Cybersecurity in the European Union: Resilience through Regulation?

Ramses A. Wessel
Professor of International and European Law and Governance, University of Twente, The Netherlands

Draft chapter – to be published in Elena Conde, Zhaklin Yaneva, Marzia Scopelliti (eds), *Routledge Handbook of EU Security Law and Policy*, Routledge, 2019, pp. 283-300

"We must develop capabilities in trusted digital services and products
and in cyber technologies to enhance our resilience"
(EU Global Strategy, 2016)

Summary
Cybersecurity is high on the policy agenda of the European Union and can be seen as an emerging field of research, both in policy and legal studies. The recent adoption of new Directives on information and network security and on cybercrime reveal the possibilities of the EU to use existing competences in other policy fields to regulate aspects of cybersecurity. 'Resilience' of existing structures as well as of EU values is at the core of the Union's approach to cybersecurity. Yet, a comprehensive approach is missing, leading to a risk of fragmentation and incoherence. So far, measures related to the Single Digital Market and to cooperation on criminal law have been more elaborate than measures related to cyberdefence.

1. Introduction: Defining Cybersecurity in the EU Context

"European security policy is changing in fundamental ways. The old threat scenario involving tank divisions from the East has been replaced by the challenge posed by invisible adversaries whose geographical source can often not be determined. Virtual attacks threatening critical infrastructure, government institutions and personal data form one of the key challenges to security policy in the 21st century."[1] These words by Bendiek underline the need for the European Union to adapt its security strategy to new threats. 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,[2] 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.[3]

At the same time, cybersecurity triggers the emergence of a new field of research in European law and policy (and perhaps also in European Studies more generally[4]). Whereas 'law & technology' in

[1] A. Bendiek, *European Cyber Security Policy*, SWP Research Paper 13/2012 (Berlin: Stiftung Wissenschaft und Politik, October 2012), at 5.
[2] See for an overview R.A. Wessel and Joris Larik (eds), *EU External Relations Law: Text, Cases and Materials*, (Oxford: Hart Publishing, 2020), Chapter 12.
[3] See further on these initiatives: https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en
[4] Cf. H. Carrapico and A. Barrinha, 'European Union cyber security as an emerging research and policy field', *European Politics and Society*, Vol. 19, No. 3, 2018, pp. 299-303 (at 300): "Although cyber security has now become part of our daily lives and concerns, European Studies as a discipline is yet to fully embrace the area as a subject of in-depth research". See also R.S. Dewar, *Cyber Security in the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern*, PhD thesis University of Glasgow, 2017 (http://theses.gla.ac.uk/8188/).

general has become an established field of study,[5] EU law & technology and in particular 'EU cybersecurity law' still seems to be in its first infancy. As the present contribution will reveal, this is partly due to two distinct factors. First of all, cybersecurity can be seen as a cross-cutting policy area, which not only concerns by the Union's security policy, but also policies related to, *inter alia*, the internal market and the Area of Freedom, Security and Justice (AFSJ). This makes it difficult for specialists in any of these EU policy areas to provide comprehensive analyses and approach the topic as such. Secondly, despite the by now extensive number of policy documents, there is as yet not so much law for lawyers to analyse. Yet, a shift is visible: it is increasingly acknowledged that "Current literature on the regulation of cyberspace is no longer focused on whether cyberspace can be regulated. Instead, discussion focuses on how cyberspace is regulated and who are the regulators."[6]

Cybersecurity is not mentioned as such in the EU Treaties as an area to be dealt with by the European Union. The perhaps most obvious policy area to have mentioned cybersecurity, CSDP, largely developed (and intentionally so) as military and civilian cooperation to be used for "missions outside the Union for peace-keeping, conflict prevention and strengthening international security […]" as stated in Article 42(1) TEU. Also the more specific list of tasks in Article 43(1) TEU does not include a reference to cybersecurity.[7] The same holds true for the Treaty provisions on the internal market and on the AFSJ, which are equally silent on cybersecurity.

Nevertheless, after a number of earlier policy initiatives in cybersecurity,[8] cybersecurity is high on the EU's agenda in particular with the adoption of the 2013 Cybersecurity Strategy (updated in 2017[9]) and the 2015 Council conclusions on cyber-diplomacy.[10] It has been argued 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."[11] The reasons are obvious: over the past years the number of cyber-attacks on states and critical infrastructure have been constantly growing,[12] and by its nature cyber

---

[5] See for the many dimensions for instance the comprehensive overview by R. Brownsword, E. Scotford and K. Young, *The Oxford Handbook of Law, Regulation, and Technology*, Oxford University Press, 2017; as well as Chapter 44 in that book by D.S. Wall, 'Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing', pp. 1075-1096.

[6] L.Y.C. Chang and P. Grabosky, 'The Governance of Cyberspace' in P. Drahos (ed.), *Regulatory Theory: Foundations and Applications* (ANU Press, 2017), 533-552 at 535.

[7] Art. 43(1) TEU: "The tasks referred to in Article 42(1), in the course of which the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories.".

[8] 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. For a reference to some earlier documents, see also R.A. Wessel, 'Towards EU Cybersecurity Law: Regulating a New Policy Field', in N. Tsagourias and R. Buchan (Eds.), *Research Handbook on International Law and Cyber Space* (Cheltenham/Northhampton: Edward Elgar Publishing, 2015), pp. 403-425. Parts of the present contribution further build on that publication.

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

[10] 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.

[11] Carrapico and Barrinha, 'European Union cyber security'.

[12] A. Bendiek, *European Cyber Security Policy*; as well as J. Odermatt, 'The European Union as a Cybersecurity Actor', in S. Blockmans and P. Koutrakos (Eds.), *Research Handbook on EU Common Foreign and Security Policy* (Cheltenham/Northhampton: Edward Elgar Publishing, 2018; forthcoming). See earlier also the report by N. Robinson et al., *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*, Brussels: European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy, Sep. 2013; J. Argomaniz, 'The European Union Policies on the Protection of

security needs cross-border cooperation.[13] The EU measures aim to build resilience, fight cybercrime, build cyberdefence, develop industrial and technical resources and elaborate a diplomatic strategy for cyberspace.[14] Indeed, 'resilience' is a key-word in the EU's 2016 Global Strategy,[15] and this strategy seems far more aimed at responding to threats than at promoting values and transformation of its surroundings, which were the focus of the 2013 Security Strategy. Cybersecurity is now presented as a key-element in the EU's security and resilience policies.[16]

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 further below).[17] This piecemeal approach has made it difficult to understand what exactly is covered by cybersecurity and, on that basis, to allocate tasks and responsibilities.[18] The definition of cybersecurity that was included in the 2013 Cybersecurity Strategy of the European Union (EUCSS) has a broad scope:[19]

> *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 more narrow definition was provided by the special agency of the EU in this area, ENISA (European Union Agency for Network and Information Security):[20]

> […] the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment.

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

Infrastructure from Terrorist Attacks: A Critical Assessment', *Intelligence and Security*, 2013; P. Cornish, 'Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks', Brussels, European Parliament / Policy Department External Policies, 2009.

[13] Cf. the remarks by the European Commission 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.

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

[15] 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

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

[17] Cf. also Wessel, 'Towards EU Cybersecurity Law' at 425.

[18] Cf. Odermatt, 'The European Union as a Cybersecurity Actor'; as well as K.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 F. Di Camillo and V. Miranda, 'Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward', Working Paper No. 11, IAI 26 September 2011.

[19] 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').

[20] U. Helmbrecht, S. Purser, and M. Ritter Klejnstrup, *Cyber Security: Future Challenges and Opportunities* (ENISA 2012) 13.

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.[21] 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.[22] 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.[23] Given the Union's activities under the heading of 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.[24] Nevertheless, over the past few years in particular, the EU has taken policy initiatives to include cyberthreats in its CSDP (see further below).

2. EU Objectives and Ambitions in 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'.[25] 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:[26] "The Strategy

---

[21] See for a discussion on definitional questions also E. Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, 2014, pp. 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).

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

[23] Cf. A. Bendiek and A.L. Porter, 'European Cyber Security Policy within a Global Multistakeholder Structure', *European Foreign Affairs Review*, 2013, no. 2, pp. 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.

[24] G. 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."

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

[26] 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."

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."[27] Yet, the idea of autonomy should not be read as to isolate the EU; "Together with its partners, the EU will [also] promote resilience in its surrounding regions".[28] And, this is done in cooperation with international partners. Thus, in 2014, for instance, EU Members were asked to check their cyber-defence capabilities also in the context of the Atlantic cooperation.[29] 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.[30] 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.[31]

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."[32]

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.[33]

More concrete ambitions can be found in the 2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,[34] that addresses different dimensions of cybersecurity, including network and information security (NIS), cybercrime, and cyberdefence. The starting point is the following: "For cyberspace to remain open and free, the same norms, principles and values that the

[27] EU Global Strategy, at 4.
[28] EU Global Strategy, at 23.
[29] EU Council, *EU Cyber Defence Policy Framework*, 15585/14 (Brussels, 18 November 2014), https://ccdcoe.org/sites/default/ files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf . See further also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18.
[30] Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18; and B. Lété and D. Dege, *NATO Cybersecurity: A Roadmap to Resilience*, Policy Brief 3, 2017 (Washington: The German Marshall Fund of the United States, July 2017).
[31] T. 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).
[32] Global Strategy, at 21-22; emphasis added.
[33] Cf. also Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy', at 18.
[34] See above.

EU upholds offline, should also apply online".[35] 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[36] – and in the framework of the EU-US Working Group on Cyber-Security and Cyber-Crime (WGCC).[37] Part of the Cybersecurity Strategy is related to linking core EU values that exist in the 'physical world' to the '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."[38] 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 28 Member States to take the necessary measures, however, risks fragmentation (see further below). Primarily to overcome this risk, the 2015 European Agenda on Security (EAS) was adopted, as "an effective and coordinated response at European level",[39] providing a strategic framework for EU initiatives in the field of cybersecurity for the period 2015- 2020. Specific policies in relation to CSDP had already been formulated in the 2014 EU Cyber Defence Policy Framework,[40] 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.

Most recently, the Commission laid down the EU ambitions in a comprehensive 'cybersecurity package': *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.[41] This policy document 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

---

[35] EU Cybersecurity Strategy, at 1.

[36] *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).

[37] EU-U.S. Summit 20 November 2010, Lisbon - Joint Statement, European Commission - MEMO/10/597 20/11/2010. See also M. Grazie Porcedda, 'Transatlantic Approaches to cyber-security and cybercrime', in P. 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'.

[38] 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).

[39] 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.

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

[41] 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.

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.[42] 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."[43] This is not to say that the Union is completely passive in its external relations with regard to cybersecurity initiatives. The EU recently adopted a framework for a joint EU diplomatic response to malicious cyber activities (the so-called 'cyber diplomacy toolbox'), which sets out the measures under the broader Common Foreign and Security Policy (CFSP), including restrictive measures which can be used to strengthen the EU's response to activities that harm its political, security and economic interests.[44] 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".[45] The question, however, remains, to what extent the EU has the competence to realise all these 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."[46]

Irrespective of this statement by the Commission, the question is whether also in a legal sense, too, the EU is "well placed" to address cybersecurity.[47] Given the inherent cross-border nature of cybersecurity, the complete absence of the issue in the EU treaties is striking. 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

[42] 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).
[43] Odermatt, 'The European Union as a Cybersecurity Actor'.
[44] 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.
[45] See A. Bendiek, 'The EU as a Force for Peace in International Cyber Diplomacy', *SWP Comment*, No. 19, April 2018.
[46] 2017 Joint Communication to the European Parliament and the Council.
[47] 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 F.C. Mayer, 'Europe and the Internet: The Old World and the New Medium', *European Journal of International Law*, 2000, pp. 149-169. According to the European Commission, the EU's regulatory role has evolved over the years, to keep pace with the evolving ICT landscape: introducing rules covering all electronic communications networks and services ensuring fair access to basic services (phone, fax, internet, free emergency calls) at affordable prices, for all customers - including people with disabilities stimulating competition by reducing the dominant position that former national telecom monopolies used to maintained for certain services, like high-speed internet access. The rules are applied independently by the authorities in each EU country, with national regulators coordinating their policies at EU level through forums like the Body of European Regulators for Electronic Communications (BEREC). See for a summary: http://europa.eu/pol/infso/index_en.htm. See on the role of the EU in Internet governance also Communication from the Commission to the European Parliament and the Council of 18 June 2009 - *Internet governance: the next steps* (COM(2009) 277 final); as well as the overview of activities by the Commission on http://europa.eu/legislation_summaries/information_society/internet/index_en.htm. See also C.T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge: Cambridge University Press, 2011.

of the larger, global scope of the challenge and the involvement of multiple actors.[48] Indeed, initiatives such as the *Tallinn Manual on International Law Applicable to Cyber Warfare* reveal the struggle to formulate rules on 'non-physical' phenomenal in a state structure based on national jurisdictions.[49]

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. And in the absence of express powers, they will need to be found in relation to other policy sectors.[50] In 2016, this was also emphasised by the European Parliament:

"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."[51]

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. The fact that external competences often depend on the existence (and/or use) of internal competences,[52] has indeed limited the Union's legal powers as a global actor in this field.[53]

---

[48] Cf. J. Kleijssen and P. Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', *Netherlands Yearbook of International Law*, 2016, pp. 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'.

[49] See on some theoretical discussions L.J.M. Boer, 'Spoofed Presence Does not Suffice': On Territoriality in the Tallinn Manual', *Netherlands Yearbook of International Law*, 2016, pp. 131-145. Cf. also Cf. J. Zekoll, 'Jurisdiction in Cyberspace', in G. Handl, J. Zekoll and P. Zumbansen, *Beyond Territoriality – Transnational Legal Authority in an Age of Globalization* (Leiden/Boston: Martinus Nijhoff Publishers, 2012), pp. 341-369; U. Kohl, 'Jurisdiction in Cyberspace', in Tsagourias and Buchan, *International Law and Cyberspace*, pp. 30-54; A.A. Cottim, 'Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of The COE Convention on Cybercrime', *European Journal of Legal Studies*, 2010, pp. 55-79.

[50] 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.

[51] 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

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

[53] 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"

In an institutional sense, a number of initiatives have been taken to create specialised bodies, but again in specific fields only.[54] Thus, a special EU Cybercrime Centre was established in 2012.[55] This centre – named 'EC3' – is located at one of the EU's agencies, Europol in The Hague.[56] 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. 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 the European Union Agency for Cybersecurity (ENISA).[57] This latter agency also works to improve cooperation between Member States to implement emergency response plans, conduct regular emergency drills, and develop a European Information Sharing and Alert System (EISAS) to guard against attacks on critical infrastructure.[58]

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.[59] The following sub-sections will provide some examples of legal bases used to tackle different dimensions of cybersecurity.

3.1 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'. 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.[60] 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.[61]

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

---

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

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

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

[57] Regulation (EC) No 460/2004.

[58] http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder.

[59] See also Wessel, 'Towards EU Cybersecurity Law'.

[60] 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.

[61] 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'), *Official Journal* L 178, 17.7.2000.

market. A concrete example is formed by using Article 114 TFEU, which formed the basis for the Directive on Security of Network and Information Systems ('NIS Directive').[62] 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, but it has become clear already that this deadline was not met by most Member States.[63] 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",[64] 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."[65]

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.[66] 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.[67]

Enhancing trust in the internal market is also pursued by the 2014 Regulation on electronic identification and trust services for electronic transactions in the EU internal market.[68] 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[69] lists a large number of contributing threats

---

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

[63] See 'EU countries miss cybersecurity deadline', EU Observer, 30 July 2018; https://euobserver.com/digital/142493

[64] 'NIS Directive', Explanatory memorandum.

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

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

[67] 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.

[68] 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.

[69] 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

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."

3.2 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.[70] 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').[71] 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:

"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.[72] It also provides minimum rules on the definitions of crimes included in the Directive.

Earlier 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,[73] and the 2001 Framework Decision on combating fraud and counterfeiting.[74]

Digital Single Market Strategy, *A Connected Digital Single Market for All*, Brussels, 10.5.2017, COM(2017) 228 final.

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

[71] See above.

[72] 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.

[73] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337, 18.12.2009, 11.

[74] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OJ L 149, 2.6.2001, 1.

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),[75]although it participates in the Cybercrime Convention Committee (T-CY).

3.3 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",[76] despite the claim that "the next war will begin in cyberspace".[77]

The above-mentioned Cybersecurity Strategy also mentions one particular field of cooperation related to the so-called 'solidarity clause' laid down in Article 222 TFEU.[78] On the basis of that provision

> "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, cybersecurity is not mentioned explicitly. Yet, it easily fits 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 […]".[79] In fact, the EP even went a step further and also mentioned cyberattacks 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 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 […]".[80] While in the case of the solidarity clause it may be

---

[75] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Cf. also M. Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law & Policy*, 2002-2003, p. 287-327.

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

[77] 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', *International Affairs*, 2010, pp. 523–541.

[78] See for instance Y. Bogmann-Prebil and M. Ross (Eds.), *Promoting Solidarity in the European Union*, Oxford: Oxford University Press, 2010.

[79] 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.

[80] Ibid, at par. 13.

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.[81] 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 relatively slow acknowledgement of the need to regulate cyberspace is not related only to the absence of 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."[82] Yet, "this 'first generation thinking' […] proved to be a fallacy"[83] and both the EU and its Member States realised that "if information flows freely, it is because we allow it to do so."[84] As we have seen, the regulation of cybersecurity is high on the EU agenda.

Over the years, the European Union has put great efforts in formulating ambitious cybersecurity policies. While this has resulted in an impressive pile of policy papers produced by the various EU institutions (the Commission in particular), clear legal competences to actually regulate the field are 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."[85] 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."[86] This also led to path dependencies and made it more difficult to connect to newer policy areas (perhaps such as CSDP). At the same time, cyberdefence is now emerging as a key issue and the EU is clearly attempting to mainstream cyber issues throughout its exiting foreign and security policy. One reason is that it is increasingly difficult to separate internal and external threats in this field: "Not only may Internet-based attacks on critical infrastructure originate in Ghana, Russia or elsewhere, but also often it is difficult (if not impossible) to identify the source of the attack. […] An appropriate response to such an attack requires cross-border cooperation between authorities. It is here that the current division of responsibilities between civil defence, military defence, and law enforcement falters".[87]

---

[81] See for examples of cyber attacks A. Klimburg and H.Tirmaa-Klaar, *Cyber Security and Cyber Power: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, study commissioned by the European Parliament, PE 433 828, 54 (Brussels 2011). See also M. Roscini, 'Cyber operations as a Use of Force' in Tsagourias and Buchan, *International Law and Cyberspace*, pp. 233-254; and C. Focarelli, 'Sef-Defence in Cyberspace', in Tsagourias and Buchan, *International Law and Cyberspace*, pp. 255- 283.
[82] Zekoll, 'Jurisdiction in Cyberspace', at 342-343.
[83] Ibid. at 343.
[84] H. Muir Watt, 'Yahoo! Cyberspace-Collision of Cultures: Who Regulates', *Michigan Journal of International Law*, 2003, p. 673, at 683. Also quoted in Zekoll, 'Jurisdiction in Cyberspace', at 344.
[85] Odermatt, 'The European Union as a Cybersecurity Actor'.
[86] Dewar, *Cyber Security in the European Union*, at 212.
[87] Bendiek and Porter, 'European Cyber Security Policy', at 156-157.

This chapter points to the need for a comprehensive regulatory approach. However, whereas the EU is usually able to find a connection to existing competences, allowing it to produce new legislation in many different fields, it suffers from the fact that it is not always easy (and sometimes even impossible) to combine the different cybersecurity dimensions in consistent or even connected policies. Despite the fact that the Lisbon Treaty integrated many policy fields by making an end to some diverging decision-making procedures, 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). It is the EU's complex division of powers and its diverging procedures and rules for different policy areas that seem to stand in the way of realising a comprehensive body of cybersecurity law, leaving us with a large number of partly overlapping, soft as well as hard law measures in a complex multi-actor and multi-level setting.

The current treaty regime only partly allows the EU to improve things. Despite the fact that foreign and security measures are no longer 'subordinate' to other policies (which is underlined both by Treaty provisions and recent case law[88]), a choice for the correct legal basis will still have to be made and combinations of CFSP and other policies remain difficult because of the different (and often incompatible) procedural requirements. Obviously, this is not always a problem. The EU can simply adopt different decisions related to the internal market, crime or defence issues. But 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.[89] Yet, there is no denying of the fact that something like a body of EU cybersecurity law is slowly developing. Alongside the existing decisions, the EU has announced new legislative initiatives, partly following international (transatlantic) cooperation, partly because of a connection to internal objectives related to either fundamental rights or economic motives. The fact that many options are still open will allow the EU to take its own consistency requirements seriously and aim for a comprehensive and coherent development of this new body of law. There should be no doubt that the coming years these developments will lead to the emergence of new sub-disciplines in the area of EU cybersecurity law.

[88] See also S. Blockmans and M. Spernbauer, 'Legal Obstacles to Comprehensive EU External Security Action' (2013) 18(4) *European Foreign Affairs Review*, 7-24 at 23.

[89] See also H. Carrapico and A. Barrinha, 'The EU as a Coherent (Cyber)Security Actor?', *JCMS*, 2017 Volume 55. Number 6. pp. 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."