THE INTERNATIONAL SPECTATOR
2022, VOL. 57, NO. 3, 48–65
https://doi.org/10.1080/03932729.2022.2066841

Istituto Affari Internazionali
Routledge
Taylor & Francis Group

RESEARCH ARTICLE

Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance

Xuechen Chen [a] and Yifan Yang[b]

[a]New College of the Humanities at Northeastern University, London; [b]East China Normal University, Shanghai

ABSTRACT

In order to better capture the dynamics of global cyber governance, it is important to go beyond the established West vs. non-West dichotomy in the scholarly literature and thus develop a more nuanced understanding of the variations of cyber governance norms and approaches within and beyond the traditional Western camp, as well as to take into account the role of regional organisations in reshaping the normative framework of cyber governance. Indeed, the European Union is emerging as a new norm entrepreneur and autonomous regional actor in cyber governance by proactively projecting its regulatory and normative power in the digital sphere. In contrast, the development of ASEAN's cyber governance norms is a process of norm subsidiarity based on ASEAN's unique diplomatic culture and normative structure characterised by the ASEAN Way and the principle of ASEAN centrality.

KEYWORDS

cyber governance; norms: Westlessness; EU; ASEAN

Since the mid-1990s, a ubiquitous, borderless and virtual cyberspace has penetrated political, social and economic life globally, with a great influence on international affairs. This article will look at the governance of cyberspace, which provides a testing ground for global governance to innovate on its institutional and normative foundations. Because of the diversity of the actors – states and non-state actors – involved in global cyber governance, they have taken formal and informal approaches based on their respective priorities and interests. On the one hand, formal approaches such as international treaties and governmental regulations negotiated by sovereign states through multilateral mechanisms have been implemented mainly to regulate the behaviours of states in cyberspace. Arguably, cyberspace is subject to international law, especially the United Nations (UN) Charter, and is regulated by the relevant UN bodies like the International Telecommunications Union, a specialised UN body and the oldest Information and Communication Technologies (ICTs) organisation (Tsagourias 2015, 13). Compulsory international law, however, can always encounter resistance from sovereign states, as it may limit their options for action in cyberspace and clash with their varying interests. On the other hand, therefore, a growing number of flexible approaches, including cyber norms and confidence- and capacity-building measures based on them, have been

CONTACT Xuechen Chen xuechen.chen@nchlondon.ac.uk @irischenxc1

pursued, which can be an alternative and supplementary approach to the effective governance of cyberspace. It accounts for norms as a means to the end of increasing the effectiveness and legitimacy of global governance, in that more appropriate norms formulated through global governance will better inform the calculations of international actors, stabilise their expectations and direct them towards collaborative behaviour (Linsenmaier *et al.* 2021, 3–4; 6).

In discussions about who shoulders the responsibility for governing cyberspace, a heated debate has ignited between Western and non-Western countries. Admittedly, the West – mainly referring to the United States (US) and European Union (EU) – does enjoy a privileged position in cyber governance because of its power over the technological, institutional and normative aspects. However, its superiority is eroding, as evident in the popularity of the notion of "Westlessness" in political and academic discussions after the Munich Security Conference in 2020.[1] In short, Westlessness was described as "the sense that the world, but also the West itself, was getting less Western, less rule-based, less value-oriented" (*Securityconference.org* 2021). Following this logic, it seems that the West is now so divided and challenged by the rise of the East, especially China,[2] that its entire existence is imperilled. Responding to these discussions, Joseph Nye (2020) suggests that the West will still hold an advantage in its competition with China unless it loses its confidence and is overwhelmed by the rise of populist isolationism at home. Yet, overemphasising Westlessness might miss the key point of governance discussions to some extent, given that we are gradually witnessing a world without the West's dominance but not without the West's ideas.

Against this backdrop, because of the diversification of approaches and interests of different actors, global cyber governance systems may become more fragmented, while also creating space for further dialogue and enhanced cooperation rather than compulsory standards imposed only by Western countries. To be sure, according to the report "Cyber Capabilities and National Power: A Net Assessment" (IISS 2021), the US remains the world's dominant power in cyberspace as it has been since the mid-1990s, given that it is the only country with a heavy global footprint in both the civil and military use of cyberspace. However, the US' central position has been challenged by such stakeholders as sovereign states, regional organisations and private sectors within and beyond the West. Among these challengers, regional organisations such as the EU and the Association of Southeast Asian Nations (ASEAN) have a special role to play.

Within the Western world, the cyber governance strategies of the US and the EU are not as aligned as expected (Komaitis and Sherman 2021). Facing the US' securitisation of cyberspace and the fierce competition over cyberspace between the US and China, the EU has introduced the concept of 'digital sovereignty', which both reflects and shapes the different political contexts in which member states are designing their respective cyber governance models. To protect the EU's digital economy and counter competition from the US and other nations, Brussels is planning to adopt more regulations. In general, the EU and its member states are more willing to embrace regulation than the US (Burwell and Propp 2020; Taylor and Hoffmann 2019, 17). Outside the Western world, a regional organisation such as ASEAN, due to the heterogeneity among its

[1]See Chen and Yang's (2022, 1–14) discussion of Westlessness.
[2]See Gao's (2022, 15–30) article on China's approaches to cyber governance.

member states in terms of regime type and technical capabilities, resorted to norm subsidiarity by either reaffirming international norms in the local context or highlighting regional norms that are integral to preserving the autonomy of its member states (Ali 2021, 133–4).

As two important regional organisations with different characteristics, the EU and ASEAN have therefore developed their respective institutional and normative frameworks to address the challenges and problems of cyberspace. The EU has taken on the role of norm entrepreneur both within and beyond its borders, aiming to apply "the same norms, principles and values that the EU upholds [namely, fundamental rights, democracy and the rule of law] to the online" space (Claessen 2020, 152); at the same time, it has also moved to more inward-looking cyber governance. The ASEAN method of cyber governance is reflected in its confidence- and capacity-building measures, intended as practical solutions to establish region-wide cyber norms (Tran Dai and Gomez 2018, 229) while still maintaining strict adherence to the historical principle of non-interference in the internal affairs of ASEAN member states. Both the EU within and ASEAN without the Western camp thus seem to be adopting approaches to cyber governance beyond traditional Western-centric methods, reflecting their regional specificities instead. In any event, this diversity of approaches to cyber governance clearly shows that the 'West' and the 'non-West' are not homogenous camps or blocs.

By studying and comparing the normative and institutional foundations of the cyber governance practices of the EU and ASEAN, this article aims to discuss and compare their respective approaches to governing cyberspace, to determine how Westlessness has gradually emerged as the 'new normal' in cyber governance. The remainder of this article consists of four sections. The first provides an overview of cyber governance practices in international politics and the importance of cyber norms in governing cyberspace. The second offers a comparison between the EU's and ASEAN's norms and approaches to cyber governance, shedding light on how the traditional Western-centric approach has been challenged within and beyond the Western world and how a critical conceptualisation of Westlessness can contribute to an understanding of the fragmented structure of cyber governance and to moving beyond it. The third discusses how EU–ASEAN interactions and engagement in cyber governance can contribute to dissolving the West vs. non-West dichotomy, followed by a conclusion.

Cyber governance and cyber norms

Cyber governance in a globalised world

Since the mid-1990s, governing the Internet by allocating network addresses and domain names to users at the international level has gradually become a fundamental practice (Mueller, Mathiason *et al.* 2007, 237), evidenced by the founding of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. However, global cyber governance means more than that. Indeed, cyberspace is much broader than just the Internet and consists of four layers: its physical foundations, the platforms (the Internet being just one of them), the information and the people involved (Choucri and Clark 2018, 35). Thus, the governance of cyberspace involves different factors across these different layers.

The diversity of actors pertinent to the question of who should govern cyberspace further increases the complexity of global cyber governance (Jayawardane *et al.* 2015, 16). A rising number of issues relating to new practices of cyber technology utilisation – from the destruction of physical infrastructure and the compromise of logical elements to the manipulation of information and deception of users – need to be managed through policymaking and coordination (Choucri and Clark 2018, 39). The use and abuse of this complex, borderless and virtual space can impinge on economic development, public safety and even security across national borders in the physical world (Macak 2017, 879). Accordingly, the conflict between maintaining freedom in cyberspace as a basic human right and re-territorialising cyberspace under national sovereignty makes cyber governance a rather complicated domain and calls for global cooperation in structuring public policies at a global level.

To deal with the complexity of global cyber management, two competing modes of governance – multi-stakeholderism and multilateralism – have emerged. The multi-stakeholder mode is understood as "a constantly shifting balance of powers between private industry, international technical governance institutions, governments, and civil society"; it centres on questions concerning what form of administration is necessary in any particular context rather than isolating a single value that needs to be applied widely (DeNardis 2014, 226–7). In this sense, the multi-stakeholder mode diversifies the participants in cyber governance, thus diminishing the power of sovereign states in this domain. In contrast, the multilateral approach places state sovereignty centrally; it "views cyberspace in Hobbesian terms and supports the role of sovereign states in formulating international public policies in cyberspace", which is advanced by Russia, China and most developing countries (Liaropoulos 2016, 18).

Traditionally, there has been a consensus in the West that cyberspace, as a global common comprising areas and resources that are not subject to the national jurisdiction of a particular state, is incompatible with sovereignty (Schrijver 2016, 1252). Instead, this view holds that the cyber domain must follow a bottom-up transnational governance approach that mainly stresses the role of private actors (Mueller, Milton 2020, 780). Thus, it aims to 'keep the state out' of cyber governance and insists on the multi-stakeholder mode to ensure the domain's openness and robustness (Fang 2018, 126). Although multi-stakeholderism has the potential to weaken sovereign states' influence, the same Western countries that advocate for this mode do enjoy advantages from it, given that they are home to influential Internet companies or play a predominant role in non-governmental organisations pertinent to cyber governance (Jayawardane *et al.* 2015, 6). Thus, in contrast to the official multi-stakeholder discourse over cyber governance, Western countries can still benefit from multi-stakeholderism to enhance their sovereign rights in practice.

With the growing influence and participation of various actors from the non-Western world in cyber governance, a state-centric multilateral approach has been proposed. Several non-Western countries have tried to apply sovereignty to the domain of cyberspace by arguing that this domain cannot exist without support from infrastructures and digital equipment in the physical world (Shen 2016, 83). Emerging and developing countries in the non-Western bloc, particularly Russia and China, claim that the Internet has a rather negative influence on politics and morality (Pew Research Center 2015, 30), strengthening the importance of the state in regulating cyberspace. The proponents of

state-centric multilateralism consider that powerful states are still the most important actors on the world stage governing the social and political externalities created by globalisation and the Internet: therefore, they believe that the multi-stakeholder mode of global cyber governance only focuses on a small part of the larger question of how globalisation affects global governance and departs from the inaccurate assumption that globalisation leads to the rise of non-state actors and the decline of states (Drezner 2004, 477-8).

More importantly, the argument for state-centric multilateralism is underpinned by demographic factors. Given that, by 2020, over 90 per cent of Internet users were from countries not included in the Organisation for Economic Co-operation and Development and that the influence of non-Western countries in the world economy is growing, cyberspace is becoming more international and less Western-centric. Furthermore, with the increasing capacity of non-Western countries in physical infrastructure and normative influence, a shift to a non-Western world of cyber governance has begun to emerge (Nocetti 2015, 111, 120).

This growing influence of the non-Western world has led to the trend of Westlessness being spotted in almost every aspect of global governance. Several scholars have argued that the two competing approaches to cyber governance of multi-stakeholderism and multilateralism are split between Western and non-Western countries respectively, leading to conflicts over the institutions and norms in the cyber domain based on their relative levels of power and interests (Liaropoulos 2016, 19). However, overemphasising this dichotomy certainly misses the opportunity for future collaboration and cooperation between the West and the non-West based on norm interaction and policy convergence. Indeed, a strong dichotomy between the West and non-West already partly misrepresent reality, since internal friction and divergence can be witnessed in both camps, as highlighted by the regional approaches of the EU and ASEAN that we will discuss below.

Cyber norms and their dynamics

The effectiveness and legitimacy of global governance call for universally accepted norms; so too does cyber governance. Norms – standards determining the appropriate behaviour of actors within a given identity – embody 'oughtness' and shared moral assessment (Finnemore and Sikkink 1998, 891–2). Therefore, implementing international norms is a core aspect of global governance (Jörgens 2004, 246). However, something cannot be declared a norm just by saying so. Rather, a norm can only exist when relevant actors or groups agree with and hold particular beliefs about expected behaviours. Therefore, a norm emerges not only because it has been proposed and announced as a solution to the puzzle of what substantive normative prescriptions will address a given problem, but also because others "buy in and recognize that the norm's behavioural prescriptions apply to them (or to other actors who can be held to account)" (Finnemore 2017).

Cyber governance is urgent, but it faces a rising number of problems and challenges ultimately rooted in diverse communities of actors – a heterogeneity that requires equally diverse normative solutions (Finnemore and Hollis 2016, 427). As the most important actor in global governance, the UN has a crucial role to play in producing and diffusing cyber norms. Indeed, the First Committee of the United Nations General

Assembly (UNGA) placed cyber norms on its agenda already in 1998 (Raymond 2016, 123). Within the UN, norms and principles establishing regulations on responsible behaviours are generated and diffused by specific working groups of UN institutions. There are two such groups that have worked to do so in the field of cyber governance. One is the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (formerly known as the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security), established in 2004; the other is the Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security, established in 2018.

In its 2015 report, the GGE demands that full respect for human rights, such as privacy, freedom of expression and free flow of information, should be included as cyber norms. More importantly, the GGE's 2015 report also offers eleven voluntary, non-binding norms, rules or principles of responsible behaviour of states that aim at promoting an open, secure, stable, accessible and peaceful ICT environment (UNGA 2015). These norms are also included in the final report of the OEWG in 2021 (UNGA 2021a). Furthermore, the GGE's 2021 report reaffirms the applicability of international law, and in particular the UN Charter, in its entirety to the ICT environment, also noting the applicability of international humanitarian law in situations of armed conflict (UNGA 2021b). This inclusion addresses a gap in its 2015 report regarding how international law can be applied to cyberspace (Korzak 2015). Ironically, besides reflecting the expectations of the international community and setting standards for responsible international behaviours, the reports of GGE 2015 and OEWG 2021 also emphasise that norms allow the international community to assess the activities and intentions of states, although this phrase is missing in the 2021 GGE's report. Thus, the eleven norms included in the 2015 and 2021 GGE's reports still seem rather thin and even threadbare, without any concrete measures to regulate and assess the compliance of the states.

Because of the limitations of the diffusion of cyber norms through UN systems, sovereign states on the world stage strive to produce and promote different versions of such norms in relation to their own political and technological contexts. Western countries, particularly the US, highlight Internet openness, security, liberty and free speech, with minimal government oversight and surveillance, as their preferred cyberspace norms (Farrell 2015). Net neutrality was once regarded in the West as a globally applicable principle to governing cyberspace because of the technological and normative aspects of Internet connectivity. Given that cyberspace does not conform to national borders, the argument goes, it can operate smoothly based on self-regulation without interference from network operators or overbearing governments (Mueller, Cogburn *et al.* 2007). On the contrary, any attempts to expand sovereign control over cyberspace will jeopardise the US' long-held belief in guaranteeing a free, open and liberal cyberspace (Runde and Ramanujam 2021).

Other countries within and outside the Western world have come to see the content distributed and diffused in cyberspace as a potential and even real threat to domestic values and stability that needs to be managed or controlled rather than encouraged (Flonk *et al.* 2020, 368). They strive for the recognition and legitimacy of state control over cyberspace and highlight such norms as state rights, information security, territorial

integrity, national sovereignty and domestic stability. Thus, the proliferation of cyberspace and the diversity of its users have shifted the centre of gravity of cyberspace away from the US, bringing with it a shift in cyber norms specifically. At the same time, a worrying increase in states' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of other states has also been documented (UNGA 2021b), evident in accusations of spreading disinformation, popularised during the Covid-19 outbreak (Burwell and Propp 2020).

Against this backdrop, critical discussions over Westlessness seem to offer an opportunity for the West and non-West to dialogue and mutually shape cyber norms through socialisation. Socialisation is commonly used to describe how international actors develop shared cognitive beliefs and norms by interacting with each other. This process, in turn, contributes to shaping actors' perceptions of the legitimacy of certain norms or policies and may result in the redefinition of actors' normative considerations due to the internalisation of such norms (Checkel 2005; Finnemore and Sikkink 1998). In the conventional literature on norm diffusion, socialisation is conceptualised as a one-way process that induces actors to adopt the norms of a given society (Checkel 2005). In this view, it is often Western powers that socialise non-Western actors into the West-dominated international society through the diffusion of their preferred norms and rules. This vision has recently been challenged by numerous scholars who argue that, as non-Western actors gain increasing clout in global politics, socialisation should be understood as a two-way process (Pu 2012; Chin 2012) wherein an international actor can actively shape norms while simultaneously being a receiver of international normative pressure (Pu 2012).

Considering that a rising number of actors participate in cyber governance, emphasising US dominance thus seems to contradict the reality in the field. In fact, the differences and even conflicts over cyber governance between the US and other nations reflect a trend of challenging US dominance within and outside the Western world in this domain (Nocetti 2015, 112). This, however, does not necessarily imply responsibility must be entirely handed over to sovereign states. Indeed, applying national sovereignty to cyberspace might also harm its smooth operation as a global public good that benefits all citizens of the world and is global in scope. In consequence, regional approaches to cyber norms might provide a balanced and workable way for cyber governance to proceed.

Regionalisation grants regions and regional organisations a central place in global governance. Compared to bodies like the UNGA, regional organisations, with fewer members involved, can offer greater legitimacy and easier consensus-building. They have better insights into national priorities and cultures, and more efficient mechanisms to advance cooperation. Thus, regional organisations, including the EU and ASEAN, have a special role to play in cyber governance by both protecting the interests of regions and member states and importing international norms and exporting domestic (regional) norms.

EU and ASEAN approaches to cyber governance

By examining the approaches to cyber governance taken up by the EU and ASEAN, this section shows that both organisations have developed a set of distinct norms and

instruments for cyber governance based on their pre-existing normative structures, political and institutional contexts, and the maturity levels of their cyber capabilities. Both the EU and ASEAN have contributed to contesting and challenging the US-centric approach to cyber governance, albeit in different ways. Specifically, through the active promotion of a set of EU-specific norms and regulations in cyberspace, as well as the idea of digital sovereignty, the EU has increasingly been regarded as a nascent norm entrepreneur in global cyber governance, seeking to contest and reform the normative framework of this field predominated by the US from within the Western camp. ASEAN, in contrast, embraces a different set of cyberspace norms that derive primarily from its unique diplomatic culture and cognitive structure, namely the 'ASEAN Way', which emphasises informality, organisational minimalism, inclusiveness, intensive consultations and non-interference (Acharya 1998). Although ASEAN has not yet proactively externalised its cyber norms and approaches, its prioritisation of principles such as non-interference, consensus-based decision-making, regional autonomy and ASEAN centrality has resulted in the development of a distinct, non-Western approach to cyber governance, drawing on the pre-existing normative structure of the Southeast Asian context.

The EU's approach to cyber governance

Over the last two decades, the EU has emerged as a nascent but increasingly important actor in the field of cyber governance (Dunn Cavelty 2018). At the fundamental level, the normative underpinnings of the EU's approach to cyberspace have generally aligned with the US and the wider Western community in the sense that they all embrace several core principles, such as freedom, openness, interoperability and multi-stakeholderism (Taylor and Hoffmann 2019). The EU's Council Conclusions on Internet Governance, published in 2014, provide good examples of the common values and interests held by the EU and the US-led Western camp, including the development of "a vision of Internet as a single, open, neutral, free, un-fragmented network" and the "commitment to promote multistakeholder governance structures" (Council of the EU 2014, 3–4).

Nevertheless, the past two decades have witnessed the growth of normative fault lines between the cyber approaches of the EU and the US. The EU's norms and practices in the digital sphere have emerged as a new variant of the Western approach previously dominated by the US (Drissel 2006). The rise of the EU as a distinct normative power (Manners 2002) and norm entrepreneur in cyber governance has contributed to contesting and unsettling the US-centric approach from within the Western community. Despite sharing several common cyber principles with the US, the EU's normative underpinnings and practices differ from the US' approach in at least two broad dimensions: (i) the preference for a regulatory strategy, as evidenced in the expansion of the "Brussels effect" in the digital sphere (Bradford 2020, 1); and (ii) the prioritisation of EU-specific fundamental values in this arena.

First, whereas the US has long preferred a privatised model or a 'hands-off-the-Internet' approach (Komaitis and Sherman 2021), thus favouring a free market-driven economy with limited government-led regulatory interference and decentralised governance (Taylor and Hoffmann 2019; Drissel 2006), the EU has sought to expand its sphere of influence in cyberspace by proactively reinforcing regulatory standards not only

within the Union but also beyond its borders (Wessel 2019). The EU has thus become a newly emerging "regulatory power" in cyberspace, especially in the sphere of transnational data governance (Liaropoulos 2021). This line of argument echoes Anu Bradford's (2020) conceptualisation of the "Brussels effect", which refers to the global influence of the EU's regulatory policies resulting from the Union's externalisation of its laws and regulations outside its borders through market mechanisms, generating a "Europeanisation" of regulations and standards across the globe (see also Bygrave 2021).

One example of the EU's promotion of regulatory power can be found in its data protection regime. Adopted in 2016, the General Data Protection Regulation (GDPR) establishes strict conditions on the handling of the personal data of EU citizens, asserting jurisdiction over the processing of European personal data even in the case that the data or citizens are physically outside of the EU. By adopting the GDPR, the EU established a rigorous framework designed to harmonise data privacy laws across member states with an aim to "strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market" (European Commission 2022a). The GDPR not only marks a crucial development in the EU's internal data protection regime but also has a strong external dimension in the sense that European data protection law became applicable outside the borders of the EU. Specifically, under the GDPR, the EU's territorial scope was broadened so that non-EU data controllers and processors must comply with specific data protection obligations when they process data from individuals within the EU (European Union 2016). EU member states' national implementation of the GDPR means that companies can only transfer personal data out of the European Economic Area to jurisdictions that have been recognised by the European Commission as providing adequate protection for personal data (European Commission 2022b). As the EU represents one of the largest and most developed consumer markets worldwide, large multinational firms tend to comply with these data protection obligations as the price of doing business in the EU. Since such corporations prefer to streamline business operations, they often voluntarily apply these regulations to their global operations so as to avoid the costs of adhering to multiple regulatory regimes (Kuo 2021; Mahieu *et al.* 2021). Indeed, large corporations such as Apple, Google, Facebook and Microsoft decided to adopt one global privacy policy that heavily mirrors the GDPR (Kuo 2021). As pointed out by numerous scholars, the GDPR is thus a telling example of the 'Brussels effect', a phenomenon wherein the regulations and rules set by the EU result in a tangible impact on global economic activities and the lives of citizens beyond the EU's borders (Bradford 2020; Mahieu *et al.* 2021).

In addition, the EU has proactively encouraged third countries to adopt GDPR-like regulations and laws, and its regulatory approach has indeed proven attractive to numerous third countries. An interesting example of how the EU has exercised its regulatory power to pressure other economies to adopt or emulate its data protection law can be found in the EU–Japan Economic Partnership Agreement (EPA). During the negotiation process, Brussels maintained that data protection is a fundamental right in the EU, and therefore it is not up for negotiation (Kanetake and Taylor 2017). To obtain reciprocal adequacy, Japan decided to implement additional safeguards and put in place stricter regulations for the transfer of personal data. Following Japan's remodelling of its regulations, the EU and Japan eventually agreed to recognise each other's data protection

regimes in July 2018. This is indicative of the EU's increasing ambition to provide leadership in shaping regulatory environments in cyberspace.

The second feature characteristic of the EU's approach to cyber governance lies in the Union's prioritisation and active promotion of a specific set of socio-political norms and values in cyberspace. Specifically, the EU's approach to cyber governance attaches more importance to defending the universal values and norms (for example, peace, liberty, democracy, the rule of law and respect for human rights) that lie at the core of the EU's international identity (Diez 2005). As noted by Ian Manners (2002, 239), the EU distinguishes itself from other international actors through its "normative power of an ideational nature characterised by common principles and a willingness to disregard Westphalian conventions". The EU's intention to act as a normative power is particularly well reflected in the Union's approach to cyber governance. Remarkably, its first cybersecurity strategy, published in 2013, stresses that "the same norms, principles and values that the EU upholds offline, should also apply online" and that "fundamental rights, democracy, and the rule of law need to be protected in cyberspace" (European Commission 2013, 2). Moreover, Brussels has played an increasingly proactive role in diffusing its rights-based and value-driven cyber governance model through its external relations. For example, in its External Cyber Capacity Building Guidelines, the Council points out that the EU should use its cyber diplomacy tools and external cyber capacity to promote and protect human rights, digital gender equality, the rule of law and sustainable development (Council of the EU 2018, 3). The document also stresses that the EU's cyber governance approach should be "rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms" (7).

Furthermore, in recent years, the notion of "technological or digital sovereignty" has emerged as a new theme within the EU as a means of promoting European leadership and strategic autonomy in the digital field. This focus reveals the EU's ambition to "act independently in the digital world" against the backdrop of growing rivalry between the US and China over 5G, artificial intelligence (AI), cloud computing and the Internet of Things (IoT). The EU's promotion of digital sovereignty largely results from mounting concerns over the socio-economic impact of non-EU technology companies, which not only constrain the growth of EU high-tech firms and the ability of EU rule-makers to enforce their laws and regulations, but also threaten the EU's control over personal data (European Parliament 2020). In conclusion, although still aligning with the US on core interests and values in cyber governance, the EU's recent cyber strategies manifest stronger intentions to counter the position of US digital companies in the European market while also seeking a greater level of autonomy in the digital sphere (Burwell and Propp 2020).

ASEAN's approach to cyber governance

In contrast to the EU's role as a proactive norm entrepreneur, ASEAN's approach revolves around "norm subsidiarity", whereby local actors establish new rules or reaffirm international norms in the regional context with the aim of preserving their autonomy from neglect, dominance or abuse by powerful external actors (Acharya 2011; Ali 2021). Based on analysis of the institutional structure and key documents related to ASEAN's digital and cyber policies, we observe that its approach to cyber

governance has two distinct characteristics: (i) the guiding principles and norms that ASEAN adopts resonate strongly with the conventional ASEAN Way; and (ii) the principle of ASEAN centrality constantly features in the grouping's vision of cyber governance, particularly in its cooperation with external actors in the digital sphere.

A close look at the normative underpinnings of ASEAN's cyber governance reveals that its norms and practices in the cyber context have been rendered subsidiary to the organisation's longstanding regional norms – namely, the ASEAN Way. While the meaning of the ASEAN Way has been contested, the term is commonly adopted by ASEAN policy-makers and scholars to describe the organisation's pattern of intramural interaction, which differs from Western multilateralism (Acharya 2011). The ASEAN Way includes norms such as respect for state sovereignty, non-interference, informality, organisational minimalism and intensive consultations leading to consensus, which stand in contrast to legally binding agreements and regulatory frameworks (Solingen 2005; Haacke 2013). As far as cyber governance is concerned, in 2018, during the third ASEAN Ministerial Conference on Cybersecurity held in Singapore, its member states decided to endorse the eleven voluntary and non-binding norms recommended by the UN's GGE in 2015 (Van Raemdonck 2021). At first glance, ASEAN would thus appear to be a passive norm recipient of the GGE norms for cyber governance. However, a more detailed investigation into recent policy documents and practices suggests that, through the process of norm subsidiarity, the grouping has become an increasingly important contributor to the international debate on cyber governance norms by highlighting its pre-existing norms and the diplomacy culture of the ASEAN Way (Haacke 2013).

ASEAN's institutional framework and policies related to cyber governance have been largely informed by the organisation's fundamental principles of non-interference in member states' domestic affairs, consensus-based decision-making, and informal and non-binding institutional mechanisms that typically result in memoranda, declarations, statements and loose cooperative initiatives (Ali 2021). Instead of leaning towards legally binding treaties and highly institutionalised policy initiatives, ASEAN's regional cyber cooperation is defined by strict adherence to an intergovernmental approach. For example, within the organisation's institutional structure of the digital sector, the ASEAN Digital Ministers' Meeting (ADGMIN), previously ASEAN Telecommunications and Information Technology Ministers Meeting – a ministry-level event held annually by ASEAN – serves as the most important institutional platform for promoting cooperation in ICT sectors among the ten member states. While ADGMIN is responsible for setting the overarching direction of ICT-related policy, ASEAN's cooperation in the digital sphere is supported by several institutional organs, such as the ASEAN Digital Senior Officials' Meeting, the ASEAN Telecommunication Regulators' Council and the ASEAN ICT Centre. Although each aims to deepen cooperation among ASEAN member states, their working mechanism complies strictly with the ASEAN Way in the sense that all policy initiatives are non-binding and based on the principle of non-interference in the internal affairs of member states, as set out in the ASEAN Charter (ASEAN 2008).

Another example of ASEAN's adherence to the subsidiary norms of the ASEAN Way in cyber governance can be found in the ASEAN Framework on Personal Data Protection, which seeks to strengthen the protection of personal data in the ASEAN region with

a view to promoting the regional flow of information (ASEAN 2015). This initiative sets an ambitious goal, aiming to facilitate the transformation of ASEAN into a secure, sustainable and digitally enabled economy, but its actual implementation is constrained by the principles of non-interference, informality and respect for individual member states' sovereignty and legal systems. As a result, instead of creating a binding regulation that harmonises domestic law on data protection in ASEAN member states, this framework encourages participants to promote and implement a set of principles surrounding personal data protection in their domestic regulations. In addition, member states that implement the framework can adopt exceptions that match their domestic circumstances. In contrast to the EU's GDPR, the framework does not result in the creation of legally binding domestic obligations for ASEAN member states (GSMA 2018).

In addition to resonating with the ASEAN Way, the second key feature of ASEAN's cyber governance approach is its emphasis on the principle of ASEAN centrality, that is, the idea that ASEAN should remain at the centre of the institutional architecture, driving wider regional cooperation initiatives in the Asia–Pacific region. ASEAN centrality constitutes an important principle informing the grouping's management of external relations with powerful agents, including China, the US, Japan and increasingly other actors such as South Korea, the EU and India. This principle has incrementally resulted in the creation of an ASEAN-led institutionalised system of dialogue partners, which can be seen as a distinct form of transregional cooperation in the Global South (Mueller, Lukas 2020). With regard to cyber governance, ASEAN demonstrates a strong desire to invoke and strengthen the principle of ASEAN centrality through ASEAN-led institutional mechanisms, such as the ASEAN Regional Forum (ARF) and ASEAN Plus Three. Remarkably, promoting cooperation on cybersecurity to create a resilient and secure regional cyberspace has become a top priority for the ASEAN Plus Three Cooperation Work Plan (2018–2022). The work plan seeks to promote the exchange of visits and enhanced dialogue and law enforcement on cybersecurity between ASEAN and three major regional actors: China, Japan and South Korea (ASEAN 2020). Furthermore, the ARF – a crucial ASEAN-led multilateral platform built for security dialogue in the Indo-Pacific region – has played a vital role in invoking ASEAN centrality in regional cyber governance. Since 2004, the ARF has regularly organised workshops and seminars on cyberspace, with a particular focus on cybercrime, cyber terrorism, national capacity-building and the threat of proxy actors (ARF 2012). Through the ARF, ASEAN has been particularly keen on promoting cyber confidence-building measures that resonate with its diplomatic culture, which encourages the gradual downplaying and prevention of disputes through building confidence. The ARF thus facilitates the creation of a regional cooperation approach to cyber governance that is primarily focused on the resilience of national capabilities and mutual confidence (Tran Dai and Gomez 2018), with ASEAN lying at the institutional and diplomatic centre of the wider Asia-Pacific region. In addition, recent analyses note that, instead of choosing between an exclusively state-centric multilateral cyber governance approach and a market-based multi-stakeholder approach, ASEAN seeks to be a "broker" between the Chinese and US approaches to cyber governance (Van Raemdonck 2021). Whereas ASEAN and China do share similar normative positions on the overarching principles of respect for state sovereignty and non-interference in internal affairs, subtle differences between ASEAN's and China's approaches to cyber governance can be observed. For

example, China has long been sceptical about the multi-stakeholder approach that is at odds with China's emphasis on sovereign government-led, multilateral cyber governance (Rosenbach and Chong 2019). In contrast, ASEAN has started to embrace the idea of multi-stakeholderism in cyberspace governance. As indicated in a recent policy paper entitled "ASEAN Cybersecurity Cooperation Strategy 2021-2025", ASEAN seeks to pursue a "multi-disciplinary, modular, measurable multi-stakeholder" approach to cybersecurity capacity building (ASEAN 2022). By highlighting the importance of both the "multilateral" and "multi-stakeholder" approaches, this document further demonstrates ASEAN's intention to carve out a middle way that transcends the US's and China's models of cyber governance.

EU–ASEAN engagement in cyber governance: bridging the West/non-West divide

Having analysed the respective normative structures and approaches to cyber governance of the EU and ASEAN, we will now move on to discuss the interregional interaction between these organisations in the digital sphere. In 2020, the EU and ASEAN upgraded their relations to form a "strategic partnership", which not only consolidated the existing cooperative arrangements between them but also paved the way for deepening cooperation in new policy areas, such as green growth, digital connectivity and cybersecurity (EU–ASEAN 2021). This EU–ASEAN interregional engagement with digital and cyber governance can be seen as a process of "two-way socialisation" through which both the EU and ASEAN act as proactive agents seeking to influence the content and outcome of norm diffusion and socialisation processes (Pu 2012). Through this process, which facilitates mutual understanding and the sharing of best practices, EU–ASEAN interregional interactions may contribute to bridging the normative divide between the West and the non-West in cyber governance.

Specifically, ASEAN has been keen on drawing lessons from the EU's approach to and experiences in the digital economy and connectivity, including the areas of policy, digital innovation ecosystems and regulation. For example, ASEAN has been increasingly willing to engage with EU-initiated projects on digital benchmarking indexes and to learn from the EU's experience in measuring the digital economy through the EU–ASEAN Regional Dialogue Instrument (European Commission 2019). Furthermore, with regard to the issue of data protection, policy-makers and researchers in ASEAN countries argue that "ASEAN needs to take lessons from the EU and come up with a proper framework that truly protects the privacy of its people without emboldening state powers", noting that ASEAN's policy on data needs to be comprehensive and all-encompassing, "similar to the one enforced by the EU" (*The ASEAN Post* 2018). Just as ASEAN manifests this strong interest, the EU has likewise been socialised by ASEAN-specific norms and principles through mutual engagement. Recent research on EU-ASEAN interregional relations shows that ASEAN's identities and norms have played a crucial role in reshaping the EU's perception of and resultant behaviours towards ASEAN. After gaining a better understanding of ASEAN norms, the EU has significantly elevated ASEAN's profile in its external relations and has incrementally recognised ASEAN as a strategic partner, rather than a norm recipient (Chen 2018). This process is particularly evidenced by the EU's increasingly proactive engagement with ASEAN Regional Forum's Inter-Sessional Meetings on ICT Security, as well as the

EU's willingness to support ASEAN's non-binding and voluntary approach and the principle of ASEAN centrality. As reflected in the EU-ASEAN Statement on Cybersecurity Cooperation adopted in 2019, the EU demonstrates a strong commitment to engaging in cybersecurity through relevant ASEAN-led mechanisms, including the ARF, the ADGMIN and the ASEAN Ministerial Conference on Cybersecurity (ASEAN 2019). As recognised by a recent study conducted by the EU Cyber Direct, the EU regards ASEAN centrality and the support for the ASEAN-led multilateral architecture in the Asia-Pacific region as an important aspect in the EU's cybersecurity strategy towards Asia (Van Raemdonck 2021).

Conclusion

By analysing the distinct regional norms and approaches to cyber governance undertaken by the EU and ASEAN, this article challenged existing scholarly views centring around the West vs. non-West dichotomy and the newly emerging concept of Westlessness in political and academic discussions. It demonstrated that, in order to better capture the dynamics of global cyber governance, it is important to develop a more nuanced understanding of the variations of cyber governance norms and approaches within and beyond the traditional Western camp, as well as taking into account the role regional organisations can play in reshaping the normative framework of cyber governance. In particular, this article showed that the EU is emerging as a new norm entrepreneur and autonomous regional actor in cyber governance. By proactively externalising its regulatory power in the digital sphere, prioritising a rights-based and value-oriented vision of cyber governance and promoting the idea of digital sovereignty, the EU contributes to challenging the predominant US-centric approach to cyber governance from within the Western community. In contrast, the development of ASEAN's cyber governance norms is a process of norm subsidiarity based on ASEAN's unique diplomatic culture and normative structure. This process results in the emergence of a distinct pattern of cyber governance based on the principles of the ASEAN Way and ASEAN centrality and renders ASEAN an increasingly important actor in cyber governance in the Asia-Pacific region, contributing to shaping the debate on the digital sphere from a non-Western perspective. In addition, EU–ASEAN interaction in cyber governance represents a good example of two-way socialisation between two regional organisations that have different normative underpinnings and visions regarding cyber governance. Instead of reinforcing the West vs. non-West fault line, EU-ASEAN inter-regionalism, by engaging in high-level dialogues, promoting cooperation programmes and developing new policy instruments, shows great potential to bridge the West vs. non-West divide in cyber governance norms and approaches in the future.

Notes on contributors

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

Yifan Yang is an Associate Professor in International Politics at East China Normal University, Shanghai, China. Email: yangyifanblue@gmail.com

ORCID

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

References

Acharya, Amitav. 1998. Culture, Security, Multilateralism: The 'ASEAN Way' and Regional Order. *Contemporary Security Policy* 19 (1): 55–84.

Acharya, Amitav. 2011. Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-making in the Third World. *International Studies Quarterly* 55 (1): 95–123.

Ali, Hanan Mohamed. 2021. 'Norm Subsidiarity' or 'Norm Diffusion'? *The Journal of Intelligence, Conflict, and Warfare* 4 (1): 122–48.

ARF (ASEAN Regional Forum). 2012. Co-Chairs' Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace. Seoul, Republic of Korea, 11-12 September. https://moam.info/arf-seminar-on-confidence-building-measures-in-cyberspace_59f42a1f1723dd150a32914c.html.

ASEAN (Association of Southeast Asian Nations). 2008. The ASEAN Charter. January. https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf.

ASEAN. 2015. The ASEAN ICT Masterplan 2020. https://www.gica.global/resources/asean-ict-masterplan-2020.

ASEAN. 2019. ASEAN-EU Statement on Cybersecurity Cooperation. https://asean.org/wp-content/uploads/2021/09/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf.

ASEAN. 2020. ASEAN Plus Three Cooperation Work Plan (2018–2022). https://asean.org/asean-plus-three-cooperation-work-plan-2018-2022/#:~:text=The%20ASEAN%20Plus%20Three%20(APT,establishing%20an%20East%20Asia%20community.

ASEAN. 2022. ASEAN Cybersecurity Cooperation Strategy (2021–2025). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.

Burwell, Frances, and Propp, Kenneth. 2020. The European Union and the Search for Digital Sovereignty. *Atlantic Council*, June. https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.

Bygrave, Lee A. 2021. The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects. *Computer Law & Security Review* 40: 105460.

Checkel, Jeffrey T. 2005. International Institutions and Socialization in Europe. *International Organization* 59 (4): 801–26.

Chen, Xuechen. 2018. The Role of ASEAN's Identities in Reshaping the ASEAN–EU Relationship. *Contemporary Southeast Asia* 40 (2): 222–46.

Chen, Xuechen, and Yang, Yifan. 2022. Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. *The International Spectator*, forthcoming.

Chin, Gregory. 2012. Two-way Socialization: China, the World Bank, and Hegemonic Weakening. *The Brown Journal of World Affairs* 19 (1): 211–30.

Choucri, Nazli, and Clark, David. 2018. *International Relations in the Cyber Age*. London: The MIT Press.

Claessen, Eva. 2020. Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance. *Journal of Cyber Policy* 5 (1): 140–57.

Council of the EU (European Union). 2014. Council Conclusions on Internet Governance. 27 November. https://data.consilium.europa.eu/doc/document/ST-16200-2014-INIT/en/pdf.

Council of the EU. 2018. EU External Cyber Capacity Building Guidelines. 26 June. https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven (CT)-London: Yale University Press.

Diez, Thomas. 2005. Constructing the Self and Changing Others: Reconsidering Normative Power Europe. *Millennium* 33 (3): 613–36.
Drezner, Daniel W. 2004. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly* 119 (3): 477–98.
Drissel, David. 2006. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs* 19 (1): 105–20.
Dunn Cavelty, Myriam. 2018. Europe's Cyber-power. *European Politics and Society* 19 (3): 304–20.
EU-ASEAN. 2021. EU-ASEAN Strategic Partners 2021. https://www.eeas.europa.eu/sites/default/files/fact-sheet-eu-asean-strategic-partnership.pdf.
European Commission. 2013. EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.
European Commission. 2019. The EU and ASEAN: Building Stronger Digital Economy & Connectivity Cooperation. 30 October. https://digital-strategy.ec.europa.eu/en/library/eu-and-asean-building-stronger-digital-economy-connectivity-cooperation.
European Commission. 2022a. Data Protection in the EU. Accessed 10 March 2022. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.
European Commission. 2022b. Adequacy Decisions. Accessed 10 March 2022. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
European Parliament. 2020. Digital Sovereignty for Europe. *EPRS Ideas Paper*, July. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.
European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj.
Fang, Binxing. 2018. *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Singapore: Springer.
Farrell, Henry. 2015. Promoting Norms for Cyberspace. *Council on Foreign Relations Cyber Brief*, 6 April. https://www.cfr.org/report/promoting-norms-cyberspace.
Finnemore, Martha. 2017. Cybersecurity and the Concept of Norms. *The Carnegie Endowment for International Peace*, 30 November. https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870.
Finnemore, Martha, and Hollis, Duncan B. 2016. Constructing Norms for Global Cybersecurity. *The American Journal of International Law* 110 (3): 425–79.
Finnemore, Martha, and Sikkink, Kathryn. 1998. International Norm Dynamics and Political Change. *International Organisation* 52 (4): 887–917.
Flonk, Daniëlle, Jachtenfuchs, Markus, and Obendiek, Anke. 2020. Authority Conflicts in Internet Governance: Liberal vs. Sovereigntists. *Global Constitutionalism* 9 (2): 364–86.
Gao, Xinchuchu. 2022. An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator*, forthcoming.
GSMA. 2018. Regional Privacy Frameworks and Cross-Border Data Flows How ASEAN and APEC Can Protect Data and Drive Innovation. September. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.
Haacke, Jurgen. 2013. *ASEAN's Diplomatic and Security Culture: Origins, Development and Prospects*. London-New York: Routledge.
IISS (International Institute for Strategic Studies). 2021. Cyber Capabilities and National Power: A Net Assessment. *Research Papers*, 28 June. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
Jayawardane, Sash, Larik, Joris, and Jackson, Erin. 2015. Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. *Policy Brief* 17. Hague: The Hague Institute for Global Justice, November. https://scholarlypublications.universiteitleiden.nl/access/item%3A2869007/view.

Jörgens, Helge. 2004. Governance by Diffusion. In William Lafferty, ed. *Governance for Sustainable Development: The Challenge of Adapting Form to Function:* 246–83. Cheltenham: Edward Elgar.
Kanetake, Machiko, and Taylor, Mistale. 2017. A Right to Be Forgotten Case Before the Japanese Supreme Court. *Renforce Blog*, 7 February. http://blog.renforce.eu/index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/.
Komaitis, Konstantinos, and Sherman, Justin. 2021. US and EU Tech Strategy Aren't as Aligned as You Think. *Brookings Tech Stream*, 11 May. https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/.
Korzak, Elaine. 2015. The 2015 GGE Report: What Next for Norms in Cyberspace? *Lawfare*, 23 September.
Kuo, Mercy A. 2021. The Brussels Effect and China: Shaping Tech Standards. *The Diplomat*, 7 January. https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/.
Liaropoulos, A. 2016. Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics. *Journal of Information Warfare* 15 (4): 14–26.
Liaropoulos, Andrew. 2021. EU Digital Sovereignty: A Regulatory Power Searching for Its Strategic Autonomy in the Digital Domain. In Thaddeus Eze, Lee Speakman and Cyril Onwubiko. *Proceedings of the 20th European Conference on Cyber Warfare and Security*: 245–52. Reading: Academic Conferences Inter Ltd.
Linsenmaier, Thomas, Schmidt, Dennis R., and Spandler, Kilian. 2021. On the Meaning(s) of Norms: Ambiguity and Global Governance in a Post-hegemonic World. *Review of International Studies* 47 (4): 508–27.
Macak, Kubo. 2017. From Cyber Norms to Cyber Rules. *Leiden Journal of International Law* 30 (4): 877–99.
Mahieu, René, *et. al.* 2021. Measuring the Brussels Effect through Access Requests. *Journal of Information Policy* 11: 301–49.
Manners, Ian. 2002. Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies* 40 (2): 235–58.
Mueller, Lukas Maximilian. 2020. Challenges to ASEAN Centrality and Hedging in Connectivity Governance. *The Pacific Review* 34: 747–77.
Mueller, Milton L. 2020. Against Sovereignty in Cyberspace. *International Studies Review* 22 (4): 779–801.
Mueller, Milton, Cogburn, Derrick, Mathiason, John, and Hofmann, Jeanette. 2007. *Net Neutrality as Global Principle for Internet Governance*. GigaNet: Global Internet Governance Academic Network, Annual Symposium 2007. DOI: http://doi.org/10.2139/ssrn.2798314.
Mueller, Milton, Mathiason, John, and Klein, Hans. 2007. The Internet and Global Governance. *Global Governance* 13 (2): 237–54.
Nocetti, Julien. 2015. Contest and Conquest: Russia and Global Internet Governance. *International Affairs* 91 (1): 111–30.
Nye, Joseph S. 2020. The Dangers of Westlessness. *The Diplomat*, 8 March. https://thediplomat.com/2020/03/the-dangers-of-westlessness/.
Pew Research Center. 2015. Internet Seen as Positive Influence on Education but Negative in Emerging and Developing Nations. *Report*, 19 March. https://www.pewresearch.org/global/2015/03/19/internet-seen-as-positive-influence-on-education-but-negative-influence-on-morality-in-emerging-and-developing-nations/.
Pu, Xiaoyu. 2012. Socialisation as a Two-way Process. *The Chinese Journal of International Politics* 5 (4): 341–67.
Raymond, Mark. 2016. Managing Decentralised Cyber Governance. *Strategic Studies Quarterly* 10 (4): 123–49.
Rosenbach, Eric, and Chong, Shu Min. 2019. Governing Cyberspace: State Control vs. the Multistakeholder Model. *Paper*. Belfer Center for Science and International Affairs, Harvard Kennedy School, August. https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

Runde, Daniel F., and Ramanujam, Sundar R. 2021. Digital Governance. *Centre for Strategic & International Studies Policy Brief*, 2 August. https://www.csis.org/analysis/digital-governance-it-time-united-states-lead-again.

Schrijver, Nico. 2016. Managing the Global Commons. *Third World Quarterly* 37 (7): 1252–67.

Securityconference.org. 2021. Beyond Westlessness: Report from the MSC Special Edition 2021. 19 February. https://securityconference.org/en/news/full/beyond-westlessness-a-report-from-the-msc-special-edition-2021/.

Shen, Yi. 2016. Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review* 1 (1): 81-93.

Solingen, Etel. 2005. ASEAN Cooperation: The Legacy of the Economic Crisis. *International Relations of the Asia-Pacific* 5 (1): 1–29.

Taylor, Emily, and Hoffmann, Stacie. 2019. EU–US Relations on Internet Governance. *Research Paper*. Chatham House, 14 November. https://www.chathamhouse.org/publication/eu-us-relations-internet-governance.

The ASEAN Post. 2018. Data Protection: Lessons from the EU. 27 December. https://theaseanpost.com/article/data-protection-lessons-eu.

Tran Dai, Candice, and Gomez, Miguel Alberto. 2018. Challenges and Opportunities for Cyber Norms in ASEAN. *Journal of Cyber Policy* 3 (2): 217–35.

Tsagourias, Nicholas. 2015. The Legal Status of Cyberspace. In Nicholas Tsagourias and Russell Buchan, eds. *Research Handbook on International Law and Cyberspace*: 9–31. Cheltenham: Edward Elgar.

UNGA (United Nations General Assembly). 2015. Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July. https://digitallibrary.un.org/record/799853?ln=en.

UNGA. 2021a. Report of the GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. 14 July. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

UNGA. 2021b. Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 10 March. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Van Raemdonck, Nathalie. 2021. Cyber Diplomacy in Southeast Asia. EU Cyber Direct. 20 May. https://eucyberdirect.eu/content_research/cyber-diplomacy-in-southeast-asia/.

Wessel, Ramese A. 2019. Cybersecurity in the European Union. In *The Routledge Handbook of European Security Law and Policy*: 283–300. Routledge.