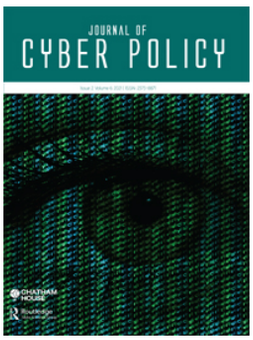

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

The European Union-United States cybersecurity relationship: a transatlantic functional cooperation

Dimitrios Anagnostakis

To cite this article: Dimitrios Anagnostakis (2021) The European Union-United States cybersecurity relationship: a transatlantic functional cooperation, Journal of Cyber Policy, 6:2, 243-261, DOI: 10.1080/23738871.2021.1916975

To link to this article: https://doi.org/10.1080/23738871.2021.1916975

Published online: 22 Apr 2021.

JOURNAL OF CYBER POLICY
2021, VOL. 6, NO. 2, 243–261
https://doi.org/10.1080/23738871.2021.1916975

Routledge
Taylor & Francis Group

The European Union-United States cybersecurity relationship: a transatlantic functional cooperation

Dimitrios Anagnostakis

Department of Politics and International Relations, University of Aberdeen, Aberdeen, UK

ABSTRACT

This article explores the European Union (EU)-United States (US) cybersecurity relationship through an international relations perspective focusing on threat perceptions and interests, principles and norms and institutions. It uses data from publicly available EU and US documents and speeches and from three interviews conducted by the author with EU officials. The main argument of this research is that the transatlantic security relationship is not in a process of rift with regard to cybersecurity; cooperation and coordination continues despite the broader political disagreements that arise from time to time. The EU and the US share common threat perceptions and interests, they converge around a number of cybersecurity principles and norms, and they coordinate their actions in practice. In other words, the EU-US cybersecurity relationship has taken the form of a functional cooperation which aims at safeguarding common interests and avoiding the costs and the vulnerabilities that arise from the EU-US interdependencies in the cyber realm. At the same time, not all policy areas related to cybersecurity have been equally prioritised by the two actors.

ARTICLE HISTORY
Received 6 August 2020
Revised 13 January 2021
Accepted 9 March 2021

KEYWORDS
Transatlantic relations; cybersecurity; European Union; EU-US relations; cybercrime

Introduction

In August 2019, 15 years after the publication of Kagan's polemic *Of Paradise and Power* (Kagan 2004) which painted a bleak picture of transatlantic relations, the President of the United States (US) Donald Trump mentioned that 'the European Union (EU) is worse than China' (Reuters 2019). In a similar remark in 2018, he stated that the EU is one of the largest foes of the US with regard to international trade. In the cyber realm, the US president threatened that the US would stop sharing intelligence with any European country that continued to rely on the Chinese company, Huawei for their telecommunications needs and networks. These developments have brought again into the surface questions about whether we are witnessing a transatlantic rift and about the health of the transatlantic security relationship. Similar questions had previously emerged in the period after the 9/11 terrorist attacks. During the same period, however, the cooperation between the EU and the US on internal security issues has expanded significantly (Rees 2006; Anagnostakis 2017). As the EU developed more competences in these areas, which were mostly

CONTACT Dimitrios Anagnostakis dimitrios.anagnostakis@abdn.ac.uk

covered by the EU's Justice and Home Affairs policies, there was a parallel increase in the EU-US interactions in the same field (Peterson 2016, 102; Anagnostakis 2016; Ilbiz, Kaunert, and Anagnostakis 2017).

Concerning cybersecurity in particular, since the late 2000s there are increased interactions between the EU and the US in this field which has, as a result, emerged as a separate policy area in the broader EU-US relations (Christou 2016). The two actors established a 'Working Group on Cybersecurity and Cybercrime' in 2010 (European Commission 2010) and since then the EU and the US have included in their discussions issues 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 (White House 2014).

Therefore, a research puzzle emerges from the above as to what this internal security cooperation and the EU-US cybersecurity relationship in specific mean with regard to the state of the transatlantic security relationship. On the one hand, there have been significant political differences and tensions between the EU and the US, one of the latest being the issue of 5G security and 5G vendors. On the other hand, the EU and the US have at the same time elevated cybersecurity as a key issue of their bilateral relationship. Therefore, the aim of this article is to investigate what this apparent paradox means for the transatlantic relationship and to explore how the EU and the US cooperate with each other in the field of cybersecurity with a particular focus on the EU-US institutions.

This article dismisses the notion of a transatlantic rift and it argues that the EU-US cybersecurity cooperation is sustained and based on common interests and threat perceptions and on the desire of cybersecurity professionals and officials from both sides to systematically engage with each other in this policy area. The day-to-day cybersecurity cooperation between the two actors has been shielded from the occasional friction caused by political developments and disagreements. In other words, the EU and the US have established a functional cybersecurity cooperation based on the aim of the two sides to manage their cybersecurity interdependencies and to create an institutional space where future conflicts that may arise could be discussed and solved.

Regarding data sources, this research has used publicly available EU and US documents and reports, news/media sources, and speeches from EU and US officials. In particular, the various websites of the relevant US and EU departments and agencies were searched using keywords and phrases (e.g., 'transatlantic cybersecurity', 'transatlantic relations', etc.) related to the researched topic. The 'Lexis Library (LexisNexis)' database was similarly used to search for news/media sources relevant to the research question. The documents collected in that way were then filtered on the basis of the presence of data which is linked to this article's research question.

The use of documents has been triangulated with data from three semi-structured elite interviews with officials from the European Union that took place in November 2018 in Brussels. Interviewing elites is one of the most effective ways for researchers to collect data on decision-making processes as well as information that would be otherwise difficult to find through other sources. The underlying assumption is that there are certain people who are more knowledgeable regarding the researched topic and had more influence than others in the decision-making or negotiating procedure examined.

The first step was to identify the persons to be interviewed. The aim was to interview the officials who had a direct role in the EU-US cybersecurity relations. Through the

Commission's official directory of employees, the websites of the relevant bodies and units of the EU, and the organisation charts of these units, a number of EU officials were identified who, given the position they held, could be knowledgeable about the researched topic. Pierce's suggestion to 'aim higher rather than low by approaching the "A-list" elites rather than lesser elites' (Pierce 2008, 121) who may be considered more approachable was also followed. E-mails with interview requests were, therefore, sent to eight EU officials; four of the officials declined the request, one of them did not reply, and three gave a positive reply. In particular, two officials working in the European Commission and one official working in the European External Action Service (EEAS) were interviewed. All the interviewees have been involved in the EU-US cybersecurity relations and have, as a result, a deep knowledge of this particular policy area.

While the small number of interviews can be a potential limitation for this research, this limitation has been largely overcome by using EU and US documents and reports that are publicly available. Moreover, when interviewing elites who are involved in a very specific policy area, there are only a few people who occupy this position and to whom one can send interview requests. Additionally, a potential limitation related to the scope of this article is that this research does not look in detail at the positions and views of the European Parliament; however, this body is not directly involved in the work of the EU-US cybersecurity institutions, and a detailed examination of the views of the European Parliament on transatlantic relations in general would require a separate research.

This article employs as a conceptual guide for the exploration of the EU-US cybersecurity relationship a security communities' approach, which is derived from the International Relations literature, and which focuses on common interests and threat perceptions, principles and norms and institutions. Karl Deutsch was the first to conceptualise the North Atlantic area as a pluralistic security community with his seminal work *Political Community and the North Atlantic Area* (Deutsch 1957). One of the key strengths of the security communities' approach is that it can be used as a heuristic tool to guide research and to make useful observations based on it (Adler and Barnett 1998). Especially regarding the transatlantic area, this framework can be used to assess empirically the security community's situation 'against the background of the reported rifts in Transatlantic relations' (Ditrych 2014, 261).

Interests are defined here as 'preferences over outcomes' (Hasenclever, Mayer, and Rittberger 1997, 32). Principles are beliefs of fact or causation while norms are 'standards of behaviour defined in terms of rights and obligations' (Hasenclever, Mayer, and Rittberger 1997, 32). Finally, security communities are also associated with increased transactions between their members, policy coordination, cooperation and social learning through a dense network of institutions, and a sense of togetherness.

Neither the EU cybersecurity strategy nor the US national strategy on cyberspace define explicitly the term 'cybersecurity'. However, both documents refer to a similar set of 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.[1] The emphasis of this article is, therefore, on the EU-US cooperation on these issues[2] with the exception, however, of the EU-US relationship in the area of cyber defence which is so far very little developed. Similarly, this article does not look at the EU-NATO cooperation which has emerged only very recently and has focused predominantly on cyber defence rather than on issues such as cybercrime and internet governance.

The next section examines the EU-US cybersecurity threat perceptions and interests and principles and norms. It is followed by an analysis of the EU-US institutions that have emerged in the policy area of cybersecurity and the EU-US policy coordination in the same field.

Threat perceptions and interests

By the end of the 2000s there was an increasing awareness about cybersecurity threats at the EU level resulting in the publication of the first cybersecurity strategy of the EU in 2013 (European Commission 2013), the enhancement of the European Network and Information Security Agency (ENISA) which was established in 2004, and the initiatives of the Commission regarding the Network and Information Security (NIS) Directive.[3] The EU's cybersecurity strategy focused, among others, on the economic costs that cyberattacks and cybercrime inflict on the EU member states and societies due to the reliance of energy, transport, health and financial systems on digital platforms and computer networks (Jones 2012; Kroes 2013), and the predominant EU framing of cybersecurity was that of 'resilience' (Christou 2016; Carrapico and Barrinha 2017).

Moreover, the cyberattacks against Estonia in 2007 and against Georgia and Lithuania in 2008 were crucial in galvanising the efforts of the EU to establish a more coherent and holistic approach to cybersecurity (European Commission 2009). More recently, ENISA has been strengthened with the 2019 'EU Cybersecurity Act', and cybersecurity has been included in the EU's Joint Framework on countering hybrid threats in which particular attention is paid to cyberattacks against financial, energy and transport systems (European Commission 2016).

The US policy documents and strategies have focused on threats similar to those identified in the EU reports and they speak the same language with regard to cybersecurity. In 2003 the first US national strategy for securing the cyberspace was published (White House 2003) highlighting, among others, the vulnerability of critical infrastructures and the importance of fighting cybercrime. The 2009 Cyberspace Policy Review was even more alarming stressing that 'cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century' and that the 'status quo is no longer acceptable' (White House 2009). The administration of Barack Obama placed cybersecurity at the top of the US policy agenda and its priorities were similar to those of the EU: protection of critical infrastructure, sharing information about breaches and security gaps, international cooperation, and engaging with the private sector (Pellerin 2015).

The cybersecurity policies of the Donald Trump administration have continued along similar lines. In May 2017 the US President signed the 'Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure' (White House 2017) which implemented policies and plans that were initiated by the previous administration. Moreover, the EU and US officials highlighted in their meetings in 2017 the importance of enhancing and continuing their cybersecurity cooperation in issues such as the fight against cybercrime and their policy coordination in multilateral settings (Council of the EU 2017; US Department of Homeland Security 2017). This was also stressed by two EU officials who were interviewed by the author and who mentioned that the change of the US administration did not have any major impact on the EU-US cybersecurity

cooperation given that the cybersecurity officials from both sides shared the same concerns and the same goals and aims (Interview 2; Interview 3).

On the basis of the above shared threat perceptions the EU and the US have coalesced around three common interests. The first one is the interest of both parties to avoid conflicting standards. The fact that the EU and the US economies are closely interlinked with each other creates the danger of having multiple and fragmented cybersecurity standards in the transatlantic area (Council of the EU 2015). The importance of cybersecurity for trade can be seen in the emphasis that the US Chamber of Commerce has placed in the EU-US cybersecurity relationship and the establishment of compatible standards (US Chamber of Commerce 2017). Therefore, a common interest between the EU and the US is to establish the interoperability of their respective digital systems and platforms (for the management of critical infrastructure, for instance) and cybersecurity frameworks ensuring in this way that trade is not impeded (Jones 2012; Kroes 2013). In other words, and from a functionalist perspective, the existence of cross-border transatlantic interdependencies between digital service providers and operators of essential services have pressured the EU and the US to establish processes through which they can manage these interdependencies and reduce the associated risks.

A second incentive for the EU-US cybersecurity relationship is the interest of the EU and the US in shaping the global standards for cybersecurity and the realisation that only by their combined weight the EU and the US can effectively shape the global cyber agenda and the cybersecurity rules and policy responses that have started to emerge (Council of the EU 2015). For example, a central aim of the EU-US cybersecurity cooperation has been the promotion of the Council of Europe's Convention on Cybercrime (Budapest Convention) (Council of Europe 2001), and the two sides have worked together in the United Nations trying to avoid a dilution of this treaty as shown below in this article.

Finally, the EU-US cybersecurity relationship has also been shaped by the conflict between the EU and the US, on the one hand, and Russia and China on the other on issues related to cybersecurity, internet governance and human rights on the internet. In the context of the competition for the establishment of global standards, the EU and the US have resisted the efforts of Russia and China to control and censor internet content and to undermine the current multi-stakeholder internet governance model replacing it with more intergovernmental and state-centric structures (Pritzker 2016; European Political Strategy Centre 2017; Taylor and Hoffmann 2019, 13).

In particular, both the EU and the US have placed importance on jointly promoting the multi-stakeholder internet governance model (Andrianavaly 2012) in which the private sector and the digital industry play an important role and which is institutionalised through organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (Taylor and Hoffmann 2019, 6–7).[4] Russia and China, however, have aimed to increase governmental control over the internet and to promote alternative venues for the management of the internet (for example, the International Telecommunications Union) (Hurwitz 2014; Pritzker 2016). Moreover, while Russia and China have insisted on states having broad discretionary powers to censor and block online material that could stir domestic unrest (Hurwitz 2014, 237–238) the EU and the US have emphasised the importance of a free and open internet for democracy promotion and the empowerment of civil society. Referring to Russia's and China's emphasis on censorship and the two countries' aim to increase

state control of the internet, the US Secretary of Commerce stressed in 2016 that 'we must not let that happen' (Pritzker 2016). Similarly, the US National Cyber Strategy of 2018 (White House 2018) has referred to China and Russia as potential adversaries in the cyber realm.

All of the above show that the EU and the US have shared common threats with regard to cybersecurity as well as common interests: avoiding fragmented and conflicting standards, shaping global standards, and resisting Russia and China. However, while the convergence of interests is a positive indicator for the health of the transatlantic security community this convergence is not enough on its own to ensure the long-term maintenance and vitality of this cooperation. A vibrant cooperation on security issues is also characterised by at least a 'modest coordination of security policies', increased interactions, and the emergence of a 'dense network of relations' in the form of institutions and common principles and norms (Adler and Barnett 1998, 50, 53). The following section explores and analyses these indicators in the context of the EU-US cybersecurity relationship.

Principles and norms

This section shows that the EU and the US share a common set of general principles with regard to cybersecurity. The specific norms that have emerged out of these principles focus on different aspects of cybersecurity, namely the fight against cybercrime, the protection of critical digital infrastructure, human rights and internet governance.

Firstly, the EU and the US agree on the principle that international cooperation is a central element of cybersecurity (European Commission 2011; US Department of State 2016). In particular, the EU's cybersecurity strategy has mentioned that one of the strategic priorities of the Union is establishing an international cyberspace policy and cooperating with international partners on issues related to cyberspace and cybersecurity. The US is the only country that is explicitly mentioned in this strategy; cooperation with Americans is described as 'particularly important and will be further developed' (European Commission 2013, 15). A particular norm that follows from this principle is that states should cooperate with each other on investigating and fighting cybercrime. This norm is operationalised through the joint EU-US support for the Council of Europe's 'Budapest Convention' which has been the first multilateral legal treaty on cybercrime.

Secondly, the EU and the US share the principle that the involvement of the private sector is crucial for cybersecurity (EU-US Working Group 2011; Malmström 2012). The specific norm that follows from this principle is that the private sector has a responsibility to engage with states and international organisations in the formation of cybersecurity risk management frameworks for critical infrastructure and to implement these frameworks as effectively as possible.[5] The key technology giants (for example, Microsoft, Apple, and Amazon) themselves have spent during the last years massive amounts of money on lobbying in Brussels, especially regarding data protection issues and cyber governance.

Thirdly, a common principle shared by the EU and the US is that cybersecurity should not come at the expense of fundamental rights and freedoms (White House 2011; Council of the EU 2015). Therefore, two interrelated norms that follow from this principle are first, that cybersecurity measures should not undermine fundamental rights and freedoms and

second, that the violation of human rights online, such as, for example, internet censorship and the suppression of the freedom of expression, is not acceptable. Particular emphasis is placed on the freedom of expression and the free flow of information (Schaake and Vermeulen 2016). The Council of the EU has adopted the 'EU Guidelines on Freedom of Expression Online and Offline' and one of the aims of the US-EU Cyber Dialogue is the close coordination of the EU and US policies on the promotion and protection of human rights online in international forums such as the 'Freedom Online Coalition' (White House 2014).

Finally, a fourth common transatlantic principle is the support of both actors for the current multi-stakeholder governance model for the management of cyberspace and the internet, as mentioned previously. The EU and the US converge on the norm that internet governance should be regulated through a mixture of state and industry and private sector involvement rather than through direct and heavy-handed governmental control as Russia and China suggest.

The above shared principles and norms can also facilitate the emergence of a common transatlantic cybersecurity identity. Identities are relational, and they are shaped not only by the interactions between the members of a community or group, but also by the interactions with the actors that are placed outside the boundaries of the community (Adler and Barnett 1998, 47). The last two principles, namely, finding a right balance between security and the protection of fundamental freedoms and protecting the current multi-stakeholder model of internet governance put the EU and the US in a collision course with the states that have antithetical views; two of the most important of these states are Russia and China which have built coalitions of like-minded states in the field of cybersecurity through the activities and initiatives of the Shanghai Cooperation Organization (Malmström 2013). Therefore, the convergence of the EU and the US principles and norms through the joint focus on international cooperation, the involvement of the private sector, finding a right balance between security and fundamental human rights, and protecting the current multi-stakeholder model of internet governance can also facilitate the emergence of a normative 'glue' that binds the EU and the US together.

The EU-US cybersecurity institutions and policy coordination in practice

A question that follows from the above examination of the transatlantic cybersecurity norms and principles is whether the two actors have made any progress in promoting and implementing these norms in practice. In terms of the security communities literature, institutions and working groups may facilitate socialisation, social learning, trust building, and the consolidation of common identities. They also facilitate the establishment of a 'dense network of relations' through which at least a 'modest coordination' of the participating actors' policies can emerge (Adler and Barnett 1998, 50, 53).

In practice, the EU and the US have established two key institutions in order to discuss their policies and potentially coordinate their actions: the EU-US 'Working Group on Cybersecurity and Cybercrime'[6] (EU-US WG) and the EU-US 'Cyber Dialogue'.[7] A number of US agencies, such as the Federal Bureau of Investigation (FBI) and the Secret Service, have also intensified their cooperation on operational matters with Europol's European Cybercrime Centre (EC3).

The EU-US Working Group on Cybersecurity and Cybercrime was established in 2010 after the EU-US Summit of November 2010 in Lisbon, and it had five priority areas: (1) Cyber Incident Management; (2) Public-private Partnerships; (3) Awareness Raising; (4) Cybercrime; and (5) Outreach (EU-US Working Group 2011, 7). The aims of the two sides are to share and exchange good practices, to develop common plans and compatible approaches, to prepare reports and briefings, to establish common principles and guidelines, and to coordinate their activities. The first meetings of this group focused on internet governance and the fight against the sexual abuse of children online (Jones 2012). By the time of the establishment of this group the US agencies were already cooperating with Europol on operational matters.

The EU-US Cyber Dialogue started its work in December 2014 and its mission was more oriented towards the strategic aspects of global cybersecurity and the coordination of the two actors' foreign policies on cyber issues (White House 2014). In particular, it focuses on international cyberspace developments, the promotion and protection of human rights online, cybersecurity capacity building in third countries, and international security issues, such as the establishment of norms of behaviour and confidence building measures in cyberspace and the application of existing international law in cyberspace (White House 2014).

In terms of the realisation of the deliverables in the five priority areas identified by the EU-US working group, the situation is mixed differing from one sub-field of cybersecurity to another. The two sides launched in 2012 the 'Global Alliance Against Child Sexual Abuse Online' which brought together 54 countries and which aimed to enhance these countries' fight against the sexual exploitation of children online. This initiative was a direct product of the EU-US working group, and it is considered one of the most successful outcomes of the EU-US cybersecurity cooperation and an effective EU-US promotion of the norm that states should cooperate with each other in investigating and fighting cybercrime (Interview 3). In the subsequent meetings a number of operational targets were set for the governments to fulfil and these were monitored through progress reports. This project, which later merged with the UK's initiative 'We Protect', was described by a Commission official as an 'outstanding' product of the EU-US working group on cybersecurity and as a good example of how the two sides can shape global standards in this policy area (Interview 3). Similarly, another Commission official presented the technical tools and the 'Notice and Take Down' (NTD) standards which were developed in the context of the Global Alliance as deliverables which stemmed directly from the cooperation that was taking place in the EU-US cybersecurity institutions (Andrianavaly 2012).

One of the aims of the EU-US working group on cybersecurity and cybercrime has also been the coordination of the EU and US efforts in order to get a number of law enforcement recommendations endorsed by the Governmental Advisory Committee of ICANN (Jones 2012, Interview 1). These recommendations were related to the misuse of internet domain names and IP addresses for illegal purposes, and on that occasion the EU was cooperating very closely with the FBI (Interview 1). The recommendations were finally supported by the ICANN and the private sector, and the then EU Commissioner for Home Affairs, Cecilia Malmström and the EU official, Valérie Andrianavaly have presented this development as a direct result and outcome of the EU-US cooperation in the context of the cybercrime and cybersecurity working group (Andrianavaly 2012; Malmström

2012). Similarly, one of the EU officials interviewed by the author stressed that in this case the EU-US cybersecurity cooperation resulted in a 'direct and very tangible benefit' (Interview 1). In other words, this has been an additional successful effort of the EU and the US to promote and act on the cybersecurity principles and norms which guide their cybersecurity relationship.

An additional aim of the EU-US working group and a frequent topic of the EU-US is the promotion of the Budapest Convention on Cybercrime and the encouragement of both EU and non-EU states to become parties or to ratify the convention; this particular aim follows directly from the shared EU-US norm that states should cooperate with each other in the fight against cybercrime. In addition to the EU states which ratified the treaty in the 2000s (i.e. Finland, France, Germany, Hungary, Italy, Romania, etc.), by 2013, Austria, Belgium, the Czech Republic, Malta, Spain, Portugal and the United Kingdom from the EU, and Australia, the Dominican Republic, Japan, Georgia, Montenegro and Switzerland had ratified the convention. The US and EU officials have presented this progress as a success directly linked to the EU-US coordination and joint pressure towards laggard states (Malmström 2013; Daniel 2013). For example, the EU and the US have focused on joint outreach campaigns and on organising meetings with like-minded countries such as Japan and South Korea (Interview 2; Interview 3). Additionally, at the UN level the EU and the US work together at the various groups of intergovernmental experts and they aim to give the same message and to coordinate with each other when drafting resolutions (Interview 2; Interview 3). For example, in a General Assembly discussion in December 2019 on Russia's proposal for an alternative treaty against cybercrime the EU and the US representatives spoke one after the other and they used similar language and suggestions. Finland, speaking on behalf of the European Union, stressed that 'the process to establish a new international legal instrument on cybercrime would duplicate existing work and pre-empt the conclusions of the existing open-ended intergovernmental Expert Group … ' (United Nations General Assembly 2019). Similarly, the US representative mentioned that the proposed Russian resolution 'prejudges the outcome of the existing work of the Expert Group' and that 'it will undermine the work of the Expert Group before it completes its 2018–2021 work-plan and offers its recommendations to Member States' (United Nations General Assembly 2019). At the same time, in the EU-US Ministerial Meeting on Justice and Home Affairs that took place in December 2019, the two sides 'discussed the importance of making swift progress' regarding the Second Additional Protocol of the Budapest Convention 'which remains the instrument of choice for international cooperation on cybercrimes for both the EU and the United States' (Council of the EU 2019a).

Therefore, the EU and the US do not only converge rhetorically on the importance of the Budapest Convention for the fight against cybercrime but they also coordinate their efforts in practice and they act jointly in order to promote this standard internationally. Apart from a transatlantic agreement on the substantive content of the treaty, the statements of the US and the EU representatives in the UN General Assembly which are cited above also reveal a functionalist logic behind their support for the Budapest Convention; the EU and the US have stressed that the Budapest Convention is so far the only international legal instrument regarding cybercrime and, therefore, negotiating a new treaty, as Russia and China have suggested, would be a time-consuming procedure which would significantly impede the global fight against cybercrime.

Regarding the norm that the private sector and the cybersecurity industry have a responsibility to engage with states and international organisations in the formation of cybersecurity risk management frameworks, the EU and the US have aimed to establish minimum standards on cybersecurity for the private sector and a general culture of awareness concerning cyber risks. In particular, the EU-US working group on cybersecurity and cybercrime stressed in its 2011 Concept Paper that the two parties will develop compatible approaches to public-private partnerships (PPPs) and that the issue of PPPs is especially important given that it 'cuts across all other priority areas' of the working group (EU-US Working Group 2011, 2).

Contrary to the other aspects of the EU-US cybersecurity relationship, little progress has been made in this area in terms of direct EU-US institutional relations. The US National Institute of Standards and Technology's (NIST's) 'Framework for Improving Critical Infrastructure Cybersecurity' and the EU's 'Network and Information Security' (NIS) Directive were established in 2014 and 2016 respectively. In particular, in 2015 a number of officials from NIST visited the EU and presented their cybersecurity framework to their EU counterparts (Interview 1). This was followed by a workshop between the US Department of Homeland Security and the EU Commission on the same topic (Interview 1).

However, most of the EU-US interactions in this policy issue have followed a pattern of voluntary adoption and imitation of each other's practices rather than a pattern of systematic and sustained relations within an institutionalised setting. For example, ENISA's framework for mapping the interdependencies of Operators of Essential Services (OES) and Digital Service Providers (DSPs) is partly based on the US NIST's cybersecurity framework and indicators (ENISA 2018a). Similarly, the Information Sharing and Analysis Centers (ISACs) which are supported by ENISA were originally established in the US in the 1990s (Interview 1; ENISA 2018b, 7). This was also one of the suggestions of the US Chamber of Commerce, namely that the EU should adopt elements of the NIST platform in its implementation of NIS, given that the two sides' 'approaches to cybersecurity are aligned in essential ways' (US Chamber of Commerce 2017). Moreover, according to one of the EU officials interviewed by the author, on the issue of public-private cybersecurity partnerships there have been more meetings and interactions with representatives from US Information and Communications Technology (ICT) companies who are engaged in lobbying work in Brussels rather than with officials from the US (Interview 1). In other words, the EU learns from the US but this does not necessarily happen through a formalised institutional framework; according to the same interviewee, 'all the information [about the US approaches to public-private partnerships] is publicly available' and at the same time the EU officials and representatives from US companies interact frequently with each other and exchange ideas in conferences, meetings and workshops.

Therefore, on the one hand there has been a rhetorical convergence of interests on the issue of public-private partnerships and risk management frameworks but no sustained policy coordination in practice. This lack of sustained EU-US institutional cooperation in this issue has been partly due to the two actors' prioritisation and focus on the fight against cybercrime and the promotion of the Budapest Convention (Interview 1). The change in the 'personal constellations' (Interview 1) within the EU-US groups has also played a role, highlighting the issue of continuity when institutions rely too much on personal contacts for their effective functioning. Moreover, the Commission has focused primarily on consolidating the NIS Directive within the EU (Interview 1). On the other hand,

there is evidence of learning; this learning has taken place more through a process of voluntary imitation of standards and through an exchange of best practices with non-governmental cybersecurity professionals and experts, rather than through the formalised EU-US institutionalised settings.

Finally, Europol's European Cybercrime Centre has become the hub for the EU-US operational cooperation on cybersecurity matters (Council of the EU 2017). In December 2016 Europol and European law enforcement agencies together with their American counterparts launched operation 'Avalanche' which aimed to take down one of the biggest cybercrime enterprises to emerge, involving more than 30 different jurisdictions and 20 different firms (Wainwright and Cilluffo 2017). The preparation for this operation took four years and the victims of this cybercrime enterprise were located in more than 180 countries. A similar success was the joint operation against the botnet 'GameOver ZeuS' and the 'CryptoLocker' ransomware which inflicted economic damage of more than $100 million (Europol 2014). Similar operations in which the FBI and the Secret Service took part together with European agencies and Europol were the targeting of the 'Shylock' malware in 2014 and the 'Beebone' and 'Simda' botnets in 2015 and the dismantling of a credit card fraud network in 2017 (Europol 2017). The announcements that accompany these successful joint operations often emphasise the economic damage that cybercrime inflicts upon the US and the EU economies and the need for continuous and close transatlantic cooperation against cybercrime given that the EU and the US are so closely linked in terms of trade and digital platforms. This emphasis on the transatlantic interdependencies and the common EU-US vulnerabilities in the cyber realm as the key driver of the EU-US cooperation strengthens the argument that the main form that the EU-US cybersecurity relationship has taken is that of essentially a functional cooperation based on common interests.

In general, the EU-US cybersecurity institutions have created an environment in which policy officials can share expertise and experiences and exchange views on how to address common problems (Interview 2; Interview 3). In other words, these groups have become venues through which learning and mutual influence can take place. For example, according to the former EU Commissioner, Cecilia Malmström, the EU-US talks helped create the necessary impetus for the development of the cybersecurity strategies of the EU and of the EU member states, and these strategies were partially inspired by elements of the US approach to cybersecurity (Malmström 2013). Various ideas that have become part of the EU cybersecurity agenda have been imitated from the US, as shown previously in this article (Interview 1). This aspect of the EU-US relationship, namely that transatlantic relations become the catalyst of further EU integration, has been a common feature of the EU-US internal security cooperation since the 9/11 terrorist attacks (Anagnostakis 2017).

Cutting across the above areas of cooperation is the function of the various EU-US cybersecurity groups and the EU-US institutions in general as forums in which the two sides can present to each other their respective policies and plans before they are implemented (Interview 2; EU-US Working Group 2011). This joint reflection on future policies aims to reduce friction between the two sides which has been caused in the past by unilateral measures taken without prior consultation (Interview 2). The functioning of the EU-US cybersecurity institutions as mechanisms for the solving of potential problems

arising, for example, from the EU-US interdependencies in this area suggests again that the EU-US cybersecurity relationship has taken primarily a functionalist form.

The Snowden leaks and the case of the WHOIS database

Two examples of how the EU-US institutions functioned as tension-diffusing mechanisms are the case of the revelations of Edward Snowden about the surveillance tactics of the US National Security Agency (NSA) and the EU-US differences on data protection issues in general.[8] While these issues created an atmosphere of distrust at the political level they did not have any significant or long-term impact on the cybersecurity cooperation of the two sides on topics such as the fight against cybercrime or the protection of critical infrastructure. (Interview 2; Interview 3). In a EU-US meeting on 18 November 2013, in the immediate aftermath of the Snowden revelations, the EU was stressing that while there was a need to restore confidence, practical cooperation should continue and 'negotiations on trade and on judicial cooperation should move forward' (Council of the EU 2013). The EU also highlighted that cooperation in the context of the EU-US Working Group on cybersecurity and cybercrime was successful and that 'thanks to law enforcement cooperation with the FBI and ICE, several networks have been dismantled' (Council of the EU 2013). Similarly, while Germany, which was the largest target of the NSA surveillance programme, was arguing initially in favour of establishing 'digital data sovereignty' in the EU these plans did not receive much support in Europe at that time.[9] In practice, the EU-US cybersecurity cooperation continued unabated as the subsequent joint operational successes demonstrated. While there was initially distrust at the political level this distrust did not trickle down to the lower working level where there was a common interest to continue data flows, information exchanges and operational cooperation, and where both sides were stressing that 'we have to get things done' (Interview 2; Interview 3). In other words, cooperation on cybersecurity issues such as the fight against cybercrime has so far remained compartmentalised.

An issue that has recently caused some friction between the US and the EU has been the effect of the EU's General Data Protection Regulation (GDPR), which came into force in 2018, on the WHOIS database of ICANN. The WHOIS database collects information from domain registrars about the owners of internet domains and is routinely used by law enforcement authorities for their investigations. The entry into force of GDPR has put the domain registrars in a difficult position, given that if they transfer information about domain owners to WHOIS they are at risk of being fined from the national data protection authorities and national courts within the EU (Taylor 2018). Not only the law enforcement authorities of the US but also those of the EU member states are dissatisfied with this situation arguing that it hinders law enforcement (Politico 2020). The issue of WHOIS reform in general has been one of the priorities of the EU's Renewed Internal Security Strategy (2015–2020) and it has been followed closely by two EU groups: the 'Horizontal Working Party on Cyber Issues' and the 'High Level Group on Internet Governance' (Council of the EU 2020). The clash between GDPR and WHOIS is still an ongoing issue but ICANN has already initiated a number of temporary and transitional measures, such as the Phase 2 Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD (generic Top Level Domain) Registration Data (ICANN 2019), and consultations are taking place between EU representatives and ICANN stakeholders (Council

of the EU 2020, 14).[10] Moreover, the issue of WHOIS data is included in the new EU proposal for a Directive that builds on and repeals the EU's NIS Directive; this update Directive specifies that member states should ensure that the databases of domain name registration data have accurate and relevant data about the holders of domain names, that domain name registration services 'respond without undue delay to all requests for access', and that at the same time there is compliance with EU data protection law (European Commission 2020a). Similarly in the case of the Snowden leaks, the broader EU-US relationship has remained unaffected; for example, the EU and the US have recently started negotiations on an agreement which will facilitate access to electronic evidence in criminal investigations (Council of the EU 2019a, 2019b).

The case of Huawei

An additional issue that has caused friction between the EU and the US since 2018 has been the determination of Washington to ban the Chinese telecommunications company Huawei from operating within the country and to persuade the US allies to take similar measures. Despite the confrontational rhetoric of Donald Trump and the aggressive lobbying campaign of the US Secretary of State, Mike Pompeo, the issue of 5G security has been a constant topic of discussion for the EU-US Information Society Dialogue and the EU-US Justice and Home Affairs Ministerial Meetings, and the tone of these talks has been softer; for example, Robert Strayer, who has represented the US in EU-US Information Society Dialogue since at least 2018, referred to the EU measures on 5G security in an approving way in the statements he gave for two Senate hearings. Speaking about the EU's 2019 report on coordinated risk assessment of 5G networks security, Robert Strayer noted that he welcomed this 'assessment and how it clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances in place' (Strayer 2019). He also highlighted that the EU's report 'aligns with the U.S. assessment that you cannot mitigate the risk of untrusted suppliers by limiting them to certain parts of a network' (Strayer 2019).

Similarly, the issue of 5G has been discussed in the bi-annual EU-US Justice and Home Affairs Ministerial Meetings, where participants have shared best practices and informed each other about policy changes. For example, one internal EU document mentions that the EU-US Justice and Home Affairs Ministerial Meeting of June 2019 was a constructive 'opportunity for both sides to discuss ways to expand their cooperation and best practice exchanges in areas like cybersecurity', with a particular focus on the security of 5G networks (Council of the EU 2019c). In the same meeting, the EU and the US briefed each other about their respective initiatives: the EU presented the 5G risk assessments that member states were conducting while the US talked about its initiatives on international benchmarks for the security of 5G networks.

Moreover, while the EU did not advocate for an outright ban of Huawei, as early as in December 2018 the EU Commissioner, Andrus Ansip was noting that 'we have to be worried' about Huawei (Politico 2018). In the same month, more than one thousand hacked EU documents were leaked to the newspaper, the *New York Times*, which stated that hackers allegedly linked with the Chinese army managed to infiltrate the EU communication systems and collected classified information for years. The European

Commission had already commissioned a study on industrial espionage and cyber theft of trade secrets which was finally published in December 2018 and which made extensive mention of the activities of Chinese hackers (allegedly state-sponsored). Similarly, in March 2019, the Commission submitted a report to the European Council titled 'EU–China – A strategic outlook' which highlighted that in some policy areas China is a 'systemic rival' (European Commission 2019). The report also stressed that foreign investment in strategic sectors, such as in 5G networks, 'can pose risks to the EU's security'. The EU member states shared in general these threat perceptions although the security measures that were proposed by national governments differed in their strictness.

In the course of two years (2019–2020), the Commission introduced a Recommendation on the cybersecurity of 5G networks (March 2019); the member states published a report on the EU coordinated risk assessment of 5G networks security (October 2019) which highlighted that 'threats posed by States or State-backed actors, are perceived to be of highest relevance … [and] they represent indeed the most serious as well as the most likely threat actors' (NIS Cooperation Group 2019); ENISA published a report on the threat landscape for 5G Networks (November 2019); and finally the Commission launched a toolbox on 5G security (January 2020) which urged the EU member states to specify and implement security measures and risk mitigation criteria for 5G vendors.

Both the EU's toolbox and its implementation by the member states have gained praise from the US, with the US Secretary of State mentioning in July 2020 that 'there is a transatlantic awakening' to the threat posed by China (US Department of State 2020). Moreover, in August 2020, the US launched its 'Clean Network' initiative which is an effort by Washington to promote its risk management criteria for telecommunications networks and services, such as 5G networks or cloud computing, abroad. The EU's toolbox became part of the Clean Network and the two actors issued a joint declaration in October 2020 highlighting 'their commitment to shared principles on 5G security and the synergies between the EU 5G cybersecurity Toolbox and the Clean Network' (European Commission 2020b).

Conclusion

This article has focused on the interests and threat perceptions, the principles and norms, and the institutions of the EU and the US in the field of cybersecurity. The central argument of this research and the main answer to the article's research question is that there has been no rupture of the EU-US relationship in this policy area and no transatlantic rift. On the contrary, the EU and the US interests and threat perceptions converge; there is a common basis of shared cybersecurity principles and norms; and cooperation and coordination continue despite the broader political disagreements that may arise from time to time. Cooperation on the various cybersecurity issues of common importance has remained compartmentalised through the use of transatlantic institutions as communication channels.

The data from the various reports and strategies, from the documents from the EU-US institutional meetings, and from the interviews of EU officials with the author also shows that so far the main driver of the EU-US cybersecurity cooperation has been the functional logic of safeguarding common interests and avoiding the costs and the vulnerabilities that arise from the EU-US interdependencies in the cyber realm. More importantly,

there is evidence that the EU and the US have moved beyond rhetoric alone and they coordinate their policies and actions on issues such as the promotion of the Budapest Convention and the fight against cybercrime. However, less progress has been made on the issue of public-private partnerships.

In terms of identities and values, the transatlantic emphasis on human rights online, the joint efforts of the EU and the US to thwart the Russian and Chinese attempts to promote a model of internet governance based on state-control and censorship, and the occasional references of the EU and the US to their shared culture and values indicate that there is also some degree of a 'sense of togetherness' and common identity.

An additional issue that can be explored in the future is the EU-NATO cybersecurity cooperation with its focus on cyber defence, which has started growing since 2016. Moreover, given the EU's initiatives in the field of fighting hybrid threats over the last few years, it is also worth exploring how the EU's cybersecurity policies and the EU-US cybersecurity cooperation fit within the context of the EU response to hybrid threats, which often materialise through attacks in the cyberspace.

Notes

1. For an overview of the different conceptualizations of the term 'cybersecurity' see the report of the European Network and Information Security Agency 'Definition of Cybersecurity – Gaps and overlaps in standardisation' (ENISA 2015).
2. While one could argue that topics such as the fight against cybercrime and the promotion of the multi-stakeholder model of internet governance are different issues, both the EU and the US put them together in their cybersecurity strategies. They are, therefore, within the scope of this article.
3. The NIS entered into force in August 2016.
4. For the subtle differences between the EU and the US support for the multi-stakeholder model, see Taylor and Hoffmann (2019, 8) and O'Hara and Hall (2018).
5. For a suggested global model of public-private governance for the prevention of the online financing of terrorism, see Ilbiz (2019).
6. Before the creation of this group, cybersecurity issues were discussed in the European Community-US 'Task Force on Critical Infrastructure Protection' that was established after the signing of the 1998 'Agreement for Scientific and Technological Cooperation'.
7. The EU and the US have also established the 'Information Society Dialogue' that focuses on the digital market and the economic aspects of information and communication technologies.
8. A thorough examination of the EU-US differences on data protection is out of the scope of this article.
9. More recently however, the EU has started emphasising more the need for stronger EU cyber and technological sovereignty (Claessen 2020), which is one of the key priorities of the Commission President, Ursula von der Leyen. The Digital Europe Programme, for example, has a budget of €7.6 billion and one of its aims is 'asserting Europe's digital sovereignty' (European Parliament 2020). The European Court of Justice had also ruled in 2016, in a critical case (Tele2 Sverige AB and Watson) about the massive retention of electronic communications data, that the retained data should be stored within the EU, given the high levels of data security and protection required.
10. See the presentation of two Commission officials (DG CONNECT) on the latest development on WHOIS and data protection at a meeting of the EU'S 'High Level Group on Internet Governance', available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=17715. In June 2020 at a meeting of the same group there was an ICANN presentation and discussion on the programme of the upcoming

'ICANN68 Virtual Policy Forum 22–25 June 2020'. The presentation is available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=19491.

Acknowledgements

The author is grateful to the interviewees for sharing their thoughts and insights. The author would also like to thank the anonymous referees for their comments and feedback and the editorial team for their assistance throughout the publication process.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Dimitrios Anagnostakis is a lecturer in the Department of Politics and International Relations at the University of Aberdeen. His research interests cover transatlantic relations and the EU-US relationship, the EU's policies in the area of Justice and Home Affairs, cybersecurity and internet governance, theories of international regimes, and terrorism and counterterrorism. He is the author of a research monograph on the EU-US cooperation on internal security issues (*EU-US Cooperation on Internal Security: Building a Transatlantic Regime*. Abingdon: Routledge, 2017).

ORCID

Dimitrios Anagnostakis http://orcid.org/0000-0001-9153-1664

References

Adler, Emanuel, and Michael Barnett. 1998. "A Framework for the Study of Security Communities." In *Security Communities*, edited by Emanuel Adler, and Michael Barnett, 29–66. Cambridge: Cambridge University Press.

Anagnostakis, Dimitrios. 2016. "Securing the Transatlantic Maritime Supply Chains from Counterterrorism: EU–U.S. Cooperation and the Emergence of a Transatlantic Customs Security Regime." *Studies in Conflict & Terrorism* 39 (5): 451–471. doi:10.1080/1057610X.2015.1108087.

Anagnostakis, Dimitrios. 2017. *EU-US Cooperation on Internal Security: Building a Transatlantic Regime*. Abingdon: Routledge.

Andrianavaly, Valérie. 2012. "EU Policy on Network and Information Security (NIS) and Critical Information Infrastructure Protection (CIIP)." http://slideplayer.com/slide/4545833/.

Carrapico, Helena, and André Barrinha. 2017. "The EU as a Coherent (Cyber)Security Actor?" *JCMS: Journal of Common Market Studies* 55 (6): 1254–1272. doi:10.1111/jcms.12575.

Christou, George. 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London: Palgrave Macmillan.

Claessen, Eva. 2020. "Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU." *Journal of Cyber Policy* 5 (1): 140–157. doi:10.1080/23738871.2020.1728356.

Council of Europe. 2001. "Convention on Cybercrime." Budapest, November 23. *European Treaty Series* 185.

Council of the EU. 2013. "Summary of Conclusions of the EU-US JHA Ministerial Meeting 18 November 2013, Washington." Brussels, 25 November, 16682/13.

Council of the EU. 2015. "Council Conclusions on Cyber Diplomacy." Brussels, February 11, 6122/15.

Council of the EU. 2017. "Outcome of the EU – US Justice and Home Affairs Senior Officials Meeting, Valletta, 1–2 March 2017." Brussels, 21 March, 7163/17.
Council of the EU. 2019a. "Joint EU-US Statement Following the EU-US Justice and Home Affairs Ministerial Meeting." Brussels, December 11, 828/19.
Council of the EU. 2019b. "Criminal Justice: Joint Statement on the Launch of EU-US Negotiations to Facilitate Access to Electronic Evidence." Brussels, September 26, 19/5890.
Council of the EU. 2019c. "Outcome of Proceedings of the EU-US Justice and Home Affairs Ministerial Meeting (Bucharest, 19 June 2019)." Brussels, June 24, 10430/19.
Council of the EU. 2020. "Implementation of the Renewed EU Internal Security Strategy: Joint Presidency Paper." Brussels, February 18, 5618/1/20.
Daniel, Michael. 2013. "Cybersecurity – Strategic-political Aspects of this Global Challenge." http://docplayer.net/2411160-Cybercrime-bedrohung-intervention-abwehr-cybersecurity-strategic-political-aspects-of-this-global-challenge.html.
Deutsch, Karl. 1957. *Political Community and the North American Area: International Organization in the Light of Historical Experience*. Princeton: Princeton University Press.
Ditrych, Ondrej. 2014. "Security Community: A Future for a Troubled Concept?" *International Relations* 28 (3): 350–366. doi:10.1177/0047117814545952.
ENISA. 2015. "Definition of Cybersecurity – Gaps and Overlaps in Standardisation." https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
ENISA. 2018a. "Good Practices on Interdependencies Between OES and DSPs." https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.
ENISA. 2018b. "Information Sharing and Analysis Centres (ISACs) Cooperative models." https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.
European Commission. 2009. "Critical Information Infrastructure Protection – Protecting Europe from Large Scale Cyberattacks and Disruptions: Enhancing Preparedness, Security and Resilience." Brussels, March 30, COM (2009) 149.
European Commission. 2010. "EU-US Summit 20 November 2010, Lisbon – Joint Statement." Brussels, November 20, MEMO/10/597.
European Commission. 2011. "Neelie Kroes Discusses Internet Governance with US Administration." Brussels, May 13, MEMO/11/298.
European Commission. 2013. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Brussels, February 7, JOIN (2013) 1.
European Commission. 2016. "Joint Framework on Countering Hybrid Threats – a European Union response." Brussels, April 6, JOIN (2016) 18.
European Commission. 2019. "EU-China –A Strategic Outlook." Brussels, March 12, JOIN (2019) 5.
European Commission. 2020a. "Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148." Brussels, December 16, COM (2020) 823.
European Commission. 2020b. "Meeting Between US Under Secretary of State Krach and Commissioner Breton on Secure Telecommunications Infrastructure and Digital Agenda." https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/meeting-between-us-under-secretary-state-krach-and-commissioner-breton-secure-telecommunications_en.
European Parliament. 2020. "Digital Europe Programme: MEPs Strike Deal with Council." European Parliament, December 14. https://www.europarl.europa.eu/news/en/press-room/20201211IPR93656/digital-europe-programme-meps-strike-deal-with-council.
European Political Strategy Centre. 2017. "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level." EPSC Strategic Notes, Issue 24. Brussels, May 8.
Europol. 2014. "International Action Against 'GameOver Zeus' Botnet and 'CryptoLocker' Ransomware." Europol, June 2. https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.
Europol. 2017. "Credit Card Fraud in 130,000 Cases: Organised Crime Group Disrupted in European Cross-border Action." Europol, March 14. https://www.europol.europa.eu/newsroom/news/

credit-card-fraud-in-130-000-cases-organised-crime-group-disrupted-in-european-cross-border-action.
EU-US Working Group. 2011. "Concept Paper." https://www.statewatch.org/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf.
Hasenclever, Andreas, Peter Mayer, and Volker Rittberger. 1997. *Theories of International Regimes*. Cambridge: Cambridge University Press.
Hurwitz, Roger. 2014. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36 (5): 322–331. doi:10.1080/10803920.2014.969180.
ICANN. 2019. "GNSO Council Adopts EPDP Final Report on the Temporary Specification for gTLD Registration Data." ICANN, March 4. https://www.icann.org/news/announcement-2019-03-04-en.
Ilbiz, Ethem. 2019. "The Uberization of the United Nations' Regime to Prevent the Online Financing of Terrorism: Tackling the Problem of Obfuscation in Virtual Currencies." *Journal of Cyber Policy* 4 (3): 404–424. doi:10.1080/23738871.2019.1666892.
Ilbiz, Ethem, Christian Kaunert, and Dimitrios Anagnostakis. 2017. "The Counterterrorism Agreements of Europol with Third Countries: Data Protection and Power Asymmetry." *Terrorism and Political Violence* 29 (6): 967–984. doi:10.1080/09546553.2015.1092438.
Jones, Chris. 2012. "'Tackling New Threats Upon Which the Security and Prosperity of our Free Societies Increasingly Depend': The EU-US Working Group on Cybersecurity and Cybercrime." *Statewatch*. http://www.statewatch.org/analyses/no-191-cyber-security.pdf.
Kagan, Robert. 2004. *Of Paradise and Power: America and Europe in the New World Order*. New York: Vintage Books.
Kroes, Neelie. 2013. "Towards a Coherent International Cyberspace Policy for the EU." European Commission, January 30. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_13_82/SPEECH_13_82_EN.pdf.
Malmström, Cecilia. 2012. "The European Response to the Rising Cyberthreat." European Commission, May 2. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_315.
Malmström, Cecilia. 2013. "Next Step in the EU-US Cooperation on Cybersecurity and Cybercrime." European Commission, April 30. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_380.
NIS Cooperation Group. 2019. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.
O'Hara, Kieron, and Wendy Hall. 2018. "Four Internets: The Geopolitics of Digital Governance." Centre for International Governance Innovation. https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance.
Pellerin, Cheryl. 2015. "Obama to Propose Initiatives That Fill US Cybersecurity Gaps." US Department of Defense, January 13. https://www.defense.gov/News/Article/Article/603918/obama-to-propose-initiatives-that-fill-us-cybersecurity-gaps/.
Peterson, John. 2016. "All Roads Don't Lead to Brussels (But Most Do): European Integration and Transatlantic Relations." In *The West and the Global Power Shift: Transatlantic Relations and Global Governance*, edited by Riccardo Alcaro, John Peterson, and Ettore Greco, 101–126. London: Palgrave Macmillan.
Pierce, Roger. 2008. *Research Methods in Politics: A Practical Guide*. London: Sage.
Politico. 2018. "EU Commissioner: 'We Have to be Worried' about Huawei." *Politico*, December 7. https://www.politico.eu/article/ansip-we-have-to-be-worried-about-huawei/.
Politico. 2020. "Why Trump's Administration is Going After the GDPR." *Politico*, June 26. https://www.politico.com/news/2020/06/29/trump-administration-gdpr-345254.
Pritzker, Penny. 2016. "ICANN Transition Protects Internet freedom." *The Hill*, September 14. https://2014-2017.commerce.gov/news/opinion-editorials/2016/09/op-ed-icann-transition-protects-internet-freedom.html.
Rees, Wyn. 2006. *Transatlantic Counter-Terrorism Cooperation: The New Imperative*. Abingdon: Routledge.
Reuters. 2019. "Trump Says EU Treats US Worse Than China Does on Trade." *Reuters*, May 17. https://uk.reuters.com/article/us-usa-trade-eu/trump-says-eu-treats-u-s-worse-than-china-does-on-trade-idUKKCN1SN2FJ.

Schaake, Marietje, and Mathias Vermeulen. 2016. "Towards a Values-Based European Foreign Policy to Cybersecurity." *Journal of Cyber Policy* 1 (1): 75–84. doi:10.1080/23738871.2016.1157617.
Strayer, Robert. 2019. "Hearing Before the Senate Committee on Homeland Security and Governmental Affairs on Supply Chain Security, Global Competitiveness and 5G." https://www.hsgac.senate.gov/imo/media/doc/Testimony-Strayer-2019-10-31.pdf.
Taylor, Emily. 2018. "Why the Public Directory of Domain Names is About to Vanish." *Chatham House*. https://www.chathamhouse.org/expert/comment/why-public-directory-domain-names-about-vanish.
Taylor, Emily, and Stacie Hoffmann. 2019. "EU–US Relations on Internet Governance." *Chatham House*. https://www.chathamhouse.org/publication/eu-us-relations-internet-governance.
United Nations General Assembly. 2019. "52nd Plenary Meeting, Thursday, 19 December 2019, 10 am" New York. Official Records A/74/PV.52.
US Chamber of Commerce. 2017. "Transatlantic Cybersecurity: Forging a United Response to Universal Threats." Washington, DC: US Chamber of Commerce.
US Department of Homeland Security. 2017. "US–EU Statement Following the US –EU Justice and Home Affairs Ministerial Meeting." US Department of Homeland Security, November 17. https://www.dhs.gov/news/2017/11/17/us-eu-statement-following-us-eu-justice-and-home-affairs-ministerial-meeting.
US Department of State. 2016. "International Cyberspace Policy Strategy." Washington, DC: US Department of State.
US Department of State. 2020. "A New Transatlantic Dialogue – Speech by Michael R. Pompeo." https://www.state.gov/a-new-transatlantic-dialogue/.
Wainwright, Rob, and Frank J. Cilluffo. 2017. "Responding to Cybercrime at Scale: Operation Avalanche – A Case Study." Washington, DC: Center for Cyber and Homeland Security (The George Washington University). Issue Brief # 2017 - 03.
White House. 2003. "The National Strategy to Secure Cyberspace." Washington, DC: White House.
White House. 2009. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Washington, DC: White House.
White House. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." Washington, DC: White House.
White House. 2014. "Fact Sheet: US-EU Cyber Cooperation." White House, March 26. https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.
White House. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Washington, DC: White House.
White House. 2018. "National Cyber Strategy of the United States of America." Washington, DC: White House.

Appendix. Interviews

Interview 1: Interview of the author with official from the European Commission, Brussels, 23 November 2018.

Interview 2: Interview of the author with official from the European External Action Service, Brussels, 26 November 2018.

Interview 3: Interview of the author with official from the European Commission, Brussels, 27 November 2018.