criminal offences and sanctions with respect to attacks against information systems. [77] It also provides minimum rules on the definitions of crimes included in the Directive.

Other instruments adopted in this area include the 2011 Directive on Combatting the Sexual Exploitation of Children Online and Child Pornography, the 2002 ePrivacy directive, ensuring the confidentiality of client information,[78] and the 2001 Framework Decision on combating fraud and counterfeiting.[79] In addition, new proposals have been issued in 2018 and 2019, including a Regulation and a Directive to facilitate law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists,[80] as well as a new Directive on non-cash means of payment, which updates the legal framework, removing obstacles to operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.[81]

In terms of international cooperation, it is important to note that the EU is not a party to the main international treaty in this area, the Council of Europe Convention on Cybercrime (Budapest Convention),[82] although it participates in the Cybercrime Convention Committee (T-CY).

(c) Cyberdiplomacy

The EU's Common Foreign and Security Policy (CFSP) also does not explicitly address cybersecurity, Yet, Article 24(1) TEU provides that "the Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and *all questions relating to the Union's security*".[83] The latter part of this sentence indeed seems to allow for measures to be taken using CFSP as a legal basis.[84] While for a long time cybersecurity issues were not part of the EU's foreign policy, the EU recently adopted a framework for a joint EU diplomatic response to malicious cyber activities

[77] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, 8. This Directive replaced the 2005 EU Framework Decision on Attacks against Information Systems.
[78] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337, 18.12.2009, 11.
[79] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OJ L 149, 2.6.2001, 1.
[80] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD).
[81] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA PE/89/2018/REV/3.
[82] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Cf. also M. Keyser, 'The Council of Europe Convention on Cybercrime' (2002-2003), *Journal of Transnational Law & Policy*, 287-327.
[83] Emphasis added.
[84] See for a recent basic analysis of CFSP, Ramses A. Wessel, 'Common, Foreign, Security and Defence Policy', in Wessel and Larik, *EU External Relations Law*, 283-326.

(the so-called 'cyber diplomacy toolbox'), which sets out the measures under the broader CFSP.[85] The instrument makes a start with listing, primarily, non-military instruments that could contribute to "the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations".[86] Part of this initiative is an explicit extension of the EU's sanctions regime to cyber-attacks. In 2019 the Council adopted a Decision and a connected Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[87] Taking restrictive measures falls under the Union's competence as laid down in Articles 29 TEU and 215 TFEU. The Decision "applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States."[88] It relates to cyber-attacks aimed at critical infrastructure; services necessary for the maintenance of essential social and/or economic activities; critical State functions; the storage or processing of classified information; or government emergency response teams. EU Member States will have to take the measures necessary to prevent the entry into, or transit through, their territories of "(a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks; (b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission; (c) natural persons associated with the persons covered by points (a) and (b)",[89] and funds of these persons and entities have to be frozen.[90] The mentioned Regulation spells out the rules in more detail and underlines that the rules are binding in each of the EU Member States. The first sanctions on the basis of the new regime were adopted on 30 July 2020, when four Russians were listed that were said to be guilty of trying to hack an international institute, the Organisation for the Prohibition of Chemical Weapons, in The Hague, in 2018. In addition, two Chinese men and a Chinese company were listed, in relation to the stealing of commercially-sensitive secrets from Western multinational firms. Finally, the new Decision names a North Korean firm for a number of cyber attacks in Poland.[91]

(d) Cyberdefence

Cyberdefence is still underdeveloped in comparison to the economic and criminal law aspects of cybersecurity discussed above; it is still characterised by a piecemeal approach. As Odermatt rightfully states: "there is no comprehensive EU approach to cyberdefence",[92] despite the claim that "the next war will begin in cyberspace".[93] The EU has slowly started to realise this and in 2014 adopted the first EU Cyber Defence Policy Framework, with a most recent update in 2018.[94] This document now clearly

[85] See Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), Brussels, 7 June 2017 (OR. en) 9916/17.
[86] See Annegret Bendiek, 'The EU as a Force for Peace in International Cyber Diplomacy', *SWP Comment*, No. 19, April 2018.
[87] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I , 17.5.2019; and Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I , 17.5.2019; updated in 2020 by Council Decision (CFSP) 2020/651 of 14 May 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 153, 15.5.2020.
[88] Art. 1 of the Decision.
[89] Art. 4 of the Decision.
[90] Art. 5 of the Decision.
[91] Council Decision (CFSP) 2020/1127 of 30 July 2020, OJ 246/12, 30.7.2020.
[92] Odermatt, 'The European Union as a Cybersecurity Actor'.
[93] Gen. Keith B. Alexander, upon accepting the post to lead the first United States Cyber-Command (USCYBERCOM). Quoted by R. Hughes, 'A Treaty for Cyberspace' (2010), *International Affairs*, 523–541.
[94] Cyber Defence Policy Framework; https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.

views cybersecurity as an integral part of the Union's defence strategy: "Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities."[95] The document provides a framework for countering cyber threats and defines the cyberdefence aspects of the EU Cyber Security Strategy mentioned earlier. Its aim is to link cyberdefence issues to the Union's Common Security and Defence Policy (CSDP) and maps the various steps to be take, together with the European Defence Agency (EDA). A good example of this is also to be found in the fact that cyberdefence has also become part of the Permanent Structured Cooperation (PESCO) framework, in which EU Member State work closely together in various projects. A number of these projects specifically focus on cybersecurity, including 'Cyber Threats and Incident Response Information Sharing Platform' and 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'.[96]

To what extent could a cyber-attack trigger the common defence obligations EU Member States have on the basis of the Treaties? To answer that question, it is first of all important to note that the above-mentioned Cybersecurity Strategy refers to the so-called 'solidarity clause' laid down in Article 222 TFEU.[97] On the basis of that provision obligations exists for the Union and its Member States to combine their efforts:

"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:
(a) – prevent the terrorist threat in the territory of the Member States;
– protect democratic institutions and the civilian population from any terrorist attack;
– assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;
(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."

Indeed, cyber-attacks are not mentioned explicitly. Yet, they easily fit under some of the headings. In a 2012 Resolution, the European Parliament even explicitly mentioned cybersecurity as falling within the scope of the solidarity clause: it called for "an adequate balance between flexibility and consistency as regards the types of attacks and disasters for which the clause may be triggered, so as to ensure that no significant threats, such as attacks in cyberspace, pandemics, or energy shortages, are overlooked […]".[98] In fact, the European Parliament even went a step further and also mentioned cyber-attacks as a reason to invoke the so-called 'mutual defence clause' laid down in Article 42(7) TEU, containing a provision comparable to Article 5 of the NATO Treaty:

"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, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States."

The European Parliament took the view "that even non-armed attacks, for instance cyberattacks against

[95] Cyber Defence Policy Framework.
[96] https://pesco.europa.eu/. See also Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans, Andrea Renda, 'Strengthening the EU's Cyber Defence Capabilities', *CEPS Report*, November 2018.
[97] See for instance Yuri Bogmann-Prebil and Malcolm Ross (Eds.), *Promoting Solidarity in the European Union* (OUP, 2010).
[98] European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)), par. 20.

critical infrastructure, that are launched with the aim of causing severe damage and disruption to a Member State and are identified as coming from an external entity could qualify for being covered by the clause, if the Member State's security is significantly threatened by its consequences, while fully respecting the principle of proportionality […]".[99] While in the case of the solidarity clause it may be argued that there needs to be a link with 'terrorism', the mutual defence clause refers to 'armed aggression', which in international law terms may rule out certain cyberattacks.[100] Hence, in both cases the application of the clauses to situations of cybersecurity is not always obvious. In practice, however, invoking a solidarity or a mutual defence clause will most probably be driven more by political incentives than by legal doctrinal analysis.

4. Conclusion and Assessment

The various hard and soft law instruments to regulate cybersecurity reveal that cyberspace has clearly become part of the EU's agenda and that a sub-discipline of 'EU Cybersecurity Law' is indeed in a nascent state. The relatively slow development of this area is not only related to the absence of clear legal competences on the side of the EU, but also to the early notion that by its very nature 'cyberspace' could and should not be regulated. It could not be regulated because of the fact that the phenomenon sits uneasily with traditional notions of territorial jurisdiction and it should not be regulated because "regulatory efforts […] would unduly restrict the great potential of the Internet."[101]

Over the years, however, the European Union has put great efforts in formulating ambitious cybersecurity policies. While this has resulted in an impressive pile of policy and strategy papers produced by the various EU institutions (the Commission in particular), clear legal competences to actually regulate the field are indeed hard to find and measures do not necessarily relate to traditional notions of 'security'. As also rightfully held by others "Most of the EU's action in the field of cybersecurity has dealt with internal EU policies (e.g. internal market and consumer protection) or is linked to criminal law (combatting cybercrime) and is tied to the goals of economic growth and the internal market."[102] The focus on the social-economic dimension, is understandable since in that area connections were easier to make and the internal market still forms the core of what the EU stands for. In the words of Dewar "The system of exclusive, shared, supporting and special competences established a policy framework in which the EU was restricted to non-military, socio-economic policy choices. The result of this restriction was that only socio-economic considerations in cyber security could be developed and implemented."[103] This also led to path dependencies and made it more difficult to connect to newer policy areas.[104]

At the same time, the EU now seems to be moving beyond internal measures only. In line with the more general increased attention for its global role,[105] the EU is clearly attempting to mainstream cyber issues throughout its existing foreign and security policy. One reason is that it is increasingly difficult to separate internal and external threats in this field.[106] The more active role of the EU in global debates and the recent initiatives on the 'cyber diplomacy toolbox' and restrictive measures against

[99] Ibid, at par. 13.
[100] Cf. M. Roscini, 'Cyber operations as a Use of Force' and C. Focarelli, 'Self-Defence in Cyberspace', elsewhere in this volume […]
[101] Zekoll, 'Jurisdiction in Cyberspace', at 342-343.
[102] Odermatt, 'The European Union as a Cybersecurity Actor'.
[103] Robert Scott Dewar, *Cyber Security in the European Union*, PhD thesis University of Glasgow, at 212.
[104] See on the incremental approach of the Union's in the regulation of cybersecurity also George Christou, 'The collective securitisation of cyberspace in the European Union' (2019), 42 *West European Politics* 2, 278–301.
[105] See for a recent assessment Wessel and Larik, 'The European Union as a Global Actor'.
[106] Bendiek and Porter, 'European Cyber Security Policy', at 156-157.

persons involved in cyber-attacks, reveal that the EU has been able to use existing competences in various *offline* fields, to regulate *online* activities.

Using various competences and different policy fields does, however, come at a price. This chapter points to the need for a comprehensive regulatory approach to overcome the current fragmentation in EU cybersecurity instruments. This fragmentation is not a choice, but simply results from the fact that no express cybersecurity competence exists and that it is not always easy (and sometimes even impossible) to combine the different cybersecurity dimensions in consistent or even connected policies due to the need for different legal bases. As held by some observers, "one of the key challenges of cybersecurity regulation is to impose the right obligations on the right actors, through the right instrument."[107] Even the field of 'security' is still characterised by a substantial degree of fragmentation, with security aspects being covered by the Internal Market, the Area of Freedom, Security and Justice (AFSJ) and the Common Foreign, Security and Defence Policy. Maintaining (or in fact creating) consistency (or at least coherence) in EU cybersecurity policy might very well be the main challenge for the EU the coming years.[108]

[107] Fuster and Jasmontaite, *op.cit.*, at 109.

[108] See also Helen Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017), 55 *JCMS* 6, 1254-1272 (at 1267): "[…] the EU has an explicit ambition to be a coherent security actor. However, both the architecture put in place under the [EU Cybersecurity Strategy] and the resistance from Member States to allow the EU to have a more stringent control over their cyber activities, limit the EU's coherence in the field. That said, both the rising political importance given to cybersecurity and the progressive consolidation of what is still a rather recent field of activity, means there are signs the EU might move towards a more coherent actorness in the field."