FACULTY OF LAW
UNIVERSITY OF COPENHAGEN

iCourts Working Paper Series, No. 124, 2018

The European Union as a Cybersecurity Actor

Forthcoming in *Research Handbook on EU Common Foreign and Security Policy. ed. / Steven Blockmans; Panos Koutrakos. Cheltenham/Northhampton: Edward Elgar Publishing* (2018)

Jed Odermatt

iCourts - The Danish National Research Foundation's
Centre of Excellence for International Courts

March 2018

Abstract:

The working paper discusses the challenges facing the European Union as it seeks to become a more active player in the field of cybersecurity. It outlines the concept of cybersecurity and the various approaches to cybersecurity governance. It then discusses the EU's approach to cybersecurity issues, focusing on three elements: cybercrime, network and information security, and cyber-defence. Although a relative newcomer on the scene, the EU has made strides towards establishing a coherent policy framework across these areas. The EU is also developing a role in cyber defence, a field that has been largely left to the Member States. It finally analyses the external dimension of cybersecurity policy, and argues that the EU can influence the development of international norms. EU policy must also deal with the political and diplomatic dimension, especially as threats of state-sponsored cyber attacks increase.
KEYWORDS: Cybersecurity, European Union, Common Foreign and Security Policy, Cybercrime, Network and Information Security

Jed Odermatt, Postdoctoral Research Fellow, Centre of Excellence for International Courts, University of Copenhagen.

E-mail: jed.odermatt@jur.ku.dk

This research is funded by the Danish National Research Foundation Grant no. DNRF105.

iCourts - Centre of Excellence for International Courts - focuses on the ever-growing role of international courts, their place in a globalizing legal order, and their impact on politics and society at large. To understand these crucial and contemporary interplays of law, politics, and society, iCourts hosts a set of deeply integrated interdisciplinary research projects on the causes and consequences of the proliferation of international courts.

iCourts opened in March 2012. The centre is funded by a large grant from the Danish National Research Foundation (for the period 2012-22).

The European Union as a Cybersecurity Actor

Jed Odermatt, Postdoctoral Research Fellow, Centre of Excellence for International Courts, University of Copenhagen.

Introduction

Cyber-attacks have become more common, and have received a great deal of attention in recent years. In January 2017, the US intelligence community stated that it was confident that groups associated with the Russian government were responsible for the hacking of the Democratic National Committee (DNC) and sought to interfere directly with the US elections.[1] Incidents have also exposed the vulnerability to cyber-attacks in the EU. Germany's intelligence agency stated that groups associated with Russia were responsible for infiltrating the computer network of the German Parliament.[2] In May 2017, the head of Germany's domestic intelligence agency accused Russia of being behind cyber-attacks intended to influence the German election, and suggested the possibility of 'wiping out' Russian servers if the owners do not ensure they are not to be used for attacks.[3] The campaign team of French Presidential candidate Emmanuel Macron accused Russia of being responsible for a coordinated hacking operation intended to influence the Presidential election.[4] The EU institutions have also been a target and there has been a reported rise in the number of cyber-attacks on EU servers, including those of the European Commission.[5] The WannaCry and Petya ransomware cyberattacks (malicious software that threatens to block access to data unless a ransom is paid) affected business in the EU and the rest of the world. Such attacks are not only becoming more common but also more sophisticated. While such high-profile incidents make international headlines, there are other less visible cyber threats that also require a legal and policy response. Various forms of cybercrime, phishing, online fraud, and other criminal activity, not only cause economic damage in the EU, but can also undermine confidence in the internet and digital commerce. The list of such incidents will continue to expand.

EU citizens, businesses and governments all benefit from the interconnected digital world provided for by the internet, yet there is a growing awareness of the threats that such interconnectedness brings. In the field of cybersecurity, the European Union (EU) is a relative newcomer on the scene. While it has for a long time been involved in areas of internet governance and regulation,[6] on cybersecurity issues the Union has been more reactive to events and developments, and is still in the process of developing a coherent cybersecurity policy. As the challenges of cybersecurity becomes more prominent, the EU and the Member States have sought to catch up by strengthening resilience to threats emanating from cyberspace. This chapter examines those steps and assesses the extent to which the Union has become an effective cybersecurity actor. While the EU has made steps in addressing cybercrime and improving the resilience of communication and information systems,

[1] Intelligence Community Assessment, 'Assessing Russian Activities and Intentions in Recent US Elections, 6 January 2017. Available at <https://www.dni.gov/files/documents/ICA_2017_01.pdf>

[2] 'After a Cyberattack, Germany Fears Election Disruption' *The New York Times*, 8 December 2016.

[3] 'Germany Challenges Russia Over Alleged Cyberattacks' *Reuters*, 4 May 2017.

[4] 'Hackers Hit Macron Campaign with 'Massive' Attack' *Financial Times*, 6 May 2017 < https://www.ft.com/content/79341cc4-3233-11e7-bce4-9023f8c0fd2e?mhq5j=e1>.

[5] 'EU suffers jump in aggressive cyber attacks' *Financial Times*, 8 January, 2017. <https://www.ft.com/content/3a0f0640-d585-11e6-944b-e7eb37a6aa8e>

[6] Franz C. Mayer, 'Europe and the Internet: The Old World and the New Medium' (2000) 11(1) *EJIL* 149.

the EU is only beginning to develop a role in cyber defence, a field that has been largely left to the Member States. In line with the theme and aims of this Handbook, the present chapter will focus on the international security dimension.

The chapter begins by briefly discussing the challenges facing the EU in the field of cybersecurity. Part 1 discusses the concept of 'cybersecurity' and discusses why greater conceptual clarity is needed in order for the EU seeks to develop a more coherent approach. It then discusses the EU's general approach to cybersecurity issues, which is to separate the issue into different elements: cybercrime, network and information security, and cyber-defence. Such an approach is grounded partly in legal reasons. Without an explicit competence in the cybersecurity domain, the EU has had to find a connection with existing EU competences. Where the Union has not been able to connect cybersecurity issues with an existing EU competence, it has pursued more soft law measures to influence Member States and other actors.[7] Part 2 provides a brief overview of EU policy in the field of cybercrime, the field where the EU has been most active. Part 3 turns discusses the second pillar of the EU's approach is in the field of Network and Information Security (NIS). Part 4 discusses the EU as an emerging actor in the field of cyber defence, and outlines both the challenges and potential opportunities of establishing a comprehensive cyber defence policy. Part 5 discusses the external dimension of cybersecurity policy. Due to the global nature of the threats involved, the approach of the EU and its Member States must be developed within a global context, including other States and key international organizations and bodies. The EU acknowledges that building cyber resilience requires more than developing its own internal policies, and that it should also work at the international level to influence developments. It is in this field that the EU has the potential to develop into an international actor in the field of cyber security.

1. Cybersecurity Challenges in the EU

1.1. Defining Cyber security terms

Legal and policy documents related to cybersecurity often begin with a conceptual discussion about what exactly 'cybersecurity' means.[8] The term remains somewhat ambiguous and ill-defined, in part because of the constantly evolving nature of the threats involved.[9] Moreover, cybersecurity is often used as an umbrella term to refer to a number of different types of threats, including cybercrime, cyber espionage, cyber-attacks, cyber warfare, and cyber terrorism. There does not appear to be any coherent understanding within the EU about what cybersecurity entails.[10] In addition, there is no common definition for cyber terms used in the EU

[7] Ramses A. Wessel, 'Towards EU cybersecurity law: Regulating a new policy field' in N Tsagourias and R Buchan (eds) Research Handbook on International Law and Cyberspace (Cheltenham, Edward Elgar, 2015) 425: "While 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."

[8] Paul Cornish, Rex Hughes and David Livingstone, 'Cyberspace and the National Security of the United Kingdom Threats and Responses' Chatham House, March 2009, 1: "Cybersecurity (security in and from cyberspace) is widely regarded as an urgent and high-level problem which cannot be ignored. But the precise nature of this problem is not well defined." See Daniel T. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds), *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, 2009).

[9] See Federica Di Camillo and Valérie Miranda, 'Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward', IAI Working Papers No. 11, 26 September 2011.

[10] Krzysztof 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-

context.[11] Key terms such as 'cyberspace', 'cyber attack', 'critical infrastructure' do not have a common definition in the EU Member States, most of which have their own national strategies.[12] Without such clearly defined terms, however, it may be difficult to set boundaries as to who is responsible for different issues, especially given that cybersecurity entails a number of different state and non-state actors. The lack of a clearly defined taxonomy may also make it difficult for the EU and Member States to develop a coherent framework. This affects not only the EU's internal policy making, but also affect's the EU's ability to influence developments at the international level.

One of the key EU documents in this field is the 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* ('EUCSS')[13] which was jointly adopted by the High Representative of the Union for Foreign Affairs and Security Policy (HRVP) and the European Commission (discussed in Part 1.4.) The EUCSS provides a very broad definition of cybersecurity:

> '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.'[14]

This definition includes actions to protect the 'cyber domain', in both civilian and military fields. The benefit of such a wide-ranging definition is that it allows for policies that cut across different domains and can be applied to new cyber threats as they emerge and evolve. Nonetheless, EU policy tends to divide cybersecurity into two main elements: the security of network and information systems and cybercrime. The former refers to the ability of electronic communications systems and digital data to resist action that may compromise data stored on or transmitted via those systems.[15] Cybercrime, on the other hand, refers to the use of electronic communication networks to commit criminal acts online.

The European Union Agency for Network and Information Security (ENISA), the agency established to improve network and information security in the EU, distinguishes cyber security from other terms such as cybercrime, cyber espionage and cyber warfare. It adopts a narrower definition of cyber security that focuses on " ... 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."[16] This relates to ensuring the resilience of networks to potential attacks and the capacity to respond to such attacks.

---

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."

[11] Di Camillo and Valérie Miranda (n 9).

[12] For a list of definitions of 'cyber terms' in national strategies and other documents, see NATO Cooperative Cyber Defence Centre of Excellence, Cybe definitions. <https://ccdcoe.org/cyber-definitions.html>.

[13] 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').

[14] EUCSS (n 13) 3.

[15] The precise legal definitions of 'network and information system' and 'security of network and information systems' are found in Article 4 of the 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').

[16] Udo Helmbrecht, Steve Purser, and Maj Ritter Klejnstrup, *Cyber Security: Future Challenges and Opportunities* (Heraklion: ENISA, 2012) 13.

The EUCSS and other policy documents provide a separate definition for cybercrime, which entails:

> '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).'[17]

This is also a wide definition. It includes, not only crimes that are unique to electronic networks, such as cyber-attacks, but also the use of information systems to pursue crimes such as fraud, or the publication of illegal content, or even online fundraising and recruitment for terrorism (including 'cyber terrorism'). While the EUCSS has put forward this definition of cybercrime, there is still no common understanding in the EU, and Member States continue to have their own approaches. Moreover, since cybercrime involves such a wide range of different acts, it has been debated whether there needs to be a single definition.[18]

The last pillar of EU policy – cyber defence – also lacks common definitions of key terms in the EU context, one reason being that this remains a key competence of the EU Member States.[19] The cyber threats in the other two categories mainly involve illegal activity for private material gain, and as such are viewed as matters relating to criminal justice. Cyber defence, on the other hand, relates to actions targeted at states, often for a political motive, and is therefore viewed as a national security issue. It is not always easy to make this distinction in practice. For example, the NotPetya cyberattacks of June 2017 first appeared to be a ransomware for private gain. |Yet some security experts have pointed out that it was possibly a destructive malware disguised as ransomware, with the support or approval of a state actor, with the intention of causing damage in Ukraine and other businesses in Europe.[20] This demonstrates how difficult it can be to distinguish elements of cybercrime and cyberwarfare. Cyber attacks have been carried out by state or non-state actors and can involve a mix of private and political motives. It is difficult to distinguish which elements belong to the realm of criminal law and which are matters of national security, each of which carry their own set of responses. Conceptual debates about the boundaries between cybercrime, cyber war, and so on, continue to pervade this field. [21]

One might question whether such conceptual debates really matter. Yet without a clear definition of cybersecurity and its key terms, it is difficult for the EU to establish a comprehensive vision. States each have their own cyber security strategy documents, each containing their own terminology.[22] Definitions also matter

---

[17] EUCSS (n 13) 3.

[18] International Telecommunications Union, Understanding Cybercrime: A Guide for Developing Countries, (2009) 18. "The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term." http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[19] 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."

[20] NotPetya and WannaCry Call for a Joint Response from International Community, NATO Cooperative Cyber Defence Centre of Excellence, 30 June 2017, <https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html>. "Petya' ransomware attack: what is it and how can it be stopped?' *The Guardian*, 28 June 2017 <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>.

[21] Jukka Ruohonen, Sami Hyrynsalmi, Ville Leppänen, 'An Outlook on the Institutional Evolution of the European Union Cyber Security Aapparatus', (2016) 33 *Government Information Quarterly* 746.

[22] For a list of national documents, see NATO Cooperative Cyber Defence Centre of Excellence, Cyber Security Strategy Documents <https://ccdcoe.org/cyber-security-strategy-documents.html>.

because they relate to the different approaches, conceptions and responses to these threats. For example, it is unclear when a cyber-attack may give rise to diplomatic and military responses, and when should it be dealt with as a matter of domestic criminal law. There are also new forms of cyber warfare that may not fit into a neat category, such as the deliberate use of misinformation to destablise politics in a country.[23] Conceptual difficulties may also make it difficult to determine which bodies are responsible in a given situation. Due to the high number of actors involved – national authorities, EU bodies, businesses, civil society, international organizations – the use of different terminology used can also undermine cooperation and coordination. The development of a common understanding of cybersecurity and its key terms at the EU level would not only strengthen resilience and responses to cyber threats within the EU, it could also help the EU to push forward with this taxonomy at the global level.

1.2. Governance Challenges: The Nature of Cyberspace and Cyber Security

The nature of cyberspace and threats emanating from this sphere raise some unique challenges. By their very nature, cybercrime and cyber-attacks are a cross-border phenomenon, and purely national or regional approaches are unlikely to be effective. This not only means that cooperation should take place between EU Member States, but that the EU and the Member States must also work at the international level to forge partnerships and cooperation. Another challenge is that there is no central actor or body responsible for taking the lead in the area of cybersecurity. This means that policy has been developed by different actors, each of which have different goals and rationales, both at the EU and Member State level. In addition, any approach must involve both state and non-state actors, including private industry and technology firms (internet security companies, services providers, firms that own and manage hardware, software and infrastructure) as well as civil society. Given the number of actors involved, cyber security issues cannot be addressed purely through a 'top-down' strategy that is based on the logic of governmental control. The approach within the EU has been involve these different actors, and to indirectly influence developments and give incentives for co-operation.

This also reflects the fact that there is wide disagreement about the propose place of governments regional organizations, private industry should play in cybersecurity. EU governance in this field has pursued a 'multi-stakeholder' approach,[24] which acknowledges the need to involve bodies such as national governments, internet providers, technology and security firms, businesses, and civil society. The EUCSS endorses this multi-stakeholder approach.[25] This contrasts with the more state-centric or top down approach pursed by states such as China and Russia. The multi-stakeholder approach encourages cooperation and information sharing between different bodies, and is arguably more suited to cybersecurity given its global and decentralized nature, and the fact that non-governmental private bodies are responsible for the management of internet resources. This form of governance is also more suited to the EU, which is able to deal with multiple stakeholders, encourage cooperation, and develop standards and good practices. The EU's response, therefore, has focused less on legislation, and more on strengthening institutions and agencies, promoting joint initiatives and improving coordination. National governments, NIS authorities, law enforcement bodies, as well as the private sector will continue to be involved in preventing and responding to cyber threats, and the EU will not become a central supervisory body. Nonetheless, EU action helps to coordinate Member States and these other bodies and to link these efforts to the international level.

[23] See 'Britain says Russia is trying to undermine West by 'weaponizing misinformation', Reuters, 3 February 2017.
[24] Annegret Bendiek & Andrew L. Porter, 'European Cyber Security Policy within a Global Multistakeholder Structure' (2013) 2 *European Foreign Affairs Review* 155, 175.
[25] EUCSS (n 13) 4.

1.3. An EU approach to Cybersecurity?

As a relatively new actor in cybersecurity, the EU still lacks a comprehensive vision.[26] Yet a number of important steps have been made towards establishing such a coherent approach at the EU level. The EU Global Strategy sets out that a renewed focus on cybersecurity by the EU "requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation."[27] This is a real challenge, especially given that those policy areas straddle issues related to the internal market, criminal law, international diplomacy and defence.

Cybersecurity is not mentioned as a policy field in the EU Treaties, and there is no explicit legal basis for EU policy in this area. This has meant that, due to the principle of conferral in EU law, EU policies have had to be linked to existing EU competences. The EU has relied for the most part on the economic rationale for such action, arguing for instance that cyber attacks have an economic effect in the Union. Policies at the EU level are geared towards the functioning of the internal market. For example, the NIS Directive finds its legal basis in Article 114 TFEU, under which 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'. Because network and information systems play such a key role in the cross-border movement of goods, people and services, the disruption of networks in one Member State can have wider effects on other Member States and the EU, and can therefore consist of a barrier to the internal market.[28] The Directive on combating the sexual exploitation of children online and child pornography,[29] finds its legal basis in Articles 82(2) and 83(1) TFEU, referring to judicial cooperation in criminal matters in the Union. In the field of cybercrime and increasing critical infrastructure resilience there is a legal basis for such legislative efforts, which are aimed mostly at achieving common approaches in the EU Member States. There have been fewer developments in terms of cyber defence policy.[30] A further challenge is to link these internal legislative developments with the external aspects of EU policy.[31]

Although the EU must link its actions in cybersecurity with existing competences, this does not mean that a common approach to cybersecurity issues cannot emerge across those different domains. The EUCSS and other policy documents set out some of the key priorities for action in this field. For example, for the EU, any policy must respect fundamental rights and values in the Union. The EU and the Member States are also committed to securing a global, open and secure internet. Measures designed to enhance cyber-resilience within the EU must be balanced with protecting individual rights, including privacy or freedom of speech. The EUCSS stresses not only that EU internal policies must respect fundamental rights, but that the EU's

[26] George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan, 2016) 102: "there is no overarching framework but rather a series of legal and regulatory instruments that overlap". Sliwinski (n 10) 469: "Many EU member states have their own cyber-security strategies and their own conceptualizations of cyber-security. The EU as a whole is not entirely clear on the notion."

[27] *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*, June 2016, 22.

[28] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union /* COM/2013/048 final - 2013/0027 (COD), Point 3.1.

[29] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[30] Sliwinski (n 10) 479.

[31] Wessel (n 7) 404.

engagement on cyber issues at the international level must respect EU core values of freedom, democracy, equality and the rule of law.[32]

1.4. 2013 Cybersecurity Strategy

One of the challenges of establishing a coherent vision is that EU action in this field is separated into different dimensions, each of which has a different rationale and logic, and is at a different stage of development. Presented in 2013 by the Commission and the EU High Representative, the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*[33] sought to overcome this issue, by providing a policy initiative that cuts across the various domains of cybercrime, NIS and cyber defence. The EUCSS is broad in scope, and sets out six main priority areas for the Union. The first of these is to achieve 'cyber resilience' through a range of legislative and non-legislative measures focused on enhancing private and public capacities. The second priority is to reduce cybercrime. The third priority relates to the development a cyber defence policy the framework of the CSDP. By addressing these different fields within the same document, the EU is pursuing a more comprehensive approach, for example, by bringing together areas including CFSP/CSDP that touch upon cyber related issues.[34] The fourth priority relates to the development of industrial and technical resources to prevent and deter cyber incidents. The fifth policy turns outwards, and relates to the development of an international cyberspace policy. This also illustrates how the EUCSS seeks to 'mainstream' cyber security policies across different domains, both in the EU's internal policies as well as in its external relations. The last priority is the promotion of core EU values, an issue which can help tie together the internal and external aspects of cybersecurity policy. The EUCSS is highly ambitious, and in the years since its adoption, the EU has made progress on all of these policies. Yet one of the main challenges for the EU will be to bring together national, regional and international bodies, as well as the many actors in the private sector, and to overcome the fragmentation of policies.

2. Cybercrime

Tackling cybercrime is the first pillar of EU cybersecurity strategy and it is in this field where the EU has made the most concrete developments. The EU has mostly used a legal approach to this issue, employing EU Directives and Regulations as a form of governance. However, cyber resilience requires more than a strictly legal approach, but also the fostering of a common culture of cybersecurity, creating trust to ensure data and information sharing, and bolstering the resources of the EU Member States. Along with EUCSS, the European Agenda on Security (EAS)[35] provides a strategic framework for EU initiatives in the field of cybersecurity. The EAS for the period 2015- 2020, adopted by the Commission in April 2015, prioritises terrorism, organised crime and cybercrime as areas with a cross-border dimension where EU action can make a difference.

The 2013 EU Directive on Attacks against Information Systems[36] ('Cybercrime Directive') establishes minimum rules on the definition of criminal offences and sanctions with respect to attacks against information systems and replaces the 2005 EU Framework Decision on Attacks against Information Systems. It also provides minimum rules on the definitions of crimes included in the Directive so as to allow a consistent

[32] EUCSS (n 13) 15.
[33] EUCSS (n 13).
[34] EUCSS (n 13) 11: "cyber security efforts in the EU also involve the cyber defence dimension."
[35] 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, 28.4.2015 COM(2015) 185 final.
[36] 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.

approach among the Member States. These include illegal access to information systems, illegal system interference, illegal data interference, and illegal interception. Given the evolving nature of cyber crime activities, the Directive seeks to address some of these newer threats, including botnet attacks, identity theft, and the role of organized crime. Other developments include the 2011 Directive on Combatting the Sexual Exploitation of Children Online and Child Pornography, the 2002 ePrivacy directive,[37] ensuring the confidentiality of client information and the 2001 Framework Decision on combating fraud and counterfeiting.[38]

The EU's strategy also involves the strengthening of, and cooperation between, institutions at the EU and Member State level. The European Cybercrime Centre (EC3) was officially launched in 2013. As a distinct body attached to Europol, EC3's role is to coordinate national cybercrime authorities and the training of national cybersecurity experts, and acts as a European focal point in fighting cybercrime. EC3 seeks to co-ordinate various national cyber-crime authorities and facilitate training of national cyber-security experts. Its aim is to harmonize legal and technical provisions dealing with issues such as data protection and privacy. Cybercrime is an area where the EU has made important developments. Although the Member States remain key actors in the field, efforts at the EU level have brought together public and private bodies, identified gaps in regulation, and strengthened capabilities to deter, investigate and prosecute cybercrime. Greater efforts should be now be made to link cybercrime with the other branches of EU policy, for example, by fostering greater coordination between national law enforcement with NIS authorities and defence.

3. Network and Information Security (NIS)

The second pillar of the EU's approach is in the field of Network and Information Security. Information security is an essential element of the modern digital economy, and efforts to strengthen NIS have been motivated chiefly by this economic rationale. The 2010 Digital Agenda for Europe, an initiative under the Europe 2020 Strategy, sets out trust and security online as one of its main pillars. The goal of having a coordinated European response to cyber-attacks and rules on personal data protection are linked to the wider objective of restoring trust in digital services, which is essential for the Digital Single Market.[39] Yet beyond this economic dimension, it is now understood that NIS also involves an international security dimension, especially where it is focused on preventing attacks against critical infrastructure.

The first EU legislative instrument designed to combat cyber threats was the Directive on Security of Network and Information Systems ('NIS Directive').[40] Adopted on 6 July 2016, the NIS Directive aims at setting a high common level of Network and Information Security across the EU by removing divergences between NIS legislation across different EU Member States. The Directive has three main aims: increasing capabilities of the Member States, increasing EU-wide cooperation, and risk management and reporting. The first objective requires 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). The second objective is

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

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

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

[40] 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').

to promote cooperation between the Member States. In terms of risk management and reporting, the NIS Directive sets out requirements for security and notification, according certain actors are to notify serious incidents to national authorities. This includes businesses with in important role in the economy, operators of essential services, and digital service providers. The NIS Directive lists certain critical sectors, including energy, health, transport and banking. In these areas, companies must ensure their ability to resist a cyber-attack.

The 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[41] suggests certain market-oriented policy measures to boost industrial capabilities in Europe. This includes a system for certification and labelling to achieve a functioning single market in cybersecurity, and further investment in the cybersecurity industry. In July 2016, the Commission launched a public-private partnership on cybersecurity to promote further investment in the industry but also to improve Europe's resilience to cyber attacks. The aim is to increase cyber resilience by stimulating a cybersecurity industry within the EU, promoting public-private partnership on cybersecurity, and overcoming obstacles to a single cybersecurity market.

In terms of institutions, the European Agency for Network and Information Security (ENISA) is the most advanced European body established for dealing with cybersecurity matters. ENISA is responsible for facilitating and coordinating the exchange of information, best practices and knowledge in the field of information security, and plays a key role in the implementation of the NIS Directive. It serves as access point or hub for EU Member States and other bodies. Working with states and other stakeholders, ENISA also serves to develop advice and recommendations on good practices in the field of information security, and assists Member States with their own national cyber-security strategies. The agency was first oriented towards research and training, but has in recent years evolved a more regulatory role. The ENISA Threat Landscape[42] details emerging trends and risks in cyber security, and contributes to the goal – outlined in the EUCSS – of streamlining and consolidating available information on cyber-threats.

The EU established its own permanent Computer Emergency Response Team (CERT-EU) in 2012. The CERT-EU plays an internal, technical role focused on the EU institutions. Comprised of IT security experts from the EU institutions, it cooperates with the CERTs in other Member States as well as the IT industry. The role of CERT-EU is mainly defensive, dealing with issues such as prevention, detection, response and recovery.

The EU has also made progress in the field of network and information security, but there remain steps to improve cyber resilience in Europe. On 10 May 2017, the Commission published its mid-term review of the Digital Single Market strategy [43] in which it outlines three areas where further action is required: developing the European Data Economy, promoting online platforms as responsible players, and tackling cybersecurity challenges. By September 2017, the Commission will review the EUCSS, and the mandate of ENISA to bring them into line with a wider EU framework on cybersecurity. In addition to further developing industrial

[41] 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.

[42] European Union Agency For Network and Information Security, ENISA Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends, January 2017.

[43] Communication 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, COM(2017) 228 final, Brussels, 10.5.2017.

capacity in the cyber security sector, the next steps will be to develop common standards of security, certification and labelling. It is clear that in this field the economic rationale remains predominant, which is understandable given the importance of cybersecurity in the modern digital economy as well as the clear legal basis for EU efforts. Yet it is becoming clear that cyber resilience also carries with it a security element, and that such efforts must also be coordinated with the other pillars of EU policy, including cyber defence.

4. Cyber Defence

4.1. The Challenges of Cyber Defence Policy

The European Commission Reflection Paper on the Future of European Defence,[44] which sets out three different options for moving towards a security and defence Union, illustrates the central importance of cyber defence. Under each of the three scenarios outlined in the paper – security and defence cooperation, shared security and defence and common defence and security – cyber defence is envisaged as an area of greater cooperation through support at the EU level, since cyber threats "straddle she internal-external policy divide".[45] As the EU steps up its defence cooperation, issues related to cyber defence will remain prominent. 'Cyber defence' policy falls for the most part falls within the CSDP and remains an area of national strategies. Despite the sensitivity over this area of national security, the EU Member States have begun to cooperate through the EU framework, and one of the strategic priorities set out in the EUCSS is to develop a cyber defence policy in the framework of the CSDP.

Whereas the EU has emerged as an actor in the fields of cybercrime and network and information security discussed above, cyber defence remains the least developed dimension. Along with sea, air, land and space, the 'cyber domain' is now viewed as the fifth domain of warfare. European states only began to treat the issue as an urgent and serious threat after the 2007 attacks on public and private institutions in Estonia. Conventional military operations and activity highly depend on the use of information technology and computer networks, and these increasingly involve civilian infrastructures. Various EU Member States have taken steps to develop their own military cyber defence capabilities, but there is no comprehensive EU approach to cyber defence. The EUCSS sets out the need for an EU cyber defence policy, stressing the need to "increase the resilience of the communication and information systems supporting Member States' defence and national security interests" by focusing on the detection, response and recovery from cyber threats.[46]. Member States seek to remain in charge of issues closely related to cyber defence, yet this is also a field where there is potential for much greater EU involvement. Like in the fields of cybercrime and network and information security, the EU is in a position to encourage greater information sharing between parties, to foster research and cooperation. The EU may also be in a position to respond to cyber-attacks, such as through a coordinated diplomatic response at the EU level.

The EU has not yet sought to develop any kind of hard or offensive cyber power. Rather, the EU's approach to cyber defence so far has been guided by the logic of protection. Rather than developing offensive cyber capabilities, the focus has been on ensuring the protection of conventional military activity. Moreover, since the EU does not possess its own military forces or equipment, it is reliant on the Member States to provide

[44] European Commission, European Commission Reflection Paper on the Future of European Defence, COM(2017) 315, 7 June 2017. < https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf>. P. 6: "Peace and security at home can no longer be taken for granted in a world in which global and regional powers rearm, terrorists strike at the heart of cities in Europe and around the world and cyberattacks escalate."
[45] Ibid. p. 12
[46] EUCSS (n 13) 11.

cyber defence for EU-led operations. EU Member States have different levels of protection, approaches, cultures, and technical knowledge. This creates challenges for the EU to take measures to protect equipment and communication and information networks used in the context of CSDP missions.

Another challenge is that it is difficult to identify which issues belong to Member States competences, and those where the EU can potentially play a role. The EU will likely pursue a similar governance model as in other fields of cybersecurity, emphasizing collaboration between Member States, sharing information, and supporting and developing training and education. A key role of the EU in this field is to facilitate cooperation and partnerships, to share information and resources, and avoid duplications. This not only includes fostering cooperation between EU Member States, but also greater civil-military cooperation. This is important since EU military operations depend highly on civilian actors and infrastructure militaries, and often depend on the very same technologies that are used in the private sphere. Cooperation also makes financial sense at a time when military budgets are under strain, and costs are rising. The pooling and sharing of military capabilities, including in the domain of cyber defence, can therefore have economic benefits.[47] However, cooperation in cyber defence, as with other areas of military matters, will take time and will require building trust between various actors. It has been suggested that the EU could learn from other areas of military cooperation, such as air logistics, to strengthen capabilities within the EU.[48]

The most important step in this field has been the adoption of the EU Cyber Defence Policy Framework ('CD Policy Framework') by the Council on 18 November 2014.[49] The CD Policy Framework, developed on the basis of a proposal by the High Representative, in cooperation with the European Commission and the European Defence Agency (EDA), sets out two main goals. The first is to provide a framework to European Council Conclusions on CSDP of December 2013 together with the Council Conclusions on CSDP of November 2013, which called for a Policy Framework in the field of CSDP. Second, it sets out certain priorities for CSDP cyber defence, while establishing the different roles of the European actors in this field. The CD Policy Framework further illustrates how there are a number of actors responsible in this field, most importantly the governments and militaries of the EU Member States. The first priority is to support the development of Member States' cyber defence capabilities related to CSDP. The second goal is to enhance the protection of communication networks used in support of CSDP missions and operations. The CD Policy Framework also seeks to promote greater civil- military cooperation, as well as cooperation between governments, EU intuitions, the private sector and academia. This is in line with the goal of the EUCSS to initiate greater synergies between the civilian and military approaches,[50] including greater cooperation in research and development. Lastly, the CD Policy Framework outlines the need for cooperation with relevant external partners, most importantly NATO, in heightening cyber resilience.

The two main actors driving developments in this field have been the European Defence Agency (EDA) and the EU Military Staff (EMS). The EDA is tasked with supporting the development of the Member States' cyber defence capabilities and the CD Policy Framework sets out that the EDA should work together with the Member States and the EEAS to deliver effective cyber capability.[51] Cyber defence is one of the ten priority areas set out in the EDA's Capability Development Plan, the strategic tool used by the Agency to identify

[47] See Chapter 8, Simon Duke, Capabilities and CSDP: Resourcing Political Will or Paper Armies.
[48] Neil Robinson, 'EU cyber-defence: a work in progress', European Union Institute for Security Studies, March 2014 https://www.files.ethz.ch/isn/182329/Brief_10_Cyber_defence.pdf
[49] EU Cyber Defence Policy Framework, Brussels, 18 November 2014.
[50] EUCSS (n 13) 11.
[51] Council of the European Union, EU Cyber Defence Policy Framework, Brussels, 18 November 2014, 4.

future capabilities in the short to long term.[52] The EDA is involved in delivering training and exercises, improving cyber situational awareness, developing a Cyber Defence Research Agenda, the early detection of Advanced Persistent Threats (such as malware aimed at cyber espionage), and the development of technology used for the protection of information such as cryptography for military use. The EDA also undertakes studies into the military cyber defence capabilities of the EU Member States to assess and identify gaps and areas for cooperation and civilian-military cooperation. An EDA stocktaking study examined cyber defence capabilities in the 20 countries that participated in the study, analysing capabilities in terms of doctrine, organisation, training, material, leadership, facilities and interoperability. At the EU level, it found that incident response capabilities could be deepened, and that a culture of cybersecurity had to be developed. It also presented a 'mixed picture' with respect to Member State capabilities,[53] pointing to a low level of maturity in terms of doctrine, organization and training. According to Christou,"[t]here has been confusion or at least little clarity on the function of the military in the cyber defence domain and the relationship between broader national cybersecurity strategies and cyber defence doctrines developed by the military."[54] The EU Military Staff (EUMS) also plays a role in EU cyber defence primarily by developing policy to ensure that the cyber protection of the Member States provide sufficient collective protection to the EU force in military operations. The goal is that cyber security issues are embedded in each stage of CSDP missions from the planning to force generation phase. This requires greater clarity about how to assess and identify potential cyber security risks at each of the different stages.

4.2. NATO Cooperation

Another pillar of EU cyber defence policy is cooperation with key partners, including NATO. The EU and NATO share some of the same challenges, namely ensuring an adequate level of cyber defence capabilities in operations led by those bodies. Cyber defence is one of NATO's core tasks, and at the 2014 Wales Summit, NATO adopted an enhanced policy and action plan on cyber defence. Like the EU, it is also undergoing a similar process to enhance its cyber defence capabilities. A dialogue between EU and NATO has been established in order to find fields of common interest, for instance, by using common standards in cyber security and defence matters. CERT-EU, responsible for the EU institutions, also entered into a technical agreement relating to information sharing with the NATO Computer incident response capability (NCIRC).[55]

The European Council Conclusions of December 2016 called for a strengthening of European security and defence through closer and reinforced cooperation with NATO.[56] It urged swift follow-up of the December 2016 Council conclusions on EU-NATO cooperation, which implement the joint declaration by EU and NATO leaders at the margins of the Warsaw Summit.[57] Cyber security and cyber defence are listed as areas for closer EU-NATO cooperation. Along with terrorism and organized crime, cyber security and cyber defence are

[52] European Defence Agency, Capability Development Plan. https://www.eda.europa.eu/what-we-do/eda-priorities/strategies/Capabilities
[53] See 'Cyber Defence', European Defence Agency. https://www.eda.europa.eu/docs/default-source/eda-factsheets/cyber-defence-factsheet
[54] Christou (n 26) 139.
[55] 'EU and NATO Increase Information Sharing on Cyber Incidents – Press Release', European External Action Service, 10 February 2016.
[56] European Council meeting (15 December 2016) EUCO 34/16, Brussels, 15 December 2016, point 10.
[57] Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 15283/16, Brussels, 6 December 2016.

conceived as 'hybrid threats',[58] which are a priority of EU and NATO. The document sets out practical areas of cooperation. For example, EU and NATO will exchange concepts on how to integrate cyber defence into the planning of missions and operations, with a view to greater interoperability, and the EU and NATO will harmonise training requirements in both institutions and include each other's staff in training and cyber defence exercises. It encourages cooperation in the field of cyber defence research, building upon the Technical Arrangement on Cyber Defence concluded between NATO and EU in February 2016. The agreement sets out ways to share best practices between the two technical centres of each organization (NCIRC and CERT-EU).

The EU and NATO share the common goal of protecting the communication systems and infrastructure of their Member States. Yet neither of these organizations will become central cyber defence institutions in their own right, instead supporting and facilitating action by their membership. Beyond technological cooperation between EU and NATO, they could also further contribute to the development of international norms that apply to cyberspace (see below).

5. External Dimension of Cyber Security

The sections above relate mainly to the EU's internal policies regarding cybercrime, network and information security, and cyber defence. Yet an effective policy also requires greater action at the international level. Since cybersecurity has both internal and external dimensions, it is a field where different Union competences must be combined.[59] The EUCSS outlines the goal of establishing a coherent international cyberspace policy in order to promote core EU values.[60] Regarding NIS, the Commission stresses that a purely EU approach will not be enough to face the challenges posed: "[a]lthough the objective of building a coherent and cooperative approach within the EU remains as important as ever, it needs to be embedded into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations."[61] It is in the external dimension of cybersecurity policy where the EU can potentially have a greater impact, by co-operating with states, international organizations and non-state bodies, and by influencing the development of norms at the international level.

The *European Principles and Guidelines for Internet Resilience and Stability*,[62] developed by the European Forum for Member States on public policies for security and resilience in the context of Critical Information Infrastructure Protection,[63] aims to set out a common European approach, establishing guidelines and principles that are to guide international discussion and co-operation with third states, international organizations, and private entities. One of these principles is that action taken to ensure stability and resilience of the internet must conform to the interests and values of the European Union. It is already evident that EU and Member State policies in this field must respect fundamental values such as democracy and the rule of law, and respect human rights, including those enshrined in the EU Charter of Fundamental Rights and Freedoms. Yet this principle acknowledges that the goal of ensuring cyber resilience comes with particular risks in terms of fundamental rights, including concerns regarding privacy, data protection, and due process.

[58] See Chapter by Fiott, Military CSDP Operations: Strategy, Financing, Effectiveness, on 'hybrid threats'.
[59] Wessel (n 7) 404.
[60] EUCSS (n 13) 3.
[61] European Commission, Communication on Critical Information Infrastructure Protection, 'Achievements and next steps: towards global cyber-security', Brussels, 31.3.2011, 4.
[62] European Principles and Guidelines for Internet Resilience and Stability (2011).
[63] European Forum for Member States (EFMS), was established in 2009 as a follow-up to the CIIP policy initiative adopted by the European Commission on 30 March 2009. See COM(2009)149 of 30.03.2009. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience."

States may justify the use of massive surveillance and monitoring of internet activity or the blocking of internet connections and communications by highlighting the increased security they bring, but such activities may undermine these core values and be disproportionate to the goal of heightened resilience.[64] Importantly, these principles not only apply to the activities of the EU and the Member States, but should also be promoted at the international level.

It is in this field of international cooperation where the EU and the Member States may be most capable of having influence. The EU has a stated objective of improving its role as a global actor, and can do more to influence the developments of norms at the international level. First, the EU has been involved in bilateral cyber dialogue with a number of partners, including the US, India, Brazil, China, South Korea and Japan. Notably this includes EU-US Working Group on Cybersecurity and Cybercrime, which works to foster greater cooperation between the EU and US, mainly in the field of cybercrime.

The EU is currently active in many of the multilateral forums that are responsible for developing policy on cyber-related issues. International governance bodies include the Organisation for Economic Co-operation and Development (OECD)[65], the United Nations General Assembly (UNGA)[66]; the Organisation for Security and Co-operation in Europe (OSCE); the International Telecommunication Union (ITU), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). In these bodies, the EU will seek to uphold certain 'core values', such as the respect for democracy, human rights and the rule of law. The 2015 Council Conclusions on Cyber Diplomacy stress that is essential for an EU approach for cyber diplomacy at global level "promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression; access to information and right to privacy".[67] Was discussed above, whereas some states including China and Russia view cyber security as requiring the state to play a strong top-down role, the EU approach stresses the need for an open and secure internet, which is not built on the logic of control. Since there is disagreement on how to tackle these issues, the EU can play a greater role in influencing developments within these multilateral fora.

Another external aspect of cybersecurity policy is deciding how the EU should respond to cyber attacks, especially those that are supported by states. This issue relates not only to the technical response, but questions relating to the EU's political and diplomatic response to coercive cyber operations, against both EU Member States and third states. In this vein, the Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') adopted on 19 June 2017 are a first step.[68] It stresses the EU's commitment to resolving international disputes in cyberspace through peaceful and diplomatic means and underlines the need for a joint diplomatic response in the case of a malicious cyber activity, in order to prevent and deter such activity. What would such a diplomatic response involve? For instance, restrictive measures taken under the EU's CFSP could be employed in response to a cyber attack against individuals and third states. The EU continues to develop a Framework for a joint EU diplomatic

[64] European Principles (n 43).
[65] E.g. OECD Working Party on Security and Privacy in the Digital Economy (SPDE) develops policy recommendations in the field of digital security and privacy protection.
[66] E.g. UNGA Res. 64/211 (2009) Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures; UN Res. 58/199 (2004) Creation of a global culture of cybersecurity and the protection of critical information infrastructures.
[67] Council Conclusions on Cyber Diplomacy, Brussels, 11 February 2015.

[68] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 10474/17, Brussels, 19 June 2017.

response to malicious cyber activities, stressing that they must respect certain key principles, such as the respect for international law and fundamental rights. The suspected state-sponsored cyber attack on Kiev's power grid is an example of the type of attack that may require such a coordinated diplomatic and political response by the EU.[69] A coordinated attack on an EU Member State would also require a political response at the EU level. Developing a set of tools to respond to cyber attacks remains an important part of the external dimension of cyber security.

A related question is how the EU Member States are to treat a very serious cyber incident against an EU Member State. According to the EUCSS "a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union (TFEU))."[70] There is also the question of whether a serious cyber incident could trigger Article 42(7) TEU[71] ('mutual defence clause'). This depends on the thresholds that must be met for such an incident to be understood as an 'armed attack', which is an issue of public international law. The EU also strongly supports the concept that norms of international law must also be applied to the cyber dimension, including cyber warfare. Yet the application of international legal norms to the realm of cyberspace is a state of development. The Tallinn Manual 2.0, for instance, is a project analyzing how existing international law norms are to be applied to cyberspace. Developed by legal experts, and facilitated by the NATO Cooperative Cyber Defence Centre of Excellence, the Manual examines the international law issues associated with cyber warfare, such as the law of responsibility and the law of armed conflict.[72] In the UN context, work is also underway, albeit slowly, in the United Nations Groups of Governmental Experts on Developments (UN GGE) in the Field of Information and Telecommunications in the context of international security. As these international rules begin to develop, there is potential for the EU and the Member States to influence such rules regarding the application of international law to cyberspace. While the EU and the Member States prefer non-binding and voluntary standards, the EU can influence developments to ensure a free and secure internet, and rules that respect human rights. In addition to developing internal rules to promote cyber security, the EU can also be a leader in developing the legal norms that apply to cyberspace. To date, however, the EU is lacking a comprehensive framework that would allow the EU to play such a role at the international level.

6. Conclusion

A common theme in cybersecurity debates is the blurring of boundaries: between public authorities and non-state actors; between criminal behavior and politically motivated attacks; between law enforcement and military action; between domestic and international action; between the physical and the online worlds. Such a blurring of categories can pose challenges for the Union – which is built upon clear demarcation on such issues – when seeking to combat cyber threats in a coherent and effective fashion. Yet the EU has made many advancements in cybersecurity policy since the 2000s, and the 2013 EUCSS seeks to ensure that the EU has an approach that cuts across various policy fields. A comprehensive vision and unified approach has not yet

[69] 'Ukraine power cut 'was cyber-attack'', BBC News, 11 January 2017. http://www.bbc.com/news/technology-38573074

[70] EUCSS (n 13) 19.

[71] 42(7) TEU, "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"

[72] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual Process, <https://ccdcoe.org/tallinn-manual.html>.

emerged. The multitude of actors involved in cybersecurity, the lack of central body responsible for taking the lead in these initiatives, the lack of a formal legal basis for cybersecurity in the EU Treaties, and the absence of a common understanding of cyber terminology, all make it difficult for such a European vision to develop. These issues should be addressed as the EU updates its cybersecurity strategy.

Most of the EU's action in the field of cybersecurity has dealt with internal EU policies (e.g. internal market) or is linked to criminal law (combatting cybercrime). In the fields of cybercrime and NIS, moreover, soft law instruments are being replaced by legislation.[73] Cybersecurity, however, touches on a broad range of other policy fields, and cyber defence is now emerging as a key issue where the EU must catch up. Cybersecurity and cyber defence can no longer be seen as internal matters for the EU and the Member States; cybersecurity policy has an important international element.

The EU should continue to strengthen its cyber policies, including through the CFSP framework. Yet the inter-governmental character of decision-making and the unwillingness of Member States to give the EU a central role in a core sovereign competence present a challenge to this goal. The EU has not sought to become a 'cyber power' with offensive capabilities. Several aspects of the EU's approach to cybersecurity – its legalistic framework, the multi-stakeholder approach, its emphasis on a secure and open internet, its focus on fundamental rights and values – contrast with the approach taken by a number of states that are active in the field. Given the EU's diverging approach, it has been argued that the EU could be viewed as a potential 'institutional laboratory' for governance in this field.[74] Its defensive, bottom-up approach contrasts with those states who approach the issue with the logic of control. Much of the EU's response, moreover, has been to ensure that a technical response to cyber threats are in place. Yet EU policy must also deal with the political and diplomatic dimension, especially as threats of state-sponsored cyber attacks increase. How will the EU and the Member States react at the international level to a serious cyber incident against a Member State, or against the EU institutions? The EU has a role to play at the international level by ensuring that certain EU interests and values are reflected in global decision-making. Cybersecurity and cyber defence can therefore be a field where the EU becomes a normative global actor, capable of establishing a culture of cybersecurity that extends beyond the EU. This includes a commitment to an open and secure internet, and to ensuing fundamental rights are not sacrificed in the name of protecting cyber security. While Member States remain dominant in the field of cyber defence, the EU can act as much more than just a coordinator and a facilitator of policies, it can potentially develop into a cyber-security actor in its own right.

[73] Elaine Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking', (2014) 5 *European Journal of Risk Regulation* 46, 49.

[74] Emmanuel Darmois and Geneviève Schméder, Cybersecurity: a Case for a European Approach, Security in Transition Working Paper ((2016) 19: "given its unique features, [the EU] has in theory the potential to be a model for other regions of the world".

Author(s): Jed Odermatt
Title: The European Union as a Cybersecurity Actor
iCourts Working Paper, No. 124, 2018

Publication date: 20/March/2018

URL: http://jura.ku.dk/icourts/working-papers/

iCourts Working Paper Series
ISSN: 2246-4891

Jed Odermatt, Postdoctoral Research Fellow, Centre of Excellence for International Courts, University of Copenhagen
E-mail: jed.odermatt@jur.ku.dk