THE CITY LAW SCHOOL
CITY, UNIVERSITY OF LONDON

The University of business, practice and the professions.

www.city.ac.uk

The Evolution of EU-US Cybersecurity Law and Policy: on Drivers of Convergence

CLS Working Paper Series 2024/05

Elaine Fahey*
City Law School, City St. Georges, University of London

* The City Law School, City St. George's, University of London, London, EC1V 0HB

Elaine Fahey
The City Law School

The City Law School Working Paper Series are published by The City Law School, City University London, Northampton Square, London, EC1V 0HB.

An index to the working papers in The City Law School Working Paper Series is located at:
www.city.ac.uk/law/research/working-papers

THE EVOLUTION OF EU-US CYBERSECURITY LAW AND POLICY: ON DRIVERS OF CONVERGENCE

Forthcoming in Journal of European Integration (2024)
https://dx.doi.org/10.1080/07036337.2024.2411240

Elaine Fahey*

Abstract

The digitalisation of the economy increases vulnerability of both economies in the EU and US, as does its transborder dimensions. Cyber policy has evolved over time on both sides of the Atlantic. The EU began initially to emphasise cybercrime regulation but its focus upon cybersecurity now dominates, similar to the US. The internal market has been evolved as a rationale for regulation in the EU and to similar effect a market-led approach dominates in the US. While in the EU a comprehensive cybersecurity law has been adopted, the US lacks a uniform federal cybersecurity law. Despite many domestic divergences, there is considerable similarity between the US and the EU. Substantively, these divergences have not inhibited convergence. Geopolitical considerations as to cyber have accelerated an ongoing process, driven by the transborder nature of cyber security and the global leadership of the EU and US.

Keywords: Cybersecurity, EU, US, cyber law-making, convergence, transatlantic, international cooperation, transborder

* Elaine Fahey, Professor of Law and Deputy Head of Department, Institute for the Study of European Law (ISEL), City Law School, City St. George's, University of London, UK. Elaine.Fahey.1@city.ac.uk.

Introduction

The digitalisation of the economy on both sides of the Atlantic shows increasing challenges for law and policy-making. The pace of the digitalisation of the economy widens the subjects and objects in need of regulation. This is because the digitalisation of the economy creates new vulnerabilities, as foreign governments or non-state actors can seek access to sensitive information or can try to disrupt critical functions or infrastructure. The multifaceted nature of cybersecurity - one of the fastest expanding policy areas of global data governance - means that measures to implement it vary dramatically across countries and regions (Mishra 2024). The EU and US have similar cybersecurity concerns and these have changed broadly in sync over time from crime to national security. They have, however, adopted very different approaches to addressing cybersecurity risks, with the US being temporally first but mainly being sectoral in its focus; and initially deploying hard law as to cybercrime, but becoming increasingly soft-law oriented. EU cybersecurity law is more recent but comprehensive and hard-law based while the US lacks a single and unitary federal cybersecurity law. This difference might appear superficially to fit the common characterization of the EU as a rights-based and the US as market-based (Bradford 2023). However, the EU has been motivated by risks of market fragmentation and security issues. There are many clear parallels between the EU and US when it comes to the digitalisation of the economy and the more defensive turns emerging e.g. digital sovereignty and Defend Forward. In the EU, digital sovereignty has evolved, to justify more protectionist turns in law and policy-making. As will be outlined, this is because any shifts in EU law and policy often have parallels in the US context and even show convergence e.g. from ‘Defend Forward’ initiatives in cyber law-making to the Internet of Things (IoT) regulation. Digital sovereignty and ‘Defend Forward’ shifts show how the digitalisation of the economy widens the subjects and objects in need of regulation but also generates protectionist and sometimes nationalistic impetuses. This occurs however differently cyber issues are framed on either side of the Atlantic. Despite many domestic divergences, there is considerable similarity between the US and the EU. Substantively, these divergences have not inhibited convergence.

While the EU has generally legislated more extensively than the US, this paper argues that differences more in form than in substance result and even show legal convergence (see also Young 2024). Moreover, it contends that EU regulation has been motivated by the desire to prevent market fragmentation. The EU increasingly needs to legislate to align policy among distrustful Member States in order to protect the single market, while the US does not have that same need. In addition, the US is shifting towards further regulation and governance of cybersecurity, increasingly with parallels to EU regulation. The EU’s motivation and the US’s changed approach do not fit comfortably with the common characterization of the two

jurisdictions' regulatory approaches, in line with one of the central arguments of this special issue (Young 2024).

In addition, and in line with the rest of the special issue, the EU and US align in global leadership and actively cooperate on cybersecurity. This cooperation is facilitated by the similarities in the two jurisdictions' approaches. The ratcheting up of bilateral cooperation has been driven by the process of the digitalisation.

Overall, the paper outlines how, despite domestic or internal differences, international cooperation is nonetheless significant and regularised through dialogues. Legal instruments reveal divergences but are not conclusive or prohibitive of international cooperation. The paper first considers the evolution of transatlantic cybersecurity. It then outlines transatlantic shifts in law-making as its subjects and objects widen, towards, for example, digital sovereignty and defend forward, focusing upon this widening of the subjects and objects of regulation overall and in a select casestudy. Thereafter, it assesses transatlantic bilateral cooperation with international goals. The paper is based on the analysis of the main legal documents on both sides, focusing mainly upon the salient periods of law-making and cooperation from the 1990s to the present.

The paper draws attention to the increasingly broad nature of cybersecurity and its legal form resulting in transatlantic cooperation. It shows how the esoteric nature of cybersecurity does not fit well with existing scholarship particularly on regulatory approaches. The paper also shows how cybersecurity advances transatlantic law-making for the digitalisation the economy, both domestically and bilaterally. Cybersecurity affords a broader perspective on transatlantic international cooperation as between the EU and US. It enables us to understand the evolution of global leadership in this field. It thus demonstrates how transatlantic legal convergence taking effect in cybersecurity is worthy of study.

THE EVOLUTION OF DIGITALISATION OF CYBER RULE-MAKING

There are many challenges of defining and delimiting cybersecurity for any jurisdiction with over 400 definitions of cybersecurity existing globally, with multiple conceptual disputes as to the appropriate framing of cybercrime and cybersecurity (Deibert 2018). The EU has been understood to adopt a narrower definition of cybersecurity distinguishing cybercrime, cyber espionage and cyber warfare unlike a broader one used in the US, which is more holistic and is part of its defence strategy (Odermatt 2018; Carrapico and Farrand 2024). Neither the EU cybersecurity strategy nor the US national strategy on cyberspace define explicitly the term 'cybersecurity' albeit both refer to similar issues: critical infrastructure protection, the fight against cybercrime, internet governance and the promotion of human rights online,

cooperation with the private sector and cyber defence (Anagnostakis 2021). Thus, there is no perfectly shared lexicon between the US and EU. Cybersecurity appears, however, more 'in vogue' in both jurisdictions as a dominant regulatory policy and external relations concern, moving away from crime as will be outlined here.

Digitalisation has changed the character of regulation in both the EU and US, where it plays out more defensively through regulation. This increase in regulation is related to vulnerabilities from elsewhere, e.g. digital sovereignty in the EU, 'Defend Forward' in the US, generating a broader span of subjects and objects to regulate (See White House 2018). This increase has occurred because the digitalisation of the economy creates new vulnerabilities, as foreign governments or non-state actors can seek access to sensitive information or can try to disrupt critical functions or infrastructure (Young 2024, Brown 2024). As a result, governments around the world have increasingly begun to legislate for cybersecurity, have developed cybersecurity policies and also now engage more explicitly in foreign policy involving cybersecurity issues, from trade agreements to sanctions, arguably led by the EU and US. The US model of regulation has historically entailed that the government is only expected to step in to protect national security on cybersecurity issues, but alongside tech companies (Bradford 2023). The challenges of digitalisation have shifted the parameters of these views. Digitalisation has entailed that there are more subjects and objects to regulate, imposing obligations on manufacturers as well as users. Accordingly, transatlantic cooperation has been incentivized. The US even appears to converge more closely towards EU law in distinct fields such as the Internet of Things (IoT), as will be outlined below.

Cybersecurity has many international and transnational elements and not easily siloed into the 'domestic' 'national' or 'state' on either side of the Atlantic. The EU, in particular, initially focused on cybercrime. However, cybercrime has acquired less significance overtime on both sides of the Atlantic as the external or international dimensions of cyber have become ever more important, such as the use of cyber warfare in Ukraine and Chinese surveillance and misinformation (Brown 2024). Cybersecurity now dominates EU law. This situation is arguably similar in the US, although the precise trajectory is harder to discern given the lack of a single and unitary federal cybersecurity law.

The difference in cybersecurity approaches between the EU and US appeared historically stark i.e. where the voluntary approach to the US allegedly contrasted with the compulsory approach provided for by the EU (European Union External Action 2014; EPRS 2018). This is not per se accurate where the US has in fact been the first mover in terms of sectoral regulation since the 1980s (Table 1). The difference in cybersecurity approaches between the EU and

US suggests in theory regulatory challenges (European Union External Action 2014; EPRS 2018). In particular, the powers and competences of regulatory agencies has historically been inhibitive of transatlantic cooperation (Pollack 2005). In practice, as this paper will outline, the EU and US nonetheless share similar approaches on many levels, both shifting in their emphasis from crime to security, also increasingly at international level. As a result, they constitute a strong alliance in geopolitical terms.

Cybersecurity policy developments have proven difficult to typologise on either side of the Atlantic but the debates have often been similar as to the character of cybersecurity law and its evolution. Nearly twenty years ago, however, US scholars also critiqued then the US 'National Strategy to Secure Cyberspace' of 2003 as consisting of little beyond an unbridled faith in "the market itself" (Katyal 2003: 2263), lacking sufficient regulatory scope. Later, US legal scholars criticised the expanding language of cyberwar, indistinguishable from cybercrime, cyber-attacks (Hathaway et al. 2012: 823). Recently, EU cybersecurity has begun to be situated as an internal market policy despite its security-turn (Fahey 2022a; 2022b; Kruck and Weiss 2023). The nuances of contemporary EU and US cybersecurity policy- and their evolution- is outlined next.

EU cybersecurity policy

The evolution of the 'internal market' is a key theme of EU law, which is regulatory, comprehensive and based upon hard law. The EU has undertaken considerable efforts at cybersecurity law-making over the course of two decades culminating in a Cybersecurity Act and Cyber Agency in 2019, evolving its approach towards hard law using its internal market. The EU has had three cybersecurity strategies in almost a decade. EU cyber policy was historically situated in a criminal law rationale (Fahey 2014). It was linked to the operation of the internal market because it affected the safety of consumers and the functioning of business. There were many legal instruments on EU cybercrime although none were comprehensive until 2005, notably later than the US legislating in 1986 (Fahey 2022a).

Thereafter, however, the EU began to heavily regulate and legislate for a broadened idea of cyber law-making. Despite security falling within the competence of the member states, a 'Cybersecurity Act' was adopted in the context of the Digital Single Market Strategy grounded in Article 114 TFEU, the EU's internal market legal competence in 2019 (Regulation 2019/881/EU, 2019). The Act had the intention to establish a high level of cybersecurity, cyber resilience and trust within the Union with a view to ensuring the proper functioning of the internal market to avoid disparities between States in the absence of harmonisation. The changes this new EU Regulation sought to bring about related to both a comprehensive reform of ENISA, the EU's cyber agency and the creation of a certification framework. The Act granted

ENISA a permanent mandate, gave it more resources and new tasks, including the implementation of an EU cybersecurity certification framework for ICT products. Prior to this, ENISA had a limited fixed-term mandate and had as its mission merely to raise awareness of network and information security and to develop and promote a culture of network and information security (Markopoulou, Papakonstantinou, de Hert, 2019). This alignment of 27 Member States matters as it augmented EU unity and its policy on cybersecurity as an internal market issue.

The most recent example concerns the regulation of Internet of Things (IoT), where the EU moves beyond putting obligations for users to keep data safe to require that manufacturers design products that keep data safe e.g. in the new Cyber Resilience Act and in regulations on wireless devices, discussed above (European Commission 2022). The Act would ensure products carrying the 'CE marking 'meet a minimum level of cybersecurity checks. Sensitive products running afoul of the rulebook face fines of up to €15 million, or 2.5 percent of worldwide turnover, whichever is higher. CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements. It is required for products manufactured anywhere in the world that are then marketed in the EU. For those that can present a significant cybersecurity risk, a manufacturer would have to prove they meet the requirements to a national authority or through a third-party assessment.

Cybersecurity now straddles EU security and Digital Single Market policies but also the Common Foreign and Security Policy on account of cyber sanctions, a distinct foreign policy area requiring unanimity rather than a qualified majority of states (Carrapico and Barrinha 2017; Carrapico and Farrand 2018; Fahey 2022a). This traversal of domains reflects the hybridity of the digital domain (Broeders et al 2023).

US cybersecurity policy

In the US, unlike in EU law, no single binding cybersecurity law governs cybersecurity. A pro-market US ethos is embedded in the US regulatory framework. Rather there are a few laws that establish cybersecurity requirements for specific sectors (see Table 1). The Health Insurance Portability and Accountability Act (HIPAA) (1996) purports to control and modernize medical and healthcare information flow and contains cybersecurity requirements to protect health data. The Gramm-Leach-Bliley Act (1999) made it mandatory for financial institutions -- meaning companies that provide consumers products or services like loans, financial or investment advice, or insurance -- to explain their information-sharing practices to their customers and to safeguard their sensitive data. The Homeland Security Act (2002) included

the Federal Information Security Management Act (FISMA), which attempts to recognize the importance of information security to the economic and national security interests of the US and requires federal agencies to implement security controls to protect their information systems and data, to protect the confidentiality, integrity, and availability of the information they collect, store, and use. These requirements are robust but narrowly focused.

Because of this selective hard law, soft law and industry standards are much more significant in the US than in the EU. The 2013 National Institute of Standards and Technology (NIST) Cybersecurity Framework is regarded as the key framework although it is a voluntary standard. It aims to improve the cybersecurity posture of critical infrastructure organizations, with the intent of preventing data breaches and mitigate potential risks to system (Executive Order 2013; NIST nd). Despite being voluntary, it has been widely adopted private and public sector actors in the U.S. Other voluntary standards -- in particular the ISO/IEC 27001 'family' of a dozen international standards that enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties and ISO 22301:2019, which is designed to help organizations implement, maintain and improve a management system to prevent, prepare for, respond and recover from disruptions when they arise -- are also quite key. These ISO standards are the world's best-known non-binding standards for information security management systems (ISMS) and their requirements and a key part of US market-led cyber policies.[i]

The Cyber Incident Reporting for Critical Infrastructure Act, which was passed in 2022, requires covered entities within the critical infrastructure sector to report significant cyber incidents and ransomware payments. This is a more administrative and European-style approach to cybersecurity, also evident in a new Federal Communications Commission (FCC) program for wireless IoT products, discussed above. Thus, like the EU, the US has shifted to imposing cybersecurity obligations on manufacturers, not just users. It has, however, done so using soft law.

The US' patchwork quilt of regulation appears very different from the EU's. Superficially one might say that differences are generally explained through rights-based versus market-based characterisations (Bradford 2023). The EU's policy development has been driven more by the desire to curb market fragmentation prior to the development of digital sovereignty yet sometimes reflecting rights other times security issues (Farrell and Newman 2024).

EU cybercrime/ cybersecurity law	Binding Law	US cybercrime/ cybersecurity law	Binding Law
Cybercrime - Council Framework Decision 2005/222/JHA on attacks against information systems; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems	Y	Cybercrime- Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 1986	Y
Cybersecurity Act and Cyber Agency 2019	Y	Sectoral federal cybersecurity law • e.g., Health Insurance Portability and Accountability Act (HIPAA) 1996 • Homeland Security Act 2002: included the Federal Information Security Management Act (FISMA) • Gramm–Leach–Bliley Act 1999 • Federal Rotational Cyber Workforce Program Act 2021 • Cyber Incident Reporting for Critical Infrastructure Act, 2022 Cybersecurity Framework NIST 2013 ISO/IEC 27001 family	Y N N
Cybersecurity strategy 2013, 2017, 2020	N	Cybersecurity strategy 2003, 2018, 2023	N

IoT- Commission Delegated Regulation (EU) 2022/30; IoT- Cyber Resilience Act 2022 improving cybersecurity and cyber resilience in the EU through common cybersecurity standards for products with digital elements	Y	IoT Cyber Trust Mark	N

Table 1 Cyber regulation framework

Source: Author's own

TRANSATLANTIC SHIFTS TOWARDS DIGITAL SOVEREIGNTY AND 'DEFEND FORWARD'

There are notable parallel shifts in the EU and US towards increasingly defensive objectives in cybersecurity regulation. This section reflects on these parallels as responses to digitalisation as a general theme. It then considers how more subjects and objects to regulate through the lens of the example of the Internet of Things (IoT), notably the basis for EU-US cooperation during the Biden administration.

Parallels of defensive objectives responding to digitalisation

Cybersecurity is one of the fast-expanding policy areas of global data governance and governments increasingly understand cyber to extend well beyond the technical aspects of network and data security to include national and economic security (Mishra 2024, 62). It has increasingly taken effect with 'defensive' objectives to this regulation where increasingly protectionist and / or nationalistic law-making emerges on both sides of the Atlantic, that even explicitly emphasise sovereignty.

EU official documents and EU Member State actors increasingly reference 'digital sovereignty' (Economic, Social and Environmental Council 2019; European Parliament 2019; 2020; ENISA 2021) to justify 'mainstream' law-making (Roch and Oleart 2024). Digital sovereignty appears to be understood as Europe's ability to act independently in the digital world through further regulation and governance, even heavily contested as to its meaning (European Parliament 2020; Cf. European Commission, 2020; See De Gregorio 2022; Barrinha and Christou 2022). Digital sovereignty has 'defensive' elements, concerned with protection from attacks, threats, hostilities and systems failures and traversing with complexity industrial and other policies (Seidl and Schmitz 2023; McNamara 2023). The increasing mentions of 'digital' or 'technological sovereignty' show that the EU institutions use it as a synonym for the Union's ability to use technology in order to make the internal market work (Fahey and Poli 2022).

Notably, there are many references in cyber issues and in increasingly defensive terms. Europe's digital sovereignty is invoked explicitly in debates concerning the security of the EU and its Member States for example to tackle cyber threats but also in the context of synergies between civil defence and space (European Commission 2021). The EU is increasingly concerned about its dependence on foreign technology, including digital technology and is set to reducing this dependence to increase its security where "digital services and the finance sector are among the most frequent targets of cyberattacks, along with the public sector and manufacturing" (European Commission and High Representative 2020: 1 & 3). There is also a potentially protectionist aspect to cybersecurity. A 2023 leaked draft of the EU's proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) included certain digital sovereignty requirements, mandating providers to 'demonstrate their trustworthiness and effectiveness of their cybersecurity defences.' This is arguably a form of localisation (Propp 2023). In addition, in May 2019 the EU created a new sanctions framework that would enable the EU to impose restrictive measures in response to a cyberattack. Such sanctions were imposed for the first time in June 2024.

Although the US is not generally as concerned about digital sovereignty as the EU (Young 2024), cybersecurity is the exception (see also Brown 2024). Cybercrime is growing both in frequency and sophistication, and there are many critical examples showing how vulnerable the US digital infrastructure, whether public or private, is to intrusion by hackers (Bradford 2023: 68). The US has become victim to a broad range of significant and more recent cyber-attacks e.g. attacks on banks, persistent intellectual property theft by China, and the Russian intervention in the 2016 election. Frustration with international law and norms grew as cyberthreats mounted seemingly unabated (Goldsmith 2022, Edgar 2017). The Obama administration emphasised cyber defenses and 'deterrence by denial', a Cold-War concept that sought to deter attacks by ensuring that they would be ineffective. The US also worked to increase accession to the Council of Europe's Budapest Convention, but with little success (Edgar 2017).

The US - possessor of the world's most powerful cyber arsenal - responded in 2018 by unveiling a new Defend Forward (DF) cyber strategy (White House 2018; White House 2023; Goldsmith 2022). It was a step in the direction of more offensive action in cyberspace to proactively disrupt attacks and threaten retaliation.[ii] The US is among the world's most digitally dependent nations and has had reason to have a particularly offensive and defensive cyber law policy. Yet the US did not respond more robustly in the past because of perceived legal constraints under international law where cyber operations against the US did not rise to the level of 'uses of force' or 'armed attacks' under international law (Goldsmith 2022). In

addition, the US has adopted more explicitly discriminatory, even protectionist, cybersecurity measures. In 2023 the US adopted legislation requiring the Chinese-owned ByteDance to sell Tiktok or TikTok will be banned from the US (Brown 2024). In 2024, President Biden signed Executive Order (EO) 14117 on 'Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern' to prevent the large-scale transfer of sensitive personal data and US Government-related data to 'countries of concern' (White House 2024).

Wide subjects and objects to regulate: the Internet of Things (IoT) in the EU and US

There are more specific contemporary parallels with the lexicon of digital sovereignty and strategic autonomy emerging in EU law and policy as to the Internet of Things (IoT). It could be said to be a prominent case study of the widening of the subjects and objects of regulation. It is suggested that the US government steps aside to maximize the private sector's unfettered innovative zeal when it comes to protecting national security and including cybersecurity- and aligns with EU practice (Bradford 2023: 32). This analysis is certainly borne out as to the Internet of Things (IoT) where in the US Government-backed labelling and Cyber Trust Mark legislation is evolving, possibly shifting beyond soft law approaches for security-related reasons, closely or at least more similar to EU law.

These developments take effect because the IoT and its regulation has entailed that there are more users to regulate. It thus moves beyond users to manufacturers for its regulatory scope. For instance, Commission Delegated Regulation 2022/30 also imposes requirements on wireless devices to enhance their level of cybersecurity and the protection of networks, the protection of user privacy, protection from monetary fraud (See Commission Delegated Regulation (EU) 2022/30). The scope is very broad and it is the first time that obligations are imposed on manufacturers of products. As noted above, the European Commission has also presented a new Cyber Resilience Act proposal aimed at imposing new cybersecurity requirements on internet-connected devices, widening even further the concept and reach of cybersecurity (European Commission 2022c). Manufacturers of digitally connected products would have to meet new EU requirements, whether the products are produced in the EU or not. To similar effect, the US Federal Communications Commission (FCC) voted thereafter in 2023 to create a (voluntary) cybersecurity labelling program for wireless consumer Internet of Things ("IoT") products. Under the program, qualifying consumer smart products that meet robust cybersecurity standards will bear a label—-including a new "U.S. Cyber Trust Mark"—- to help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards (FCC 2023). As a result, the EU and

US notably could reach political agreement bilaterally in the 9th EU-US Cyber Dialogue of 2023 (discussed also below) to development a Mutual Recognition Agreement to identify the commonalities between the Cyber Resilience Act and the Cyber Trust Mark (European Commission 2023; Federal Communications Commission 2023; US Chamber of Commerce 2024). The EU and US additionally signed an Administrative Arrangement on a Joint CyberSafe Products Action Plan in 2024, with the aim to advance technical cooperation to support the goal of achieving mutual recognition in the area of cybersecurity requirements for Internet-of-things (IoT) hardware and software consumer products and deepen cooperation between relevant agencies of the EU and US (European Commission 2024). US attention has even focussed on to the extent to which the EU could converge with NIST and ISO standards (FCC 2023; European Commission 2023; US Chamber of Commerce 2024). The broad nature of vulnerabilities provided for here is of significance, showing explaining in part the hybridity of the instruments evolving (Broeders et al 2023). There is of course a complex history of EU-US Mutual Recognition Agreements, often ending in failure, outside the scope of this paper (Pollock 2005). However, this latest effort suggests a renewed interest in evolving cyber law-making-, a new era of cooperation. It also arguably indicates a form of Brussels Effect of EU law-making, seeing explicit support from the US Chamber of Commerce to learn from the EU's ENISA certification as well as US Government-level intent to reach agreement with the EU through an MRA.

A TURN TO THE GEOPOLITICAL? TRANSATLANTIC BILATERAL COOPERATION WITH INTERNATIONAL GOALS

Geopolitical considerations have given an additional impetus to transatlantic cooperation on cybersecurity beyond its transborder nature. Since the 1990s at least, the EU and US have aligned in global leadership and cooperated to a high degree. They have cooperated multilaterally and bilaterally, with bilateral cooperation becoming even more intense particularly during the Obama and Biden administrations.

The EU and US share similar views at international level on cybersecurity. Cybersecurity commitments of countries such as the US and EU are said to contrast sharply with those more sovereignty-oriented frameworks advocated by countries such as Russia and China (Johns and Riles 2016; Buchan and Navarrete 2021).

The EU and US have a significant presence in many international fora in cybersecurity, as two of the over 50 countries and regions adopting cybersecurity policies and constantly lead in key fields and policies. The EU's cybersecurity policy is becoming increasingly outward facing (Wessel 2019: 507). Like the US, the EU is also increasingly interested in nudging international cybersecurity developments. Their efforts have mainly centered on the Council

of Europe, due to stalemate until recently at the UN (Bendiek 2018; Buchan and Navarrete 2021; Delarue 2020; Kasper and Antonov 2019; Verhelst and Wouters 2020; Markopoulou et al. 2019; Carrapico and Farrand 2020; Renard 2018). The Council of Europe's 2001 Budapest Convention, which facilitates law enforcement cooperation involving digital evidence, which is not exclusive to but is particularly important with respect to cybercrime.[iii] Although the US is not a member of the Budapest Convention, it has continued to participate in this forum and more broadly to champion its evolution as an international 'gold' standard. Only recently have negotiations begun on a new treaty on cybercrimes under the auspices of the UN (UNODC 2023).

Absent a UN treaty, transatlantic cooperation on cybersecurity has been beneficial globally, (Christou 2016; Delarue 2020). By the end of 2023, nine dialogues had taken place between the EU and US in the area of cybersecurity over multiple EU and US administrations. The details of many of these dialogues are difficult to find. This is perhaps unsurprisingly as dialogues are a form of soft law collaboration, highly dependent upon political dynamics.

The first and earliest dialogue -- the 2010 'Working Group on Cybersecurity and Cybercrime' (European Commission 2010) -- however, had a clear goal; encouraging ratification of the Budapest Convention. Subsequent dialogues have focused upon global issues and in particular international law -- such as the promotion and protection of human rights online; norms of behaviour in cyberspace, and application of existing international law in cyberspace -- and cybersecurity capacity building in third countries. Here the emphasis was on trying to establish global understandings.

Geopolitical concerns have given additional impetus to transatlantic cybersecurity cooperation lately. Russia's military aggression against Ukraine has led to enhanced transatlantic cooperation and coordination to prevent, detect and respond to malicious cyber activities, including imposing sanctions (Szep 2022; Szep et al. 2023). In the context of the EU-US Trade and Technology Council, Brussels and Washington sought to evolve a common outlook on '6G' telecommunications equipment so as to prevent Chinese companies dominating the market as they have in 5G (White House 2023; Carver 2023). This more recent phase of transatlantic cybersecurity cooperation has focused on how to coordinate responses against specific third countries.

Yet another focus of transatlantic cybersecurity cooperation now seems to be emerging – mitigating the trade effects of different cybersecurity requirements. Such a focus has been common in transatlantic cooperation in general, but not in cybersecurity. The issue has moved up the agenda as both jurisdictions are preparing to establish standards to ensure that that

products associated with the IoT are cybersecure. In December 2023, in the 9th EU-US Cyber Dialogue, they agreed a Joint CyberSafe Products Action Plan in 2024, with the aim to advance technical cooperation to support the goal of achieving mutual recognition in the area of cybersecurity requirements for IoT hardware and software consumer products and deepen cooperation between relevant agencies of the EU and US (European Commission 2024). While there are many thorny issues to resolve and the transatlantic track record on mutual recognition agreements is not good, this effort suggests a new era of cooperation.

Although this paper is mostly concerned with the nefarious activities enabled by digitalisation, the consequences thereof are increasingly complex - and 'transatlantic'. Securing access to electronic evidence has become one of the key challenges for intergovernmental cooperation in criminal matters with respect to the 'globalisation of evidence' (Daskal et al. 2018), transcending legal formulas used in cumbersome mutual legal assistance instruments. The EU and US are key leaders here in recent times.

The Parties to the Budapest Convention had searched for solutions for some time on transborder access to data and Cloud Evidence through a Protocol (See Council of Europe 2019). A 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence' was adopted in late 2021 and forms a landmark in transnational cooperation. In its negotiation directives for this Protocol, the EU had raised the issue as to consistency with respect to e-evidence regimes and third countries, in particular the US and the autonomy of the EU legal order.

After protracted negotiations, involving mainly the EU on the one hand and the US, Australia and Canada on the other, a compromise was eventually reached, providing for a sufficient level of flexibility to permit adaptation to different legal systems and to evolving technology, business models and interpretation by the courts (See Polakiewicz 2022; Council of Europe, 2021: 3-4). The Protocol gives precedence, where applicable, to Convention 108+, other agreements establishing a framework for the protection of personal data (EU-US Umbrella Agreement, 2016), as well as to other mutually determined arrangements, but it also formulates a freestanding set of data protection safeguards, of particular significance (Second Protocol, Budapest Convention 2021: Article 14). It is evidence of immense transatlantic cooperation in getting to this point, with the EU's esoteric stance flexibly accommodation by an international organization and US political support (Polakiewicz 2022).

More concretely as to EU-US relations in this domain, in 2018, the US Congress enacted the Clarifying Lawful Overseas Use of Data Act, or 'CLOUD Act' in 2018 in the midst of the infamous 'Microsoft' litigation on appeal to the US Supreme Court.[iv] As a result, it is said that the EU proposed similar significant legislation allowing EU enforcement agencies to

preserve and collect cloud-based evidence outside of the mutual legal assistance treaty (MLAT) system, through a so-called E-evidence package (EPRS 2021; See European Commission, 2018a, 2018b). Then, in 2019, European Commission began negotiations with the US of comprehensive EU-US agreement on access to electronic evidence, paused to enable the EU advance its own regime (European Commission 2019).

The 'evidence' example draws attention to the effects of EU law in the US and US law in the EU in the digital era. Such cooperation across borders necessitates global leadership to protect the rule of law (see also Brown 2024). It remains a 'constant' of the relationship even in cyber policy and in an age of geopolitics.

Conclusions

This article draws attention to the benefits of considering legal issues and their framing in the evolution of cybersecurity. The article has sought to pinpoint the stages of the development of transatlantic cybersecurity cooperation in law and policy. Cybersecurity is an important addition to scholarship on transatlantic cooperation. This is because cybersecurity has expanding contours that necessitate legal changes the study of which is of value to many subjects. Convergence between the EU and US legal orders take place in the area of cybersecurity that is distinctive because the EU and US have similar cybersecurity concerns, however differently framed- and these have nonetheless changed broadly in sync over time, from crime to national security.

The case study of transatlantic approaches to cybersecurity is striking for many reasons. Both jurisdictions have adopted very different approaches to addressing cybersecurity risks, with the US being temporally first and but mainly being sectoral in its focus and initially deploying hard law as to cybercrime, but becoming increasingly soft-law oriented. From a legal perspective, soft law is of course not the only prevailing standard in the US- although overall it shows a more market-driven basis for cyber law and practice. Limited specific sectoral examples of federal cybersecurity law show a historic prominence of areas warranting regulation beyond market-based organization e.g. health, finance or security. EU cybersecurity law is then more recent but comprehensive and hard law-based. This difference might appear superficially to fit the common characterization of the EU as a rights-based and the US as market-based. However, the EU has been shown to legislate for a broader range of concerns, including market-based concerns as much as security and the directions of travel on law-making have aligned in many respects. The EU and US thus form an important study of the evolution of law and policy-making as to digitalisation from a range of perspectives, including but not limited to law, politics and international relations, because they do not fit

comfortably with conventional characterisation of the approach adopted to regulation by the EU and US.

There are noticeably also clear parallels between the EU and US when it comes to the digitalisation of the economy, on account of the expanding range of entities to regulate, that show its value as a casestudy. This paper has focused upon the more defensive turns emerging on both sides of the Atlantic e.g. digital sovereignty and Defend Forward and the realm of IoT. The paper has shown that while the forms of regulation are very different and have very different motivations, there is considerable similarity between the US and the EU on substance enabling also bilateral cooperation.

This paper has thus demonstrated how these differences in the form of policies do not lead to confrontation between the EU and the US and do not impede transatlantic cooperation. Cooperation was initially driven by the the transborder nature of cyber threats. Geopolitical considerations have subsequently accelerated the ongoing process of cooperation. The EU and US share similar views at the international level on cybersecurity, evidenced by their bilateral and multilateral cooperation and continue to cooperate multilaterally and bilaterally. The acceleration of the necessity of cyber regulation seems unlikely to abate, irrespective of shifts in the administration in the EU or US. Convergence in standards and values as to data privacy will also continue to be an important question for consideration on both sides of the Atlantic. Further institutionalised cooperation seems likely to be a source of future research with respect to the place and form of dialogues and other sites of cooperation.

References:

Anagnostakis, D. (2021). The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. Journal of Cyber Policy, 6(2), 243–261. https://doi.org/10.1080/23738871.2021.1916975.

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (EU-US Umbrella Agreement), *O.J. L 336, p. 3.*

Barrinha, A. and Christou, G. 2022. Speaking sovereignty: the EU in the cyber domain. European Security, *31: 356*.

Bendiek, A. 2018. The EU as a Force for Peace in International Cyber Diplomacy. SWP Comment No 19/2018. Available at: www.ssoar.info/ssoar/handle/document/57428 [Accessed 1 July 2024].

Bradford, A. 2023. *Digital Empires*. Oxford: Oxford University Press.

Broeders, D., Cristiano, F., & Kaminska, M. 2023. In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. JCMS: Journal of Common Market Studies, *61(5): 126.*

Brown, S.A.W. 2024. Beyond the Great Firewall: EU and US Responses to the China Challenge in the Global Digital Economy, Journal of European Integration, *46/7.*

Buchan, R. and Navarrete, I. 2021. Cyber espionage and international law. In: Tsagourias, N. (Ed.) *Research Handbook on International Law and Cyberspace*. 2nd edition. Cheltenham: Edward Elgar.

Budapest Convention on Cybercrime. 2001. ETS No. 185.

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

Carrapico, H. and Farrand, B. 2018. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. In: Bures, O. and Carrapico. H. (Eds.), *Security Privatization: How Non-Security-Related Businesses Shape Security Governance*. Cham: Springer.

Carrapico, H. and Farrand, B. 2020. Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. Journal of European Integration, *42: 1111*.

Carrapico, H. and Farrand, B. 2024. Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics. JCMS: Journal of Common Market Studies.

Carver, J. 2023. More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. The Journal of European Public Policy, *31: 1.*

Christou, G. 2016. *Cybersecurity in the European Union*. Ch 7. London: Palgrave Macmillan.

Christou, G. 2020. The collective securitisation of cyberspace in the European Union. In: Lucarelli, S. et al., *Collective Securitisation and Security Governance in the European Union*. London: Routledge.

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, *O.J. L 7*, 12.1.2022, p. 6.

Daskal, J., Swire, P. and Christakis, T. 2018. The Globalization of Criminal Evidence. 16 October. IAPP.

Deibert, R. 2018. Toward a Human-Centric Approach to Cybersecurity. Ethics & International Affairs, *32: 411.*

Delarue, F. 2020. *Cyber Operations and International Law*. Cambridge: Cambridge University Press.

De Gregorio, G. 2022*. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society.* Cambridge: Cambridge University Press.

Economic, Social and Environmental Council (France). 2019. Opinion: Towards a European Digital Sovereignty Policy. 13 March. Available at: https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf [Accessed 1 July 2024].

ENISA. 2021. Exploring Research Directions in Cybersecurity. 23 April. Available at: https://www.enisa.europa.eu/news/enisa-news/exploring-research-directions-in-cybersecurity [Accessed 1 July 2024].

European Commission. 2010. EU-US Working Group on Cybersecurity and Cybercrime. EU-US Summit of November 2010. Lisbon. MEMO/10/597.

European Commission. 2021. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan on synergies between civil, defence and space industries. COM (2021) 70 final.

European Commission. 2022. Cyber Resilience Act. 15 September. Available at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Accessed 1 July 2024].

European Commission. 2023. EU and the United States hold Cyber Dialogue in Brussels. 7 December. Available at: https://digital-strategy.ec.europa.eu/en/news/eu-and-united-states-hold-cyber-dialogue-brussels [Accessed 1 July2024].

European Commission. 2024. Administrative Arrangement on an EU-US Joint CyberSafe Products Action Plan. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan [Accessed 1 July 2024].

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2020. Joint communication to the European Parliament and the Council, “The EU’s Cybersecurity Strategy for the Digital Decade”. JOIN (2020) 18 final.

European Parliament. 2019. Resolution on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them, 2019/2575(RSP). 12 March. Available at: https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1577382&t=d&l=en

[Accessed 1 July 2024].

European Parliament. 2020. Digital sovereignty for Europe. EPRS Ideas Paper Briefing. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf [Accessed 1 July 2024]

European Parliamentary Research Service (EPRS). 2018. EU Sanctions: A Key Foreign and Security Policy Instrument. PE 621.870.

European Union External Action. 2014. Fact Sheet: EU-US cooperation on cyber security and cyberspace. 26 March. Available at: http://eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf [Accessed 1 July 2024].

Exec. Order No. 13636, 3 CFR 13636 Cybersecurity.2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity/. [Accessed 1 July 2024].

Fahey, E. 2014. The EU’s Cybercrime and Cybersecurity Rule-Making: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation, *5: 46*.

Fahey, E. 2022a. Developing EU Cybercrime and Cybersecurity: On legal challenges of EU institutionalisation of cyber. In: Hoerber, T., Weber, G. and Cabras, I. (Eds.), *The Routledge Handbook of European Integrations*. London: Routledge.

Fahey, E. 2022b. EU as a Global Digital Actor. London: Hart Publishing.

Fahey, E. and Poli, S. 2022. The strengthening of the European Technological Sovereignty and

its legal bases in the Treaties. Eurojus*, 2: 147.*

Farrand, B. 2023. The ordoliberal internet? Continuity and change in the EU's approach to the governance of cyberspace. European Law Open*. 2: 106.*

Farrell, H. Newman, A. 2024. *Underground Empire: How America Weaponised the World Economy*. Penguin Books.

Federal Communications Commission (FCC). 2023. The FCC's Proposed Voluntary Cybersecurity Labeling Program for

Internet-Enabled Devices. 10 August. Available at: https://docs.fcc.gov/public/attachments/DOC-395909A1.pdf [Accessed 1 July 2024].

Goldsmith, J. 2022. *The United States' Defend Forward Cyber.* Oxford: Oxford University Press.

Hathaway, O. A. et al. 2012. The Law of Cyber-Attack. California Law Review. *100: 817.*

Johns, F. and Riles, A. 2016. Introduction to Symposium on Cybersecurity and the Changing International Law of Data. American Journal of International Law, *110: 335.*

Kasper, A. and Antonov, A. 2019. Towards Conceptualizing EU Cybersecurity Law. ZEI Discussion Paper C253. Available at: www.researchgate.net/profile/Center-For-European-Integration-Studies/publication/338038206_ZEI_Discussion_Paper_C_253_Towards_Conceptualizing_EU_Cybersecurity_Law/links/5dfb5630a6fdcc28372c19eb/ZEI-Discussion-Paper-C-253-Towards-Conceptualizing-EU-Cybersecurity-Law.pdf [Accessed 1 July 2024].

Katyal, N. K. 2003. Digital Architecture as Crime Control. The Yale Law Journal. *112: 2261.*

Kruck, A., and Weiss, M. 2023. The regulatory security state in Europe. Journal of European public policy, *30(7): 1205*.

Markopoulou, D., Papakonstantinou, V. and De Hert, P. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, *35(6): 105336*.

Mishra, N. 2024. *International Trade Law and Global Data Governance: Aligning Perspectives and Practices*. Oxford. Hart Publishing.

NIST. nd. Cyber Accident. Available at: https://csrc.nist.gov/glossary/term/cyber_incident [Accessed 1 July 2024].

Polakiewicz, J. 2022. The Emperor's New Clothes – Data Privacy and Cybersecurity from a European Perspective. In: Fahey, E. and Mancini, I. (Eds.) *Understanding The EU As A Good Global Actor: Whose Metrics?* London: Edward Elgar.

Pollack, M. A. 2005. The New Transatlantic Agenda at Ten: Reflections on an Experiment in International Governance. JCMS: Journal of Common Market Studies, *43: 899.*

Propp, K. 2023. A US Perspective on Negotiating with the European Union. In: Fahey, E. (Ed.), *Routledge International Handbook on Transatlantic Relations*. Forthcoming. London: Routledge.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ L 151, p. 1.*

Renard, T. 2018. EU Cyber Partnerships: Assessing The EU Strategic Partnerships With Third Countries In The Cyber Domain. European Politics and Society, *19(3): 321.*

Roch, J., & Oleart, A. 2024. How 'European sovereignty' became mainstream: the geopoliticisation of the EU's 'sovereign turn' by pro-EU executive actors. Journal of European Integration, *1*.

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2021. COM(2021)57-final.

Seidl, T., and Schmitz, L. 2023. Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. Journal of European Public Policy, *1*.

Szép, V. 2022. Unmatched Levels of Sanctions Coordination: The Strength of Transatlantic Cooperation in the Russia's War on Ukraine. Verfassungsblog. 23 March. Available at: https://verfassungsblog.de/unmatched-levels-of-sanctions-coordination/ [Accessed 1 July 2024].

Szép, V. et al. 2023. Case Studies of the EU's CFSP Activity. ENGAGE Working Paper Series; No. 20. Available at: https://pure.rug.nl/ws/portalfiles/portal/634322393/ENGAGE_Working_Paper_20_Case_Studies_of_the_EU_s_CFSP_Activity_2.pdf [Accessed 1 July 2024].

UNODC. 2023. Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalisation and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes. Vienna.

Verhelst, A. and Wouters, J. 2020. Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives, International Organization, *15(2): 141.*

Wessel, R. A. 2019. Cybersecurity in the European Union: Resilience through regulation?. In: Conde, E. et al. (Eds.), *The Routledge Handbook of European Security Law and Policy*. London. Routledge.

White House. 2018. National Cyber Strategy of the United States of America. September. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed 1 July 2024].

White House. 2023. National Cybersecurity Strategy. March. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [Accessed 1 July 2024].

White House. 2024. Executive order 14117 of February 28, 2024. Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ [Accessed 1 July 2024].

Young, A.R. 2024. Governing the Digital Economy: Transatlantic Accommodation and Cooperation," Journal of European Integration, *46/7.*

[i] ISO is an international organization with national standards bodies from 124 countries contributing as full members, making it a unique nation states-oriented standardization body with global reach. ISO and IEC are best known their international standards, defined as providing "rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context." Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family. ISO 22301:2019 is similarly significant, which is an international standard for business continuity management that is designed to help organizations implement, maintain and improve a management system to prevent, prepare for, respond and recover from disruptions when they arise.

[ii] E.g. proposed EU Cyber Resilience Act (European Commission 2022) concerning software and hardware products, contrasts with the US IOT labelling scheme and the Executive Order on Software as well as associated standardisation work.

[iii] such as common risk management criteria for the protection of critical digital infrastructures, joint cyber exercises, public-private partnerships, the promotion of the Council of Europe's Budapest Convention, and joint operational responses to cybercrime

[iv] See *Microsoft v United States*, 829 F.3d 197 (2d Cir. 2016). The decision was on appeal to the U.S. Supreme Court when the CLOUD Act was enacted, mooting the case.