Defence Studies

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fdef20

Role enactment and the contestation of global cybersecurity governance

Xinchuchu Gao & Xuechen Chen

To cite this article: Xinchuchu Gao & Xuechen Chen (2022) Role enactment and the contestation of global cybersecurity governance, Defence Studies, 22:4, 689-708, DOI: 10.1080/14702436.2022.2110485

To link to this article: https://doi.org/10.1080/14702436.2022.2110485

Published online: 25 Sep 2022.

DEFENCE STUDIES
2022, VOL. 22, NO. 4, 689–708
https://doi.org/10.1080/14702436.2022.2110485

Routledge
Taylor & Francis Group

Role enactment and the contestation of global cybersecurity governance

Xinchuchu Gao[a] and Xuechen Chen[b]

[a]Visiting Fellow, London Asia-Pacific Centre for Social Science, King's College, London, UK; [b]Lecturer in Politics & IR at Faculty of Politics and International Relations, New College of the Humanities, London, UK

ABSTRACT

This research seeks to unpack the development of the EU as a security actor in cyberspace. Drawing on the theoretical approach of role theory, this article shows that the EU's role in cyberspace should be understood in relationality to the other poles. On the one hand, the declining hegemonic role of the US in cyberspace as well as the divergence between the US and the EU with regard to cybersecurity governance has made the EU more aware of the need for cyber sovereignty and strategic autonomy. Therefore, the EU seeks to pursue a role of an autonomous cybersecurity player through the enactment of cybersecurity at institutional and operational level. On the other hand, under conditions of increasing interdependence, the EU has considered international cooperation to address challenges in cyberspace as a strategic priority, therefore seeking to act as a promoter of a multi-stakeholder model. Moreover, interpolariy in cyberspace determines the contestation of EU role by other poles. While the EU has recorded some small successes as a regulation-setter, emerging poles of power in the cybersecurity domain contest the EU's desired role, promoting more state-centric approaches and seeking to transfer regulatory authority in the cybersecurity domain to the UN.

ARTICLE HISTORY
Received 21 June 2021
Accepted 3 August 2022

KEYWORDS
Interpolarity; cyberspace; European Union

Introduction

The last two decades have witnessed the development of the European Union (EU) as a security actor (Kirchner and Sperling 2018; Zwolski and Kaunert 2013). The EU clearly seeks to position itself as a significant and unique security actor in an increasingly contested world order (Langenhove and Luk 2010; Laatikainen 2012). A large volume of academic literature has explored the development of the EU overarching security strategies (see for example Koutrakos 2013; Wessel and den Hertog 2013; Bendiek and Porter 2013; Bendiek 2017), but also its pursuit of greater leverage in global security governance across different policy fields, such as energy security (Prontera 2020), anti-terrorism (Bossong 2008), and maritime security (Germond 2011). Seeking to enrich this debate, this article explores the role that the EU envisions to play in cybersecurity governance, a newly emerging and increasing important policy area. Within the existing

CONTACT Xinchuchu Gao gaoxinchuchu@gmail.com Visiting Fellow, London Asia-Pacific Centre for Social Science, King's College, London, UK

scholarly literature, a distinction exists between scholars who conceptualise cybersecurity from a human security perspective (Deibert 2013; Bossong 2008; Mueller 2017) and those who analyse the role of cyber threats in the wider context of state security (Rid 2013; Christou 2014a). Whilst acknowledging that there has been ongoing debate on the definition of cybersecurity (Amitav et al. 2019), in the context of this article, we draw on the recent scholarly discussion (Autolitana 2020; Crandall and Allan 2015; Christou 2016) and understand cybersecurity as an overarching umbrella concept that encompasses various policy areas such as network and information security measures targeting operators of essential services, and providers of critical and digital infrastructure, privacy and data protection issues; and cybercrime and cyberdefence.

Aligning with the core theme of this Special Issue, this article is locating the discussion of the EU's role in cybersecurity governance within the "interpolar" world order, being featured by increasing interdependence and redistribution of power (Grevi 2009; Baciu 2022). Unpacking the EU cybersecurity governance from the perspective of role theory, the article sheds more light on how, due to the interpolar nature of the system, the EU's role in cyberspace should be understood in relationality to the other poles. Second, the choice of the intertwined dimensions of role theory, enables an exploration of the EU's desired role in response to the dynamics of cyberspace as well as the contestation of EU role by other poles.

This paper argues that interpolarity in cyberspace is shaping the EU's desired role in global cybersecurity governance. On the one hand, the declining hegemonic role of the US in cyberspace as well as the divergence between the US and the EU with regard to cybersecurity governance has made the EU more aware of the need for cyber sovereignty and strategic autonomy. Therefore, the EU seeks to pursue a role of an autonomous cybersecurity player through the enactment of cybersecurity at institutional and operational level. On the other hand, under conditions of increasing interdependence, the EU has considered international cooperation to address challenges in cyberspace as a strategic priority, therefore seeking to act as a promoter of a multi-stakeholder model. Moreover, interpolariy in cyberspace determines the contestation of EU role by other poles. While the EU has recorded some small successes as a regulation-setter, emerging poles of power in the cybersecurity domain contest the EU's desired role, promoting more state-centric approaches and seeking to transfer regulatory authority in the cybersecurity domain to the UN.

Epistemologically, to illustrate main arguments, the paper traces the process of EU policy making in the cybersecurity domain by mapping the central institutions, political decisions and documents. It also gives examples of concrete EU activities in sub-fields of cybersecurity, such as cyber defence and data governance. Assessing the key developments at strategic, institutional and political level, allows us to shed more light on the process of the EU role in cybersecurity. The discursive practices and official documents are employed as telling data points, which can better capture the meaning and thus unveil the role conceptions that the EU wants to represent and project. The article is structured as follows: the next section explains the analytical framework drawing on a role theory perspective. The third section unpacks the concept of "interpolarity" (Grevi 2009) with the aim of reflecting on the overarching theme of this Special Issue that examines the nexus between the security policy and interpolarity. Applies the analytical framework to analyse the role of the EU in the interpolar cyber world, the fourth section discusses the

enactment of global security governance and its contestations. The final section outlines the finding of the article and discusses policy implications.

Unpacking the literature of EU's cybersecurity governance

EU cyber security is an emerging research and policy field (Carrapico and Barrinha 2018). Much scholarship has been devoted to exploring the development of the EU's cybersecurity regulations and policies. Previous studies have addressed data protection and cybersecurity in various European countries and discussed EU's efforts to create harmonised data protection regimes, form a comparative perspective (Schünemann and Baumann 2017). An important paper written by Bendiek and Porter (2013) traces the institutional structure of European cyber security policy and compares these to US cyber security policy. Anagnostakis (2021) focus on the role of EU institutions and apply the concept of the policy entrepreneur to examine the Commission's role in the decision-making process of the EU's cybersecurity policy. Other authors have seek to explain EU cybersecurity dynamics from an ontological perspective (Liebetrau and Christensen 2021) and argue that a common EU cybersecurity policy is premised by "the proliferation and entanglement of security agencies, actors, sites, and spaces" (Ibid. 25). This furthermore raises the question of coherence in this policy field. Carrapico and Barrinha (2017) therefore apply the concept of coherence to examine the EU's coherence as a cybersecurity actor. Nevertheless, the abovementioned literature puts an exclusive focus on the EU's cybersecurity policy while neglecting the discussion of the EU's role in cyber governance in a wider global context. An exception is the paper written by Carrapico and Farrand (2020), which explores the extent to which COVID-19 has impacted the EU's cybersecurity policy. Our paper therefore seeks to fill this research gap by examining the EU's role in an interpolar cyberspace from a role theory perspective on the basis of Klose's work (Klose 2018).

Building on the scholarly debate on the EU's actorness in global politics, Klose (2018) introduced a new approach in order to conceptualise the EU's actorness from a role theory perspective. This approach reconceptualises the EU's international emergence as a process of role-making. Specifically, this approach perceives the EU's actorness as its "capacity to imagine and realise roles for its "self" in (specific contexts) of international affairs" (ibid: 1146). In addition, this capacity should be considered as deriving from the complex interplay between domestic and external role expectations, creative actions, and social and material resources available to the EU (ibid: 1146). Central to this interactionist role theory is the idea that political actors express themselves in international society through the development of two intertwined dimensions of agency: "me" and "I." Whereas the "me" refers to a political entity's capacity to understand its "self" through the perspectives of others (role-taking), the "I" can be understood as its capacity to develop creative impulses in reaction to the "me" (Klose 2018). The interaction and dialogue between these two dimensions play a crucial role in enabling a political actor to realise its "self" in a given context of international society, as well as reflecting on the roles it plays within the wider international community. This interaction ultimately results in a learning process wherein an international actor gains a new understanding of its self-positioning in world affairs (Laatikainen 2012).

In Klose's role theory framework, several elements determine the EU's international actorness. The first element is internal role expectations, which are established by "individual constituent units seeking to convince each other of supporting specific EU roles" (Klose 2018, 1148). That is to say, negotiations among member states and various EU institutions will shape the type of role that the Union seeks to play in a given context. The second element, cohesion – internal agreement among different EU actors – will not only shape the Union's ability to mobilise resources, but will affect the expectations of others about the Union's roles (ibid). Additionally, Klose (ibid.) stresses that social and material resources, such as. economic and military capabilities or knowledge, and creative action will shape the EU's actorness in the sense that these elements will ultimately determine what action should be taken based on available resources and the capability to use these resources in accordance with the imaged roles.

Cybersecurity governance in the interpolar world

Reflecting the tremendous changes in international politics since the end of the Cold War, there have long been heated debates over how the global order will evolve as a result of the redistribution and diffusion of power in the international system, not least, because of the COVID-19 pandemic and the war in Ukraine. Visions of the nature of future international politics have become increasingly divergent (Amitav et al. 2019). Some scholars, such as Ikenberry (2011), believe in the durability of a liberal and rules-based order led by the US. Others contend that the US-led western liberal order has been confronted with deeper crises and undergone significant decay (Acharya 2014; Christou 2014a). In addition, some academics argue that, since the end of the Cold War, the international order has evolved into a system best described as "unipolar in multi-polarity," where the US is the single superpower and the multipolarity consists of the EU and other rising powers such as BRIC countries (Chan 2013; Schweller and Xiaoyu 2011). Recently, various new concepts have been introduced to further unpack the nature of the evolving multipolar international order.[1] In line with the key theme of this Special Issue, this study draws on the concept of interpolarity (Grevi 2009; Laatikainen 2012; Autolitana 2020) to illustrate a new scenario of the international system in general and the sphere of cybersecurity governance in particular.

The concept of interpolarity was initially proposed by Grevi (2009) to shed new light on the transition from a West-centric economic and political order to an increasingly heterogeneous international system in which emerging and resurgent actors intend to play a greater role. According to Grevi (2009, 9), interpolarity can be defined as "multipolarity in the age of interdependence." Similary, Baciu (2) define interpolarity as the interaction between various poles of different sizes. These definitions offer a clearer illustration of the current global system than the concept of multipolarity in the sense that interpolarity effectively captures two major trends in the post-Cold War international politics: (1) the shifting balance of power at a time of rising geopolitical tension, and (2) a growing level of interdependence among major global and regional powers. On the one hand, over the past two decades power diffusion and redistribution have resulted in power and knowledge shifting from the US and Western countries to developing countries and rising actors such as China, India, and Brazil. The balance of power has also shifted between state and non-state actors in the sense that non-state,

sub-state and supra-state entities now play a greater role in shaping international affairs (Laatikainen 2012). According to Grevi (2009, 28), this progressive redistribution of power at the global level has resulted in a rising level of controversy and tension among major international actors, leading to an increasingly confrontational and competitive multipolar system. On the other hand, despite the existence of tension and competition, there is a higher degree of interdependence among major and smaller "poles" within the global framework. Common challenges surrounding increased interdependence raise the issue of coordination and effectiveness of global governance (Grevi 2009, 31). Underlying Grevi's (2009) idea of interpolarity is the assumption that whereas redistribution of power at the global level generates an increasingly confrontational and competitive multipolar order, the deepening of interdependence ultimately enables international cooperation among major "poles" to tackle common economic, political and security challenges. Analyzing the dynamics of power transition and the deepening of interconnectedness through the lens of interpolarity is particularly timely and relevant when considering the field of cybersecurity governance – a newly emerging battlefield for geopolitical competition. The following paragraphs further explain how global cybersecurity governance can be understood through the lens of interpolarity.

Cybersecurity governance as a rising field of global governance has displayed the key trends outlined in Grevi's (2009) conceptualization of interpolarity. Firstly, over the past two decades, the expansion of internet connectivity globally has significantly deepened the degree of interdependence and interconnectedness among different actor at national, regional, and international levels. In his initial conceptualization of interpolarity, Grevi pointed out that three issues lie at the center of complex interdependence: economic growth, energy security and environmental sustainability (Grevi 2009, 5). We argue that cybersecurity should be considered as an additional issue that lies at the core of complex interdependence. None of the existing major powers can effectively tackle cybersecurity challenges alone, because cyberspace is by its very nature transnational. When initially created, the Internet or cyberspace was commonly perceived as a "borderless global communications medium, effectively situating electronic commerce beyond the regulatory reach of any single nation's politics or legal jurisdiction" (Drissel 2006, 116). Early analyses rightly pointed out that the transnational nature of the cybersecurity challenged the conventional understanding of territory and the principles of sovereignty associated with physical borders (Post and Johnson 1997). Due to its transnational characteristics, as noted by Barrinha and Renard (2017), cyberspace has become a "global common" that effectively connects nations and citizens and generates increasing interactions and frictions among different stakeholders in international politics. Cybersecurity as an emerging issue has significantly deepened the interdependence among different actors at individual, national and global levels, contributing to increasingly dense interconnections between sectors (Clemente 2013). This is essentially due to the fact that, as Autolitana (2020: page) point out, "cybersecurity is cutting across different areas of responsibility, requiring coordination and cooperation between a wide variety of public actors at different levels of government, but also actors from business and society when government tasks and authority are delegated downwards (localization), upwards (supranationalization), or sideways (privatization)." In brief, the growing importance of digital technologies and cybersecurity issues have contributed to deepening the trend of

complex interdependence at a global level characterized by the existence of a complex ecosystem of stakeholders (Klimburg and Faesen 2020).

Secondly, in recent years, the cyberspace has inevitably become an arena for geopolitical competition and normative contestations among major international players (Chiappetta 2019; Kello 2017). In line with about the idea of the interpolar order in cyber governance, the asymmetric distribution of power and resources generates increasing uncertainty and undermines the unilateral action of all major powers (Grevi 2009, 15). It has been widely acknowledged by the existing literature that the redistribution of power has become entangled with an increasingly confrontational and competitive multipolar system in the field of cybersecurity (Kello 2017; Duić et al. 2017). This is evidenced by growing political contestations concerning the US-led regulatory unilateralism and legitimacy of ICANN, along with the rise of emerging powers in the cyber domain. This process has sparked heated debates about the future normative and regulatory frameworks of global cybersecurity governance. Moreover, whereas the cyberspace used to be perceived as a self-regulating realm independent from the traditional geopolitical sphere or compulsory regulatory measures, this view has drastically changed in recent years. Cyberspace has increasingly come to be regarded as a new focal point of state-sponsored extraterritorial regulations as well as multi-jurisdictional decisions (Drissel 2007; see also Kobayashi and Ribstein 2003; August 2002). In other words, cybersecurity has become a policy area that is closely intertwined with traditional geopolitical rivalries, nationally focused institutions and nation-state conflicts (Mueller 2017). This observation is supported by numerous studies showing that cybersecurity has increasingly been used to "enmesh various aspects of the Internet in foreign policy and military conflicts, as well as in other national forms of regulation and control in which states are privileged" (Mueller 2017, 417; see also Segal 2016; MalcolmTurnbull 2015). At an empirical level, rising geopolitical tension and inter-state competition can be observed in this policy area. A telling example is the recent US–China tech war. The Trump administration attempted to force Beijing to abandon its policies in high-tech sectors and technology transfer from foreign enterprises in order to maintain US supremacy (Sun 2019). In addition, Russia is believed to pursue digital authoritarianism and an alternative cybersecurity governance model which directly challenges the liberal democratic values and interests defended by the US and the EU (Morgus 2018; DeNardis 2020). These observations demonstrate that the concept of interpolarity is highly relevant to the policy area of cybersecurity. Specifically, both trends underlying the interpolar order – an increasing level of interconnectedness and a process of power-shifting from the US to other major players – can be observed in the existing system of global cybersecurity governance.

The enactment of global security governance and its contestation

Using role theory, the following section investigates the desired role of the EU in response to the growing trend of interpolarity in global cyberspace, as well as the extent to which the EU has managed to achieve its role in practice. To trace the developments, the article draws on a variety of primary data and secondary sources, including a wide range of official documents published by multiple EU institutions, policy papers, as well as media reports. A combination of different types of sources enables triangulation of

evidence and helps assess the extent to which the EU's visions and desired roles have been implemented in practice. The first part of this section analyses the EU's desired role in the interpolar cyber world. Part two explores how the EU has used its resources to realise its desired role. The final section discusses the extent to which the EU has succeeded in solidifying its desired role.

Power re-distribution and increasing interdependence in the cybersecurity domain

The interaction of two basic trends in global cyberspace, namely the redistribution of power and increasing interdependence, is shaping the EU's cybersecurity strategy. On the one hand, the declining hegemonic role of the US in cyberspace as well as the divergence between the US and the EU with regard to cybersecurity governance has made the EU more aware of the need for cyber sovereignty and strategic autonomy. Therefore, the EU seeks to pursue a role of an autonomous cybersecurity player. On the other hand, under conditions of increasing interdependence, the EU has considered international cooperation to address challenges in cyberspace as a strategic priority, therefore seeking to act as a promoter of a multi-stakeholder model.

In response to the redistribution of power in the cyberspace, the EU aims to act as a more autonomous cybersecurity player and to develop its own version of cybersecurity governance approach. Global cyber governance is arguably dominated by a Western-centric approach with a commitment to delivering an open, free and accessible cyberspace through a multi-stakeholder model. This approach is widely accepted by the US government, the EU and those whose interests align with them. For instance, the Australian Communication Minister, Malcolm Turnbull, stated that Australia supported "an open Internet which is administered by multi-stakeholder organizations like ICANN and NOT" (Crandall and Allan 2015). Similarly, US Congressman Greg Walden argued that "weakening the multi-stakeholder model threatens the Internet, harming its ability to spread prosperity and freedom" (Greg Walden 2012).

The US has held a leadership role in promoting the Western-centric approach outlined above. The EU has been the US's longstanding ally in the sense that they both make commitments to principal values and norms including openness, freedom and multi-stakeholderism. Nevertheless, the EU's cybersecurity governance differs from the American approach in terms of the level of governmental involvement. While the US has adopted a "hands-off-the-internet approach," the EU has historically been more willing to embrace cybersecurity regulations and rules than the US. One example showing the EU-US differences on cybersecurity governance issues is the case of the revelations of Edward Snowden. Snowden revelations demonstrate the wide scope of surveillance conducted by the US National Security Agency (NSA) and many EU member states were targeted. The case of Snowden revelations created an atmosphere of distrust between the EU and the US and raised "the issue of whether EU and US cultures of cybersecurity were compatible when it came to personal data collection and its use for intelligence purposes" (Christou 2016). This case led to major arguments over cyber sovereignty issues in the EU. For instance, Germany, which was the major target of the NSA surveillance programme, argued in favour of "digital data sovereignty" in the EU (Broeders 2021).

Another example illustrating divergence between the EU and the US with regard to cybersecurity governance is the invalidation of the EU–US Privacy Shield. The EU–US Privacy Shield was a framework for regulating the transatlantic flow of data for commercial purposes, allowing the free transfer of data to companies certified in the US under the EU law (European Commission 2020cc). On 16 July 2020, the European Court of Justice (ECJ) invalidated the EU–US Privacy Shield in its decision in the Schrems II case, because the Privacy Shield transfer mechanisms did not meet the level of data protection required by EU law. In particular, the ECJ expressed its concerns over US domestic surveillance programmes because they "are not limited to what is strictly necessary" (EU 2020).

More recently, the US–China tech war further demonstrates that the EU needs to preserve strategic autonomy in cyberspace because the EU has been under pressure from both sides. Over the past two years, the US has unveiled a series of new legislative measures aimed at China, including the Foreign Investment Risk Review Modernization Act (FIRRMA), the Executive Order on Information and Communications Technology and Services (ICTS), and the Export Control Reform Act (ECRA). These measures signal the US government's accelerating technology war with China. The US–China technology war has significant implications for the EU, for whom the US and China represent about one-third of its total merchandise trade – 17.1% with the US and 15.4% with China in 2018 (European Commission 2019). On the one hand, there has been an intense US lobbying campaign to convince European countries to exclude Chinese suppliers from their 5 G networks. On the other hand, the EU has to consider economic realities, such as EU telecoms operators' current high level of dependence on Chinese equipment (European Parliament 2019). Therefore, it is vital for the EU to preserve its strategic autonomy in order not to be stuck in the middle of a tech rivalry between the US and China.

In response to the power redistribution in cyberspace discussed above, the EU seeks to act as an autonomous player and to develop its own version of cybersecurity governance approach. The EU has recognized the fact that strategic cyber espionage campaigns or militarily motivated cyberattacks are becoming key elements of international relations and that cyberspace is developing into a war zone (Autolitana 2020). The need for stronger EU cyber and technological sovereignty is one of the key priorities of the Commission President, Ursula von der Leyen (Claessen 2020). In July 2020, the German Presidency of the Council of the European Union, in its programmatic manifesto, announced the EU's intention "to establish digital sovereignty as a leitmotiv of European digital policy" (The German Presidency of the EU Council 2020). In a speech delivered in February 2021, Charles Michel, the President of the European Council, stressed that digital sovereignty was central to European strategic autonomy (Michel 2021).

All of the above show the EU's emphasis on ensuring strategic autonomy and its ambition of acting as a more autonomous actor in cyberspace. In particular, Snowden revelations and the US-China tech war have made the EU more aware of its vulnerability. As a result, the EU has increasingly pursued a role of an autonomous cybersecurity player with an emphasis on the need for stronger EU cyber sovereignty and strategic autonomy.

Having been aware of increasing interdependence in cyberspace, the EU seeks to act as a promoter of a multi-stakeholder model because the EU has considered international

cooperation to address challenges as a strategic priority. The European Union Agency for Network and Information Security (ENISA), for instance, has explicitly pointed out that international collaboration is an essential part of the response mechanism addressing cyber threats, because digital boundaries do not coincide with national frontiers (ENISA 2013). In a similar vein, the European Commission has emphasized that international cooperation is needed to strengthen cybersecurity (European Commission 2018).

In line with its emphasis on the importance of international cooperation, the EU has therefore proactively promoted the multi-stakeholder approach to cybersecurity governance. In its 2020 Cybersecurity Strategy, the EU stressed that it strongly supported and promoted the multi-stakeholder model for Internet governance (European Commission 2020a). Similarly, the 2017 Cybersecurity Strategy prioritized the EU's multi-stakeholder engagement in cyberspace when strengthening international cooperation in cybersecurity (European Commission 2017). Earlier, in the 2013 Cybersecurity Strategy, for instance, the EU has confirmed "the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach" (European Commission 2013).

This sub-section shows the EU seeks to act as an autonomous cyber power as well as a promoter of a multi-stakeholder model in the interpolar cyber world. The following subsection explores how the EU has used resources to achieve its desired role in cyberspace.

Institutional and operational role enactment

To achieve its role as an autonomous cyber player, the EU has published a number of policy papers to investigate cyber threats and to construct and adjust its cybersecurity strategies to address these threats. The 2013 EU Cybersecurity Strategy (EUCSS), the 2016 Network and Information Security (NIS) Directive and the 2016 Joint Framework on countering hybrid threats are major steps in this direction. The 2013 EUCSS, for instance, identified five strategic priorities: achieving cyber resilience; drastically reducing cybercrime; developing cyber defence policy and capabilities related to the Common Security and Defence Policy; developing the industrial and technological resources for cybersecurity; and establishing a coherent international cyberspace policy for the European Union to promote core EU values.

The EU also brought together resources and expertise available to the EU and its member states to jointly tackle cyber threats. For instance, the EU established the European Union Agency for Cybersecurity (ENISA) in 2014 to assist member states and Union institutions to build capabilities to prevent, detect and respond to cyber threats. To facilitate strategic cooperation, the NIS Directive established the NIS Cooperation Group, composed of representatives of the EU member state, the European Commission and the ENISA. The Recommendation on the creation of the Joint Cyber Unit is one of the most recent steps towards completing cybersecurity crisis management framework at the EU level. In June 2021, the Commission proposed to build a new Joint Cyber Unit to provide a virtual and physical platform of cooperation and to ensure an EU coordinated response to large-scale cyber crises (European Commission 2021). Meanwhile, the Commission has issued the decision on establishing the office of the European Union Agency for Cybersecurity (ENISA) in Brussels (Ibid.). The ENISA

Local Office is established with a view to enhanced more structured and regular cooperation, in order to avoid the duplication of activities.

Meanwhile, the EU has dedicated resources to develop a joint EU diplomatic response to cyber crises. The 2013 EUCSS has been a major step in developing cyber diplomacy at the EU level, placing the established of a "coherent international cyberspace policy for the EU" among its five priorities. During its 2016 Presidency of the EU Council, the Netherlands proposed to develop "a joint EU diplomatic response against coercive cyber operations" (Council of the EU 2016). In 2017, the EU Foreign Affairs Council endorsed the EU's Cyber Diplomacy Toolbox, which has been one of the key enablers for a common diplomatic response to address cyber threats. Within the framework of the Common Foreign and Security Policy (CFSP), the Council proposed a series of instruments that the EU institutions and member states could undertake, including the use of the most powerful tool – sanctions. Under the framework of Cyber Diplomacy Toolbox, in July 2020, the EU imposed the first ever sanctions against six individuals and three entities responsible for or involved in cyber-attacks (Council of the EU 2020).

In addition, the EU has adopted a regulatory approach to preserve its strategic autonomy in cyberspace. This is mostly because EU treaties do not provide a unifying legal basis for the EU to regulate cybersecurity. In this context, the EU has to formulate its approach to cybersecurity on the basis of its competences in other areas, including the internal market, the Area of Freedom, Security and Justice (AFSJ), the Common Security and Defence Policy (CSDP) and the Common Foreign and Security Policy (CFSP) (Bendiek and Matt 2019). Of these four areas, the EU merely has broad competence to regulate the single market. Therefore, over the years, "most of the EU's action in the field of cybersecurity has dealt with internal EU policies or is linked to criminal law (combating cybercrime) and is tied to the goals of economic growth and the internal market."(Odermatt 2018) In particular, the EU has frequently deployed its mandate to regulate the internal market to pursue strategic autonomy in cyberspace. As Wessel noted, compared to other cybersecurity actors with clearly defined mandates specifically addressing cybersecurity, the EU's approach to cybersecurity can be characterized as "cybersecurity by regulation" (Wessel 2019). The European Commission therefore explicitly points out that enhancing the EU's leadership on international standards in cyberspace is one of major priorities of the new Cybersecurity Strategy (European Commission 2020).

The EU's regulatory approach to preserve strategic autonomy in cyberspace can be observed in a number of EU policy papers and initiatives. In the Communication ICT Standardisation Priorities for the Digital Single Market, the Commission pointed out that standard-setting is crucial for market access and for boosting the competitiveness of EU industries and has called for a higher level of political support (European Commission 2016a). In a similar vein, in 5 G for Europe: An Action Plan, the Commission again placed an emphasis on the promotion of global standards when developing 5 G technologies (European Commission 2016b).

The EU has taken a number of steps to leverage its regulatory power in international cyberspace. By adopting the General Data Protection Regulation (GDPR) in 2016, the EU created a solid framework for ensuring the free flow of data between the EU and third parties with a comparable level of protection of personal data. Other initiatives include the Regulation on the free flow of non-personal data (FFD) (European Union 2018), the

Cybersecurity Act (CSA) (European Union 2019a), and the Open Data Directive (European Union 2019b). Moreover, the EU has engaged in digital diplomacy by recognizing 13 countries as providing an adequate level of data protection, including Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. The EU is also seeking new regulatory powers against big tech firms. EU Internal Market Commissioner Thierry Breton suggested that these new powers should include the ability, in extreme circumstances, to exclude large tech companies, such as Google and Facebook, from the European single market altogether (Hellard 2020). To achieve this goal, the EU passed the legislative proposal the Digital Services Act (DSA), which would increase responsibility and liability for social media firms and the content on their platforms (European Commission 2019).

In terms of its desired role as a promoter of the multi-stakeholder model, the EU's efforts to achieve this role could be observed at bilateral, regional and multilateral levels. Bilaterally, the EU has actively cooperated with its like-minded partners (European Parliament 2015). For instance, the leaders of the EU and South Korea "emphasized the importance of ensuring the openness and security of cyber space" and "agree to increase bilateral cooperation on cyberspace as well as to strengthen the global partnership in response to threats arising from cyberspace" (European Council 2015). Similar sentiments can be found in a number of joint statements with the EU's key partners over the past few years. Meanwhile, the EU has established regular policy dialogues on cyber issues with its partners, such as the Dialogue on IT (EU–China), the Dialogue on International Cyber Policy (EU–Brazil), and the Dialogue on ICT policy (EU–Japan).

The EU's efforts to enhance international cooperation are also exemplified by the EU's promotion of the Convention on Cybercrime of the Council of Europe, which is known as the Budapest Convention. The Convention is the only binding international instrument on cybercrime. The Budapest Convention is open to countries that are not members of the Council of Europe, which makes it a powerful instrument for global promotion of European values and norms. Meanwhile, the EU has been involved in international cooperation under the framework of the UN. Currently, there are two UN processes dealing with cybersecurity issues: a Russian-sponsored resolution calling for the establishment of an Open-Ended Working Group (OEWG) and an American-sponsored resolution calling for the establishment of a new UN Group of Governmental Experts (GGE) (Broeders 2021). The EU's active participation in both UN processes could be observed. On the one hand, the EU is regularly consulted by the GGE. As a complement to binding international laws, the EU promotes voluntary non-binding norms, rules, and responsible state behaviour in cyberspace by engaging with the GGE. On the other hand, the EU has closely worked with the OEWG. For instance, the EU and its member states have issued joint comments on the initial "pre-draft" report of the OEWG on developments in the field of Information and Telecommunication in the context of international security (EU 2020).

In addition, NATO is another important multilateral platform for the EU to promote the multi-stakeholder model and to enhance international cooperation in cyberspace. Cybersecurity governance is one of the areas of strengthened cooperation between NATO and the EU (NATO 2021). Having recognized that "hybrid and cyber attacks by hostile states and non-state actors challenge the traditional definition of interstate

conflict, espionage and sabotage," the EU emphasizes the need for further cooperation between the EU and NATO to strengthen their capabilities to "prevent, deter and respond to hybrid and cyber attacks" (European Parliament 2021). To be more specific, NATO and the EU cooperates through a Technical Arrangement on Cyber Defence, which was signed in February 2016 (NATO 2021).

Role contestation by other Poles

Moving on to the third step of analysis, this sub-section discusses the implications of the role-making process with regard to the EU's desired role in global cybersecurity governance and argues that the EU has partially fulfilled its desired role. Specifically, the EU's role as an autonomous cyber has been recognized by other cyber players in the sense that EU regulations in cyberspace are widely accepted worldwide. Nevertheless, the EU has encountered various challenges which limit its capability to further realize its desired role as an autonomous cyber player and a promoter of a multi-stakeholder model.

The EU has achieved much success in acting as a regulation-setter in the field of cybersecurity. As a report on European data sovereignty has rightly pointed out, being the first to develop a regulatory framework for data protection has given the EU a comparative advantage when externalizing its regulations (EIT Digital 2019). It has been recognized that "the GDPR remains a source of advantage for the EU" because "[the EU] is too large a market to ignore" (ibid.). In Asia, a number of new laws bearing the hallmark of the EU's GDPR demonstrate that the GDPR is influential in the region. Established data protection regimes in Asia, such as in Australia, New Zealand and Singapore, have borrowed heavily from the GDPR (Hogan Lovells 2020). Meanwhile, a number of emerging data protection regimes, such as India and Thailand, introduced new data protection laws featuring GDPR-style regulation (ibid.). The EU's success in acting as a regulation-setter in Asia is exemplified by negotiations on the EU–Japan Economic Partnership Agreement (EPA). The European Commission stressed that data protection is a fundamental right in the EU and therefore is "not up for negotiation" (*Kanetake* and *de Vries* 2018). Dutch MEP Marietje Schaake stated that "the European Parliament will not ratify an agreement that undermines data protection in the EU." (ibid.) In order to close the gap with regard to data protection between the EU and Japan, the Japanese government remodeled its privacy protection framework. Subsequently, the EU and Japanese delegations agreed to recognize each other's data protection as equivalent, and the EU–Japan EPA was signed on the same day. This example reveals the EU's ambition to provide leadership in setting regulations in cyberspace and the success it has achieved.

In addition to its influence in Asia, the GDPR has also stimulated debate and initiatives on the regulation of data protection in the US. One telling example is the California Consumer Privacy Act (CCPA), which shares certain similarities with the GDPR. As an observer pointed out, "GDPR did have an impact on CCPA" (Ruiz 2020). Similarly, in 2020 Washington state introduced a remodeled version of its Data Privacy Act, which borrows some language on data from the GDPR (ibid.).

Nevertheless, despite the EU's leading role in setting regulations in cyberspace, the EU's attempts to achieve a desired role as an autonomous cyber player and a promoter of a multi-stakeholder model have made only limited progress. The Budapest Convention

reflects this problem. The fact that the Convention was drafted without extensive input from developing countries has led to developing countries hesitating to join it. For instance, the Convention was drafted without India's participation, and India has maintained its status as a non-member of the Convention (Singh 2013). Another example of the EU's failure to convince emerging cyber power states to accept its cyber values is Russia's proposal for a new cyber treaty. Russia has consistently expressed its concerns over the Budapest Convention on the grounds of national sovereignty and has proposed a new treaty at the United Nations. In December 2019, a Russian-led and Chinese-backed resolution on cybercrime, Countering the Use of Information and Communication Technologies for Criminal Purposes, was adopted in the United Nations General Assembly (UNGA) despite opposition from major Western states. This resolution is widely considered an attempt to set up new cyber norms that counterbalance the values underpinning the Budapest Convention. Russia has actively promoted its cyber norms in other international organizations including the Shanghai Cooperation Organization (SCO) and the Collective Security Treaty Organization (CSTO) (Crandall and Allan 2015). These attempts demonstrate Russia's ambition of promoting its own version of cyber norms, reflecting the EU's lack of success in convincing Russia to accept the EU's values.

Another example showing the lack of capability of the EU to achieve its desired role is the limited use of cyber sanctions by the EU in practice. As discussed earlier, the EU Cyber Diplomacy Toolbox in general and the restrictive measures, such as cyber sanctions, in particular are considered as major tools to respond to malicious cyber activities that constitute threats to the EU. Nevertheless, to date, only eight individuals and four organizations have been sanctioned by the EU since April 2015 while the U.S. Treasury Department has imposed cyber-related sanctions on a combined 99 individuals and 59 entities (Soesanto 2021).

All of the above illustrates that despite the EU's leadership position in setting regulations in cyberspace, the EU has achieved limited progress in acting as an autonomous cyber player and a promoter of a multi-stakeholder model. The EU's efforts to achieve its desired role in cyberspace is mostly undermined by challenges from emerging cyber powers with different worldviews. The multi-stakeholder approach promoted by the EU follows a "people-centered" logic and allows all participants to get involved into the decision-making process on an equal footing (Lu 2015). In contrast, a multilateral approach to cybersecurity governance, which is promoted by China and Russia, puts an emphasis on more governmental involvement and the UN's leading role in building international consensus on rules (Segal 2018). According to DeNardis, Russia and China view the cross-border, private, distributed architecture of the Internet as a threat to state sovereignty and therefore promote top-down government control of Internet networks rather than private-sector-led multi-stakeholder governance (DeNardis 2020). Russia's emphasis on cyber sovereignty is visible in the 2000 Doctrine for Information Security, which notes that one of the sources of threats for the information security of the Russian Federation is:

> the development by a range of states of the concept of information warfare, which foresees the creation of means to exert a dangerous influence on the information sphere of other countries of the world, the disruption of the normal functioning of the information and

> telecommunication systems, the preservation of information resources and the acquisition of unauthorized access to them (Russian Government 2000).

To advance its normative framework on cybersecurity through the UN, Russia has routinely contested the dominant multi-stakeholder model and stressed the need to respect the sovereign equality of states (Kurowska 2019). China is also engaging with the normative debate in global cybersecurity governance. The concept of cyber sovereignty is key to China's broader cyber policy and is promoted at the highest level. In a speech delivered in 2015, President Xi Jinping stressed the risks of not allowing countries to govern their own cyberspace according to their own rules (Mitchell 2016). More recently, during its annual state-run World Internet Conference in October 2019, the Chinese government identified respecting sovereignty as one of the fundamental principles of governing cyberspace (World Internet Conference 2019). Other emerging cyber powers, such as India and Iran, also call for the voices of new cyber powers to be heard in existing Internet governance institutions, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) (Christou, 2014). Cybersecurity governance approaches adopted by abovementioned emerging cyber power with different worldviews have significantly challenged the EU's efforts to achieve its desired role in cyberspace.

Furthermore, the EU's capacity of acting as an autonomous cybersecurity player and a promoter of multi-stakeholder model has been hampered by the hybrid nature of the EU's institutional structure. In some sub-policy areas within the union's cybersecurity policy (e.g. cyber defence), it is observed that policy implementation has been less convergent across EU member states and that the EU has limited political and legal authority in the policy areas (Schuetze 2020). As numerous studies observe, the EU's attempts to enhance coordination in the field has not always led to coherent inter-institutional work. Instead, the EU's approach to cybersecurity remains fragmented (Carrapico and Barrinha 2017; Christou 2016; Klimburg and Tirmaa-Klaar 2011). This has subsequently resulted in limited resources allocated to the field of cybersecurity in comparison to other security areas (Carrapico and Barrinha 2017).

Conclusion

Shedding new light on the EU's security strategy and its increasingly proactive engagement in security governance within the interpolar world, this article examined the EU's desired roles and actions in cybersecurity governance. It first demonstrated that cybersecurity as a newly emerging transnational security field can be understood through the lens of the concept of interpolarity. Specifically, the current system of global cybersecurity governance is characterized by two salient trends: (1) a high level of interdependence among different stakeholders, both states and non-state actors; and (2) a process of power transition from the dominant actor (the US) to a growing number of emerging or resurgent powers, such as China and Russia, leading to an increasingly competitive and confrontational multipolar framework in the field of cybersecurity governance. This led to the central question of this study: How does the EU position itself within this interpolar system of cybersecurity governance? This paper made a twofold argument. First, it suggested that since the early 2010s the EU has actively constructed its role in

cyberspace as an autonomous cyber player and a promoter of a multi-stakeholder model within an interpolar cyber world, which distinguishes itself from other significant cybersecurity actors, such as the US, China, and Russia. In doing so, the EU has established itself as a significant "pole" and a key player within the interpolar system of cybersecurity governance. Secondly, an in-depth analysis of the EU's actions in cybersecurity demonstrated that, despite its great ambition, the EU only partially fulfils its desired two-fold role in global cybersecurity governance because of challenges and contestation from emerging cyber powers with different world-views as well as the hybrid nature of the EU's institutional structure.

Note

1. See (Acharya 2014) – multiplex order.

Disclosure statement

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

Notes on contributors

Dr. Xinchuchu Gao is a Fellow in European Political Economy at European Institute, LSE. She is also holding a Visiting Research Fellow position at the London Asia-Pacific Centre for Social Science, King's College London.

Dr. Xuechen Chen is an Assistant Professor in Politics and International Relations at Northeastern University - London, and a Visiting Research Fellow at the London Asia-Pacific Centre for Social Science, King's College London.

ORCID

Xuechen Chen http://orcid.org/0000-0002-0046-8012

References

Acharya, Amitav. 2014. "Global International Relations (IR) and Regional WorldsA New Agenda for International Studies." *International Studies Quarterly* 58 (4): 647–659. doi:10.1111/isqu.12171.

Amitav, Acharya, Antoni Estevadeordal, and Louis W. Goodman. 2019. "Reshaping Global Order in the 21st Century: G-Plus Leadership in a Multiplex World." *China & World Economy* 27 (5): 63–78. doi:10.1111/cwe.12300.

Anagnostakis, D. 2021. "The European Union-United States Cybersecurity Relationship: A Transatlantic Functional Cooperation." *Journal of Cyber Policy* 6: 1–19.

2020. Asia Pacific Data Protection and Cybersecurity Guide 2020 (Lovells Hogan).

August, Ray. 2017. "International cyber-jurisdiction: A Comparative Analysis." In *Computer Crime*, 419–462. Abingdon: Routledge.

Autolitana, S. 2020. "A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked."*Istituto Affari Internationali Commentaries20*. 1–6. online]. Accessed 16 March 2021. https://www.iai.it/en/pubblicazioni/europe-fit-digital-age-quest-cybersecurity-unpacked

Baciu, Cornelia. 2022. "Interpolarity. Re-visiting security and the global order." *Defence Studies* 22 (4): 571–590.
Barrinha, A., and T. Renard 2017. "Cyber-Diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3 (4–5): 353364.
Bendiek, Annegret 2017. "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience." SWP Research Paper, 11 2017
Bendiek, A., and E. P. Matt. 2019. *The EU's Regulatory Approach to Cyber-security, Research Division EU/Europe*. Berlin: German Insititue for International and Security Affairs.
Bendiek, A., and A. L. Porter. 2013. "European Cyber Security Policy within a Global Multistakeholder Structure." *European Foreign Affairs Review* 18 (2): 155–180.
Bossong, Raphael. 2008. "The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance." *JCMS: Journal of Common Market Studies* 46 (1): 27–48.
Brandão, Ana Paula, and Isabel Camisão. 2021. "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy." *Journal of Common Market Studies*. doi:10.1111/jcms.13158.
Broeders, D. 2021. "The (Im) Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A mid-process Assessment." *Journal of Cyber Policy* 6: 1–21.
Carrapico, Helena, and André Barrinha. 2017. "The EU as a Coherent (Cyber) Security Actor?" *JCMS: Journal of Common Market Studies* 55 (6): 1254–1272.
Carrapico, Helena, and Andre Barrinha. 2018. "European Union Cyber Security as an Emerging Research and Policy Field." *European Politics and Society* 19 (3): 299–303. doi:10.1080/23745118.2018.1430712.
Carrapico, Helena, and Benjamin Farrand. 2020. "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy." *Journal of European Integration* 42 (8): 1111–1126. doi:10.1080/07036337.2020.1853122.
Chan, Gerald. 2013. "The Rise of Multipolarity, the Reshaping of Order: China in a Brave New World?" *International Journal of China Studies* 4 (1).
Chiappetta, Andrea. 2019. "The Cybersecurity Impacts on Geopolitics." *FormaMente* 14 (1): 61–74.
Christou, G. 2014a. "The EU's Approach to Cyber Security". Policy paper series, Autumn/Winter: 5.
Christou, G. 2016. "Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience." In *Chapter 7 in Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, 169. Netherlands: Springer.
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.
Clemente, Dave. 2013. *Cyber Security and Global Interdependence: What Is Critical?* London: Chatham House, Royal Institute of International Affairs.
Council of the EU. 2016. "Non-paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations", 5797/6/16, REV 6 1–12 , 19 May 2016.
Council of the EU. 2020. "EU Imposes the First Ever Sanctions against cyber-attacks." available at https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/, accessed on 11 November 2021.
Council of the European Union. 2005. Council Framework Decision on Attacks against information systems.
Crandall, M., and C. Allan. 2015. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36 (2): 361. doi:10.1080/13523260.2015.1061765.
DeNardis, L. 2020. *The Internet in Everything: Freedom and Security in a World with No off Switch*, 181–182. New Haven: Yale University.
Drissel, David. 2006. "Internet Governance in a Multipolar World: Challenging American Hegemony." *Cambridge Review of International Affairs* 19 (1): 105–120. doi:10.1080/09557570500501812.

Duić, I., V. Cvrtila, and T. Ivanjko (2017). "International Cyber Security Challenges." In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* Croatia (pp. 1309–1313). IEEE.

Ebert, Hannes, and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34 (6): 1054–1074. doi:10.1080/01436597.2013.802502.

EEAS 2016 "Shared Vision, Common Action: A Stronger Europe- A Global Strategy for the European Union' S Foreign and Security Policy". June. Available online at: http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

EIT Digital. 2019. *European Digital Infrastructure and Data Sovereignty—A Policy Perspective* (Budapest), 6.

ENISA. 2013. "Cybersecurity Cooperation: Defending the Digital Frontline." available at: https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline, accessed on 11 October 2021.

EU. 2020. "Joint Comments from the EU and Its Member States on the Initial 'pre-draft' Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security." available at https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf accessed on 12 November 2021

European Commission. 2013a. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." *JOIN* 1 final, Brussels, 7.2. 2013

European Commission. 2013b. "Communication on a Cyber Security Strategy of the European Union." Available at: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

European Commission. 2016a. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ICT Standardisation Priorities for the Digital Single Market." *COM* 176 final.

European Commission. 2016b. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 5G for Europe: An Action Plan." *COM* 588 final.

European Commission. 2017. "Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU." In *JOIN*, 450. 13 September 2017, final, Brussels.

European Commission. 2018. "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building: A Playbook." available at https://www.iss.europa.eu/sites/default/files/Operational%20Guidance%20for%20the%20EU's%20international%20cooperation%20on%20cyber%20capacity%20building%20–%20A%20Playbook.pdf accessed on 11 October 2021

European Commission, 2019a."The Digital Services Act: Ensuring a Safe and Accountable Online Environment". https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Commission. 2019b. "Client and Supplier Countries of the EU28 in Merchandise Trade (Value`%) (2018, excluding intra-EU Trade)". Accessed 11 June 2020. http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf

European Commission. 2020. "the EU Security Union Strategy" available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

European Commission. 2020a " Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade."*JOINT* 18 final Brussels. 16 December 2020.

European Commission. 2020c. *Commercial Sector*. Brussels: EU-US Privacy Shield. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

European Commission. 2021. "EU Cybersecurity: Commission Proposes a Joint Cyber Unit to Step up Response to large-scale Security Incidents", available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088, accessed on 12 November 2021.
European Council. 2015. "*Joint Press Statement, 8th Republic of Korea-EU Summit*." Presse Release: 3.
European Council and Council of the European Union. 2018. "Cyber Defence: Council Updates Policy Framework." Accessed 11 April 2021. https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/
European Parliament. 2015. *Cyber Diplomacy: EU Dialogue with Third Countries*.
European Parliament. 2019. "5G in the EU and Chinese Telecoms Suppliers." Accessed 19 June 2020 https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf
European Parliament. 2021. "*Report on EU-NATO Cooperation in the Context of Transatlantic Relations (2020/2257(INI))*."
European Union. 2018. "*Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of non-personal Data in the European Union*."
European Union. 2019a. "*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)*."
European Union. 2019b. "*Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the re-use of Public Sector Information* (Brussels:)."
"Europe's New Aggressive Stance on Tech." Politico, 27 October 2019, available at www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen, accessed on 2 November 2021.
Germond, Basil. 2011. "The EU's Security and the Sea: Defining a Maritime Security Strategy." *European Security* 20 (4): 563–584. doi:10.1080/09662839.2011.635648.
Greg Walden. "Opening Statement at the "International Proposals to Regulate the Internet," Hearing before the Co Mmittee on Energy and Commerce." 31 May 2012, Washington, DC, p. 2.
Grevi, Giovanni. 2009. *The Interpolar World: A New Scenario*. Paris: European Union institute for security studies.
Hellard, B. 2020. "EU Seeks to New Regulatory Powers against Big Tech Firms: Powers Could Include the Ability to Exclude Large Tech Companies from the Single Market Altogether", ITPro., September 21. Accessed 18 May 2021. https://www.itpro.co.uk/business/policy-legislation/357172/eu-seeks-new-regulatory-powers-against-big-tech-firms
Ikenberry, G. John. 2011. "The Future of the Liberal World Order: Internationalism after America." *Foreign Affairs* 90 (3): 56–68.
Kello, L. 2017. Cyber Security: Gridlock and Innovation Held, David, Hale, Thomas eds. Beyond Gridlock. Cambridge: Polity.
Klimburg, A., and L. Faesen. 2020. " A Balance of Power in Cyberspace." In Broeders, Dennis, van den Berg, Bibi eds. *Governing Cyberspace: Behavior, Power and Diplomacy* (London: Rowman & Littlefield), 145–172.
Klose, S. 2018. "Theorizing the EU's Actorness: Towards an Interactionist Role Theory Framework." *JCMS: Journal of Common Market Studies* 56 (5): 1144–1160.
Kobayashi, Bruce H., and Larry E. Ribstein. 2003. "Multijurisdictional Regulation of the Internet." In *Who Rules the Net? Internet Governance and Jurisdiction*, edited by Thierer, A. and C Crews Jr, 159–215. Washington, Cato Institute.
Koutrakos, Panos. 2013. *The EU Common Security and Defence Policy*. Oxford University Press.
Kurowska, X. 2019. The Politics of cyber norms: Beyond Norm Construction towards Strategic Narrative Contestation. (Paris/Brussels: EU Institute for Security Studies).
Laatikainen, Katie Verlin. 2012. "EU Multilateralism in a Multipolar World." In *Routledge Handbook on the European Union and International Institutions*, 472–487. Routledge.

Langenhove, Van, and Luk. 2010. "The EU as a Global Actor in a Multipolar World and Multilateral Environment (Egmont Papers-36)."36 Academia Press
Liebetrau, Tobias, and Kristoffer Kjærgaard Christensen. 2021. "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites, and Spaces." *European Journal of International Security* 6 (1): 25–43. doi:10.1017/eis.2020.10.
Lu, W. 2015. "Cyber Sovereignty Must Rule Global Internet." available at https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060, accessed on 11 October 2021.
MalcolmTurnbull. 2015. "Australia Is Committed to a multi-stakeholder System of Internet Governance", Press Release on Malcolm Turnbull MP Website." 15 March 2014. Accessed 16 May 2021. https://www.malcolmturnbull.com.au/media/australian-committed-to-a-multi-stakeholder-system-of-internet-governance
Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul de Hert. 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. doi:10.1016/j.clsr.2019.06.007.
Michel, Charles 2021. "Speech by President Charles Michel at "Masters of Digital 2021." online event, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/, accessed on 11 October 2021.
Mitchell, T. 2016. "Xi's China: Smothering Dissent", Financial Times. Accessed 12 May 2021. https://www.ft.com/content/ccd94b46-4db5-11e6-88c5-db83e98a590a
Morgus, Robert. 2018. " The Spread of Russia"s Digital Authoritarianism." In Wright, Nicholas D. ed. *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspective* 85–93. and Creative 85.
Mueller, Milton. 2017. "Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings." *Digital Policy, Regulation and Governance* 19 (6): 415–428. doi:10.1108/DPRG-05-2017-0025.
NATO. 2021. Cyber defence, available at https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en, accessed on 12 November 2021.
NTIA 1998. "Statement of Policy on the Management of Internet Names and Addresses", available at: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses
Odermatt, J. 2018. "The European Union as a Cybersecurity Actor." In Blockmans , Steven, Koutrakos , Panos eds. *Research Handbook on the EU's Common Foreign and Security Policy* Research Handbooks in European Law series. Camberley/Cheltenham: Edward Elgar Publishing. 354–373.
Parliament, European. 2004. "Critical Infrastructure Protection in the Fight against Terrorism."
Petito, Fabio. 2016. "Dialogue of Civilizations in a Multipolar World: Toward a multicivilizational-multiplex World Order." *International Studies Review* 18 (1): 78–91. doi:10.1093/isr/viv030.
Post, David G., and David R. Johnson. 1997. "Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized decision-making in Complex Systems." *Chi.-Kent L. Rev* 73: 1055.
Prabhakar, Akhilesh Chandra. 2016. "Trade and Economic Integration in BRICS: Towards Multi-Polarity Erokhin, Vasily ed. ." In *Global Perspectives on Trade Integration and Economies in Transition*, 45–57. Hershey, Pennsylvania: IGI Global.
Prontera, Andrea. 2020. "Beyond the Regulatory State: Rethinking Energy Security Governance and Politics in the European Union." *Comparative European Politics* 18 (3): 330–362. doi:10.1057/s41295-019-00188-z.
Reidenberg, Joel R. 2000. "Resolving Conflicting International Data Privacy Rules in Cyberspace." *Stanford Law Review* 52 (5): 1315–1371. doi:10.2307/1229516.
Ruiz, D. 2020, "GDPR: An Impact around the World." https://blog.malwarebytes.com/privacy-2/2020/04/gdpr-an-impact-around-the-world/ Accessed 20 May 2021.

Schuetze, J. 2020. *EU-US Cybersecurity Policy Coming Together*. Leiden, Netherlands: EU Cyber Direct.

Schweller, Randall L., and Pu. Xiaoyu. 2011. "After Unipolarity: China's Visions of International Order in an Era of US Decline." *International Security* 36 (1): 41–72. doi:10.1162/ISEC_a_00044.

Schünemann, W. J., and M. O. Baumann, Eds. 2017. *Privacy, Data Protection and Cybersecurity in Europe*. Cham, Switzerland: Springer International Publishing.

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Hachette UK.

Segal, A. 2018. "When China Rules the Web," *Foreign Affairs*, September/October 2018, available at https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web, accessed on 10 October 2021.

Singh, P. V. 2013. "India Won't Sign Budapest Pact on Cyber Security". Governancenow. Accessed 12 April 2021. http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security

Soesanto, S. 2021. "After a Year of Salience, are EU Cyber Sanctions Dead." Lawfare, available at https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead,accessedon 11 November 2021.

Sun, Haiyong. 2019. "US-China Tech War: Impacts and Prospects." *China Quarterly of International Strategic Studies* 5 (2): 197–212. doi:10.1142/S237774001950012X.

Tonra, Ben, and Thomas Christiansen, edited by. *Rethinking European Union Foreign Policy*. Manchester University Press.

Wessel, Ramses A. 2015. "Towards EU Cybersecurity Law: Regulating a New Policy Field." In Tsagourias, Nicholas, Buchan, Russell eds. *Research Handbook on International Law and Cyberspace* Research Handbooks in International Law series. Camberley/Cheltenham: Edward Elgar Publishing. 403–425.

Wessel, R. A. 2019. "Cybersecurity in the European Union: Resilience through Regulation." In *Routledge Handbook of EU Security Law and Policy*, edited by Conde, Elena, Zhaklin Yaneva, and Marzia Scopelliti, 183–300. Abingdon: Routledge.

Wessel, Ramses A., and Leonhard den Hertog. 2013. " EU Foreign, Security and Defence Policy: A Competence-Responsibility Gap." In Evans, Malcolm, Koutrakos, Panos eds. *The International Responsibility of the European Union:Europeanand International Perspectives* (Oxford: Hart Publishing). 339–358.

World Internet Conference (Wuzhen Summit). 2019. "Building A Community with A Shared Future in Cyberspace." Accessed 18 Aril 2021. http://www.wuzhenwic.org/communitywithasharedfutureincyberspace.html

Zwolski, Kamil, and Christian Kaunert. 2013. *The EU as a Global Security actor–a Comprehensive Analysis beyond CFSP and JHA* Palgrave Studies in European Union Politics. Basingstoke: Palgrave Macmillan.