RESEARCH ARTICLE

**Contesting Western and non-Western Approaches to Global Cyber Governance beyond Westlessness**

Xuechen Chena and Yifan Yangb

aNew College of the Humanities at Northeastern University, London; bEast China Normal University, Shanghai

Contact: Xuechen Chen; xuechen.chen@nchlondon.ac.uk; @irischenxc1

**Abstract**

The power shift from West to East has engendered an increasingly confrontational and competitive multipolar system in cyberspace governance. Thus, the West has to confront the hard reality of its decline in the face of the rising influence of the non-Western world, as shown in the intensive discussions over ‘Westlessness’ at the 2020 Munich Security Conference. In order to address scholarly concerns around cyberspace governance in a digitalised world, this Special Core examines competing ideas and norms of cybersecurity governance from comparative perspectives, shedding light on the promising research field of global cybersecurity governance and the debate on ‘Westlessness’ in the study of international politics.

**Keywords**: cyberspace governance; cyber norms; multi-stakeholderism; multilateralism; ‘Westlessness’.

The development of digital information and communication technologies (ICTs) has played an important role in redefining “space” in the socio-economic and geographical realms and has generated a ‘conceptual space’ by virtue of the Internet linking computers (Tække 2002, 25). As defined by Daniel Kuehl (2009, 26), “cyberspace is an operational domain framed by use of electronics to [...] exploit information via interconnected systems and their associated infra structure”. Cyberspace that has been formed by physical and nonphysical components is not immune to insecurity, crime and geopolitical competition, as is evident in the intensive media coverage of hackers, data loss, leaks of personal information, compromised networks and cyber-espionage in national and transnational contexts. These new dynamics have made international cooperation more important than ever as a means to establish a stable and effective framework of global cyberspace governance. Nevertheless, at the current stage, collective actions at both national and international levels are far from sufficient, if not impossible.

Yet, the transcending nature of ICTs, on which cyberspace has been built, seems to facilitate the demise of traditional governance forms based on territory, hierarchical managerial control of populations, policing and a centralised national government at the centre (Loader 1997, 1). To address a diversity of problems that have manifested themselves within cyberspace and beyond, governance has been understood as more than government, as it requires the participation of a rising number of state and non-state actors at the local, national, regional and global levels, particularly when dealing with global problems in an anarchic international society. Admittedly, sovereign states and international governmental organisations still have crucial roles to play in traditional domains of international relations; however, given its ubiquitous, borderless and virtual features, cyberspace penetrates global political, social and economic arenas and offers a testing ground for global governance innovation.

Cyberspace governance, as one of the fastest-growing fields of global governance, has inevitably become an arena for geopolitical rivalry as well as a new focal point of normative contestation among major actors in international politics (Chiappetta 2019; Kello 2017). Whereas the US has long been considered a dominant player and a rule-shaper in the global cyberspace governance regime (Drissel 2006), the past two decades have witnessed newly emerging dynamics that have significantly challenged the US’ hegemonic position and Western dominance. Norms for governing cyberspace have become increasingly contested internationally by a variety of actors and stakeholders at the global, regional and domestic levels (Maurer 2020). In addition, the redistribution of power from West to East has engendered an increasingly confrontational and competitive multipolar system in cyberspace governance (Kello 2017). Rising powers from the non-Western camp, such as Brazil, China, Russia and South Africa, are becoming increasingly proactive and are seeking to play a greater role in the reformulation of norms and standards in cyberspace governance (Ebert and Maurer 2013).

Nevertheless, this dichotomic understanding of the difference between the Western and non-Western approaches to cyberspace governance leaves several important questions unanswered. For example, to what extent and how have the conventional Western norms and approaches to cyberspace governance been challenged and contested by a variety of newly emerging powers? How can we understand the development of contestation, tension and division over norms and approaches to cyber governance within the Western bloc? Is the dichotomy between West and non-West still valid when studying global cyberspace governance? With the aim of shedding new light on these questions, this Special Core[[1]](#footnote-2) engages with the notion of ‘Westlessness’ and critically assesses ways in which the Western-centric norms and approaches of cyberspace governance are contested by emerging actors in the non-Western world. More importantly, the diversity of approaches to cyber governance clearly shows that the West and non-West are not homogenous camps or blocs. Despite a close alignment on the principle of multi-stakeholderism in United States (US)-European Union (EU) cooperation on cyberspace governance, the EU suspects that the US’ support for multi-stakeholderism favours the interests of corporations, as is discussed below and analysed in further detail in papers included in this Core. Also, the Association of Southeast Asian Nations’ (ASEAN) practice adds value to the debate by showing that ‘non-West’ does not merely encompass China or Russia. Therefore, it offers a more comprehensive and nuanced understanding of the evolving global cyberspace governance regime by transcending the conventional ‘West versus non-West’ dichotomy.

This article constitutes the background for the rest of the Special Core. Following the introduction, the next section provides an overview of the state of knowledge about global cyber governance. The following section unpacks the notion of ‘Westlessness’ and discusses how it provides a new avenue to investigate recent dynamics in global cyberspace governance. The third section outlines the key arguments and assumptions of this Special Core and summarises the main findings of each contributor, followed by a conclusion.

**Cyberspace governance: a state-of-the-art review**

According to Joseph Nye (2014), the complex technical design and the institutional forms of cyberspace governance have been shaped by private corporations and non-governmental entities, given that these bodies maintain a comparative advantage in terms of technical and normative capacities. Following this logic, it seems that governments of sovereign states have experienced a loss of control over cyberspace. Yet, in light of the range of discussions presented in this Core’s articles regarding different approaches to cyber governance and the historical development of Internet infrastructure through central governments, especially in developing or emerging countries, sovereign states can still strengthen their power by implementing cyber policies within national borders.

Therefore, competition in cyberspace governance exists both at the domestic and global levels. At the domestic level, conflict over power in cybersecurity governance is not rare, as was evident when Twitter decided to suspend Donald Trump’s account. At the global level, competition among a diversity of international actors is becoming fiercer. On the one hand, cyberspace governance institutions can be employed to influence global flows of information and to win comparative advantages, particularly for the West; on the other hand, ideas and norms around cyberspace governance have increasingly reflected tensions in traditional power relations. As observed by Milton Mueller (2017), due to growing concerns over cybersecurity challenges, the discourse, norms and models of cyberspace governance have shifted towards state-centric visions, with a particular emphasis on geopolitical rivalries and inter-state conflicts.

In terms of cyberspace governance institutions, cyberspace governance has gradually become a notable practice since the mid-1990s. In 1998, the founding of the Internet Corporation for Assigned Names and Numbers (ICANN) reflected an attempt to govern the Internet by allocating network addresses and domain names to users at the international level; (Mueller *et al*. 2007, 237). With the emergence of a greater variety of cybersecurity problems, many governmental and non-governmental organisations have either been created for or have shifted their focus to cyber governance, including the ICANN; the International Telecommunications Union (ITU), a specialised UN body and the oldest ICT organisation, originally established in 1865; the Internet Governance Forum (IGF) established in 2006; and the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial), created in 2014.

However, different international actors have divergent preferences over cyberspace governance institutions, depending on their respective interests. In light of these dynamics, a growing volume of scholarly literature on global cyberspace governance tends to identify two different approaches, namely the multi-stakeholder approach proposed by the US and its Western allies, and the multilateral approach, defended by a number of key actors from the non-Western camp, such as China and Russia (Lantis and Bloomberg 2018; Strickling and Hill 2017; Hofmann 2016). The multi-stakeholder approach, or multi-stakeholderism, is understood as “a constantly shifting balance of powers between private industry, international technical governance institutions, governments, and civil society” (Denardis 2014, 226–7), which implies an egalitarian distribution of governing functions among governmental and non-governmental stakeholders and a view of state-based governance as non-democratic (Budnitsky 2020, 13). Alternatively, a multilateral approach to cyber governance prioritises national sovereignty and favours a multilateral system that puts both policy and power in the hands of nation-states (West 2014, 7). Thus, this approach would support the creation of relevant bodies within the UN system, while simultaneously highlighting nation-states’ sovereignty in setting their own national cyberspace policies.

In general, Western countries prefer multi-stakeholderism in cyberspace governance and emphasise the inclusive participation of all relevant actors dealing with cyberspace governance. Thus, multi-stakeholder governance fora or processes, such as the ICANN, IGF and NETmundial, have been favoured. Contrarily, most non-Western countries prefer the ITU as a means of global cyber governance because it empowers its sovereign member states to determine the policies of the organisation with very limited participation of civil society stakeholders (Jayawardane *et al*. 2015, 6). Admittedly, the multi-stakeholder approach to cyber governance benefits from inclusiveness and representation, but still suffers from a few major flaws. For instance, many countries have criticised the US’ control of the ICANN, the lack of decision-making mandate in the IGF, and the failure of NETmundial to deliver a consensus because of great-power competition (Liaropoulos 2016, 20-21).

Therefore, understanding the current situation of global cyber governance might require consideration of the two forms of so-called “contested multilateralism”: one form is “regime shifting” – the transfer of the management of an issue from a multi-stakeholder forum to existing intergovernmental organisations – and the other form is “competitive regime creation” – creating a parallel or alternative intergovernmental organisation to complement or replace the original (Morse and Keohane 2014, 985). An example of regime shifting is the attempt to transfer responsibility for cyberspace governance from bodies such as the ICANN towards the ITU at the 2012 World Conference on International Telecommunications, which certainly reflected the trend emphasising the territorialisation of cyberspace with sovereign states at the centre (Glen 2014, 651). Admittedly, creating alternative global cyber governance organisations by non-Western countries to complement or replace existing ones may take some time, but creating and promoting alternative cyber norms has already been clearly witnessed.

Indeed, when it comes to the normative foundations of cyberspace governance, implementing and enforcing relevant binding international law to cyberspace, and developing and diffusing non-binding international norms are equally important. However, there is a fundamental difference between laws and norms, although it should be noted that the two concepts are intimately intertwined, and norms may evolve into laws through rising acceptance and the establishment of enforcement mechanisms. According to Martha Finnemore and Duncan Hollis (2016, 427), national regulations, international laws, professional standards, political agreements and technical protocols all present substantial normative commitments in cyber governance, so they are certainly cyber norms. However, although a violation of binding laws, in the form of national regulations or international treaties, usually has legal consequences and confers responsibilities, the same cannot be said about the non-legal norms that are used to regulate cyber conduct (Mačák 2017, 882). International law can be applied through coercion, but the success of norm diffusion generally depends on norm receivers’ belief that following such norms is in their interests.

In this sense, we can describe norms as having “prescriptive” and “evaluative” dimensions. The “prescriptive” dimension is usually described by “oughtness” that sets norms apart from other kinds of rules and “appropriateness” that shapes the understandings of behaviours to be good, desirable and appropriate (Finnemore and Sikkink 1998, 891-912). The equally important “evaluative” dimension indicates that, for an actor to comply with specific norms proposed by a group, they must feel a psychological need to be part of it (Axelrod 1986, 1105). A rising number of norms based on a diverse set of institutions and actors and their respective interests might gain some legitimacy after being accepted by like-minded actors, but can also cause norm complexity. Studying international norms in any area of global governance requires consideration of their relations and interactions with other international norms. Inter-norm relations can be quite different (harmonious or conflictual, hierarchical or horizontal, clustered or separated), so different forms of norm interaction (co-evolution, conflicts, cascades and competitions) can lead to different outcomes (weakened or strengthened, hindered or promoted) (Fehl and Rosert 2020). In this sense, norm dynamics in international relations are influenced not only by the diverging interests of various norm supporters, but also by norm relations and norm interactions. In cyberspace, there is a diverse array of norms consisting of national regulations, international laws, professional standards, political agreements and technical protocols, so the success of cyber norms will be determined not only by the perceived interests of receivers but also by the relations among different norms.

Sovereign states consider themselves to be central in establishing norms in global cyber governance, but regional organisations and private actors, such as corporations and civil society organisations, are increasingly vocal about their role and place in the normative and regulatory domain and actively engage with the norm debate. In addition, it is worth noting that competing value systems can have impacts on the establishment of cyber norms because understandings of key values relating to security in cyberspace, including privacy, transparency and anonymity, vary between Western and non-Western countries (Erskine and Carr 2016, 95) and even between countries within the Western world. Thus, cyber norms, as they stand today, are highly contested among sovereign states, despite the efforts of diplomats and professionals to minimise the gap over different understandings of cyber norms among governments in the last three decades (Broeders and Berg 2020, 5).

Specifically, in today’s cyberspace governance, a process of asymmetric distribution of power and resources is generating increasing uncertainty and is undermining the unilateral action of all major powers. As observed by David Drissel (2006), the evolution of global cyberspace governance is characterised by a process of power transition towards an increasingly multipolar system. For instance, the US’ hegemonic position has been contested and challenged by a growing number of divergent (and often contradictory) approaches on how cyberspace should be regulated proposed by other major or emerging powers, such as the EU, China, India, Russia and Brazil. This is evidenced by growing political contestations of the US-led regulatory unilateralism and of the ICANN’s legitimacy~~,~~ with heated debates emerging about the future normative and regulatory frameworks of global cyber governance.

Moreover, whereas cyberspace was traditionally perceived as a self-regulating realm, independent of traditional geopolitical spheres or compulsory regulatory measures, this view has drastically changed in recent years. Cyberspace has increasingly been regarded as a new focal point of state-sponsored extraterritorial regulations as well as multi-jurisdictional decisions (Drissel 2006). In other words, cyberspace 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 cyberspace governance 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” (417). Empirically, a rising level of geopolitical tension and inter-state competition is evident. A telling example is the recent US–China tech war, wherein the Trump administration attempted to force Beijing to abandon its policies in high-tech sectors and technology transfers from foreign enterprises in order to maintain US supremacy (Sun 2019). In Russia’s war against Ukraine, cyber attacks have been employed by both sides (Fendorf and Miller 2022). Moreover, it is believed that emerging powers from the non-Western camp, such as BRICS (Brazil, Russia, India, China, South Africa), are pursuing alternative cyber governance models that directly challenge the liberal democratic values and interests defended by the US and the EU (Rebello 2017).

In general, with respect to institutions and norms in global cyber governance, competition and conflicts within the Western bloc and between Western and non-Western countries are rendering cyberspace governance fragmented and ineffective. The West has to confront the hard reality of its decline in the face of the rising influence of the non-Western world, as shown in the intensive discussions over ‘Westlessness’ at the 2020 Munich Security Conference (MSC).

**‘Westlessness’: A crisis or a way out?**

‘Westlessness’ was highlighted as the theme of the 57th MSC held between 14 and 16 February 2021. As indicated in the 2020 Munich Security Report, “Far-reaching power shifts in the world and rapid technological change contribute to a sense of anxiety and restlessness. The world is becoming less Western. But more importantly, the West itself may become less Western, too” (*Securityconference.org* 2020, 6). Similarly, ‘Westlessness’ was described by the MSC Chairman, German Ambassador Wolfgang Ischinger, as “the sense that the world, but also the West itself, was getting less Western, less rule-based, less value-oriented” (*Securityconference.org* 2021).

With regard to the discussion over ‘Westlessness’, the emergence of non-Western countries, particularly China, has often been spoken about as the most important cause of the West’s decline. As argued by Helena Legarda (2020), China’s rising economic capacity, increasing political influence and growing assertiveness in security matters are having a clear impact on the Western-led liberal world order; Beijing is presenting itself as both an alternative to the West for countries in the non-West, and as an alternative to the US for European states. However, this explanation might overlook the causes rooted in the Western bloc itself. Indeed, post-Cold War liberal triumphalism included the seeds for future catastrophes, such as US military interventions under the alleged justification of imposing liberal democracy and the global financial crisis (*New Statesman* 2020). This led to a crisis of legitimacy whereby the economic institutions and their moral backbone built by the West, which shaped the post-war world order, are no longer appealing to developing countries (Barnett 2020).

Interestingly, it is evident that the West and non-West see ‘Westlessness’ and possible responses to it differently. Joseph Nye (2020), one of the most influential Western scholars, believes that “a successful response rests on “allies, friendships and legitimacy – the greatest assets the West has”, reflecting the dominant Western ideology and its drive to resume its monopoly over international affairs by revitalising transatlantic cooperation and so-called “liberal values”. He adds that the decline of the West comes more from the loss of confidence and the emergence of populist isolationism at home than from the rise of China abroad, and emphasises that “the US and the West still hold high cards”. He might be correct, but his explanation still admittedly rests on a “West-centric” ideology (Nye 2020). Indeed, based on views fairly widespread in the non-Western bloc, the increasing number of global challenges, such as economic recessions, climate change, poverty and a global pandemic, cannot be solved by the West alone, “no matter how ‘Western’ the West wants the world to be” (*Chinadaily.com* 2021). Russia’s invasion of Ukraine in 2022 seems to gauge the West’s fear of Westlessness empirically and test the self-professed values of the West, which will influence not only the destiny of Ukraine but also that of the West-led order.

Against this backdrop, the West seems to perceive ‘Westlessness’ as the result of its own legitimacy crisis, whereas non-Western countries, in contrast, view it as an opportunity for current global governance regimes to adapt to changing power relations and better reflect the interests of non-Western countries. However, in the current global system, ‘Westlessness’ implies a world without Western dominance but not without Western ideas, and global cooperation matters more today than ever. In this sense, overemphasising ‘Westlessness’ or equating it with the blanket decline of the West might neglect the key point that must be taken into consideration: how to find a new approach to address global challenges.

Cyberspace governance is obviously no exception. Due to their technological and self-professed value superiority, Western sovereign states, such as the US and some EU member states, can integrate liberal norms into their policies, multilateral institutions and international treaties, and tend to promote these norms to the non-Western world. To respond to the latter normative pressure, many authoritarian states, such as China and Russia, have implemented comprehensive cybersecurity policies and strategies to monitor internal dissent and external threats for national security reasons.

To be sure, Western-centric cyberspace governance is not unproblematic. Western countries are home to a diversity of non-governmental entities (primarily large Internet companies and non-governmental organisations such as the ICANN). Due to their technological and normative superiority, Western countries emphasise the role of these non-governmental entities in the governance of cyberspace, but, in reality, they can exert direct influence on such entities in pursuit of their own national interests. Consequently, Western countries usually monopolise the institutions and norms in cyberspace governance. More ironically, states and private actors working on behalf of states that own or operate the vast majority of cyberspace infrastructure exert information control for security reasons; as a result, they revert to traditional state-based forms of authority, thus arguably leading to norm regression (Deibert and Crete-Nishihata 2012, 339). Put differently, Western countries might in fact be pioneers in highlighting *territorialised* approaches to cyberspace governance based on their technological advancement.

Worse still, the conflicts and divisions between Western countries cannot be ignored. Undeniably, the US remains the dominant power in cyberspace. It conducts surveillance of other countries and facilitates the collection of commercial and personal data from US Internet corporations, which certainly endangers the security of cyberspace (Margulies 2017, 460). Moreover, within the Western world, divergent approaches to cyberspace governance still exist. The US approach to cyber governance has been described as everything from a privatised model to a hands-off approach, which highlights minimal state intervention (Komaitis and Sherman 2021). The EU, as a successful force in shaping international norms in cyber governance, has drawn political and academic attention and has tried to diffuse norms aligned with the US and wider Western community, such as freedom, openness, interoperability and multi-stakeholderism; however, the past two decades have witnessed more regulations and a regulatory strategy adopted by Brussels to counter the impacts of the US, China and Russia (Bradford 2020, 1). Admittedly, both the US and the EU embrace multi-stakeholderism. Yet, while the US vocally supports the inclusion of all stakeholders and provides a strong position for private industry in cyberspace governance, European policymakers prefer greater accountability to the public to counterbalance corporate interests (Taylor and Hoffmann 2019, 8). Thus, more divergences than convergences can be witnessed in the US’ and EU’s approaches to cyber governance.

Beyond the Western world, sovereign states such as China, Russia and Brazil, and regional organisations such as ASEAN, are also aiming to bridge international practice with their own realities in cyber governance. Meanwhile, most non-Western countries, because of their past experience of being invaded and colonised, are quite sensitive to sovereignty and state power; therefore, they are certainly not in favour of international organisations dominated by powerful Western countries (Flonk *et al*. 2020, 367). However, cyber norms based on conventional readings of territorial rights (such as rights to defend one’s own territory and to control resources within it, as well as rights to control borders and regulate the flow of people and goods across them) and obligations (such as providing minimum protection for all persons in one’s own territory) promoted by the non-Western world might jeopardise global information flows, if they use cyber norms as an excuse to restrict freedom of expression. Given that no simple correlation exists between physical borders and state borders in cyberspace, local disruptions to the Internet because of policy or infrastructure problems might have global impacts.

**Interrogating ‘Westlessness’ and cyberspace governance: contributions to the debate**

In order to address scholarly concerns around cyberspace governance in a digitalised world, this Special Core, consisting of this introductory article plus another four articles by early-career scholars of different disciplines (International Relations, international political economy and area studies) examines competing ideas and norms on cybersecurity governance from comparative perspectives, shedding light on the promising research field of global cybersecurity governance and the debate on ‘Westlessness’ in the study of international politics. Notably, the contributors to this Special Core do not adopt the set of pre-established assumptions discussed in this introduction. On the contrary, based on the overarching theme of “Contesting Western and non-Western Approaches to Global Cyber Governance beyond Westlessness”, they develop their own arguments and search for explanations by embedding their empirical research in various conceptual or theoretical frameworks.

Xinchuchu Gao’s (2022, this Issue) article explores China’s role as an emerging cyber power in cyberspace governance and the extent to which Beijing’s approach serves as an attractive alternative to the norms and practices promoted by Western actors such as the US and the EU. Drawing on the literature on norm entrepreneurship, this article offers a comprehensive analysis of China’s normative position on cyber governance, the instruments through which China has promoted its cyber norms to reshape the global discourse of cyber governance, and the degree of recognition and acceptance by external actors. In so doing, Gao argues that it is imperative to move beyond the traditional ‘West vs. non-West’ debate, as well as to capture the complexity of China’s approach to cyber governance. Whilst acknowledging that Beijing’s normative underpinnings sharply contrast with those of many Western actors, Gao contends that China’s norms on cyberspace governance should not be reduced to sovereignty concerns and government interventionism. In fact, over the past few years, China has increasingly allowed business units to play a greater role in the development of technical standards and norms, and thus, its normative position concerning cyber governance is better understood as a result of interactions between state agencies’ and businesses’ interests. In her analysis, Gao further points out that the prevailing ‘West vs. non-West’ debate on cyber governance overlooks the complexity of normative considerations within the Western bloc, especially the emerging divergence between the US and the EU. Such divergence has resulted in different intra-group levels of receptiveness to China’s cyber norms, which may favour mediator roles for the EU in US–China rivalry in cyberspace governance. Overall, these dynamics are likely to increase the degree of convergence between China’s and Western countries’ cyber governance approaches, and thereby help transcend the dichotomy between the Western and non-Western blocs.

Saeme Kim’s (2022, this Issue) article examines Singapore’s and South Korea’s roles and limitations as middle powers in global cyber governance, and how a middle-power perspective may provide an alternative insight on the ‘West vs. non-West’ debate in cyberspace governance. Kim rightly points out that, against the backdrop of intensifying US–China rivalry, the conventional ‘West vs. non-West’ paradigm has become increasingly obsolete: a growing number of middle powers – a category of countries that are neither big nor small in quantifiable attributes – tends to pursue a pragmatic approach to US–China tensions by supporting multilateral approaches, and promoting dialogue and norm-building in global cyber governance. By critically assessing the existing debate on ‘Westlessness’, which focuses primarily on the decline in ‘Western assertiveness’ and the rise of the non-West, and on US–China rivalry in particular, Kim argues that there is more nuance to the debate in the field of cyber governance than is generally assumed. Whilst growing tensions between the US and China have resulted in an increasingly polarised global environment, changes in power configuration also present new opportunities for global governance, opening up a playing field for middle powers to assume a greater role. Building on the theoretical framework of the middle-power approach, Kim shows how Singapore and South Korea envision alternative pathways in global cyberspace governance. South Korea adopts a unique approach to cyber governance by not only advocating the establishment of international rules, trust-building and capacity-building in cyberspace governance, but also highlighting the importance of non-binding and pragmatic position as a middle power. Similarly, Singapore can be considered a so-called “facilitator”, propelling various international and regional initiatives that contribute to a rule-based multi-stakeholder approach to cyber governance. Despite Singapore’s small size, its status within ASEAN allows it to support discussions on cyber governance at the global level.

Xuechen Chen and Yifan Yang’s (2022, this Issue) article analyses the distinct regional norms and approaches to cyber governance undertaken by the EU and ASEAN. Similar to the previous two articles, their analysis seeks to offer a critical reflection on the debate centring around the ‘West vs. non-West’ dichotomy and the newly emerging concept of ‘Westlessness’. This research demonstrates that, in order to better capture the dynamics of global cyber governance, it is important to first develop a more nuanced understanding of the variations of cyber governance norms and approaches within and beyond the traditional Western camp. Second, it is crucial to take into account the role regional organisations can play in reshaping the normative framework of cyber governance. In particular, this article shows 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’. It thereby renders ASEAN an increasingly important actor in cyber governance in the Asia-Pacific region, presenting a non-Western perspective to shape the debate on the digital sphere.

Finally, Louise Marie Hurel’s (2022, this Issue) essay draws from literature on cybersecurity, International Relations and development studies to examine how the notion of ‘cyber capacities’ has emerged as a global development agenda, as well as analysing its consequences for developing regions. The essay starts with an intriguing discussion on the multiple origins and contestations of the notion of cyber capacity-building (CCB). In an attempt to explore the inner logics that underpin knowledge about CCB, this essay further unpacks two specific mechanisms through which CBB has been used as a policy tool for cyber development: measurement and norm diffusion. Drawing on extensive empirical evidence in the Global South, Hurel argues that the political and economic dynamics of CCB continue to reproduce inequalities between the West/Global North and non-West/Global South. These observations encourage critical cybersecurity scholars to interrogate a crucial question: how have the cybersecurity frameworks developed in the West or Global North become entangled with the realities and discourses in non-Western contexts or Global South? Hurel contends that many countries in the Global South have become the territory of application of CCB measurement models produced in the Global North. In other words, CCB knowledge and frameworks, which can be considered a universalising tool produced in the Global North, have been internalised in the Global South, reproducing notions of ‘development’ through ranking and measurement of gaps. On the other hand, this essay demonstrates that CCB has not only become an indispensable component in cybersecurity development, but has also become a crucial element encoded in multiple cyber norms development processes. The cyber norm contestation and diffusion processes, which involve different international and regional actors with different normative aspirations, are likely to turn CCB into an important tool for the effective implementation of cyber norms and into a way to bridge existing inequalities between the West and non-West.

**Concluding remarks and further directions**

This Special Core makes a twofold contribution to the existing debate on global cyber governance by critically engaging with the notion of ‘Westlessness’. First, by examining a diverse range of empirical cases and subfields of cyber governance, it demonstrates ways in which the Western dominance over the norms, discourses and approaches concerning cyber governance has been fiercely contested by emerging powers and nascent players in the Global South. Over the past decade, rising powers such as China, Singapore, South Korea, ASEAN and Latin America (Hurel) have all demonstrated stronger willingness and ambition to reshape the normative and regime structures in global cyber governance, according to their own values, interests and local contexts. Whilst the existing literature on the normative framework of global cyber governance has long been confined to the debate between ‘multi-stakeholderism’ and ‘multilateralism’, our contributors’ analyses provide a more nuanced understanding of the complex nature of global cyberspace governance by taking into account a wider array of positions and approaches. These observations reveal that cyberspace governance, as a newly emerging and fast-growing policy area of global governance, has been increasingly characterised by a salient trend of knowledge and power diffusion and redistribution away from countries in the Global North towards developing regions and emerging actors. Second, this Special Core offers a critical assessment of the notion of ‘Westlessness’ and its relevance to the study of international politics. Whilst the concept of ‘Westlessness’ has been primarily adopted to depict the erosion of Western dominance and the rise of the non-Western world, contributors to this Special Core argue that it is imperative to move beyond the reductionist ‘West vs. non-West’ dichotomy in global cyber governance. Specifically, it demonstrates that there is a lack of a unified ‘Western’ normative position and coherent approach towards cyber governance. For example, the EU is emerging as a new norm entrepreneur and autonomous regional actor that has proactively promoted its own vision of cyber governance (Chen and Yang 2022, this Issue). In so doing, it contributes to challenging the predominant US-centric approach from within the Western community. In addition, a dichotomous perspective highlighting the division between the West and non-West tends to neglect the increasing level of entanglements and potential normative convergence between the Global North and Global South (Gao 2022, this Issue). As evidenced in Kim’s (2022, this Issue) article, a growing number of middle powers, such as South Korea and Singapore, have sought to find an alternative ’third way’ towards cyber governance to avoid being trapped in the geopolitical rivalry between the dominant Western and non-Western powers. Moreover, as shown in Hurel’s (2022, this Issue) essay, it is necessary for researchers to shift their attention towards how CCB knowledge frameworks and normative considerations developed in the Global North have become increasingly intertwined with the realities, norms and discourses concerning cybersecurity capacity-building in the Global South.

This Special Core also seeks to pave the way for further research on global cyberspace governance. To advance our understanding of the latter beyond the conventional conceptualisation of ‘Westlessness’, two pathways can be envisioned. First, given the existence of divergent norms in cyber governance, it is worth further uncovering the conditions under which a diverse array of norms and regulatory approaches has emerged and has been sustained by taking into account the socio-economic, political and cultural contexts in different countries and regions. Second, considering the increasing degree of normative entanglement and mutual learning among different international actors, it is imperative to study the causal mechanisms underlying the processes of norm and policy diffusion in the sphere of global cyber governance. This will enrich our understanding of how cyber governance norms and policies travel across different regions, and how these norms and policies are contested, reconstructed and localised by different actors from both the Global North and the Global South.

**Acknowledgments**

The authors wish to thank the anonymous referees for their helpful suggestions, and the editorial team of *The International Spectator* for their patient and warm support.

**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

**References**

Axelrod, Robert. 1986. An Evolutionary Approach to Norms. *American Political Science Review* 80 (4): 1095-111.

Barnett, Michael. 2020. Judy Asks: Can the West Regain its Influence? *Carnegie Europe*, 15 February. <https://carnegieeurope.eu/strategiceurope/81076>.

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

Broeders, Dennis, and van den Berg, Bibi. 2020. Governing Cyberspace: Behaviour, Power, and Diplomacy. In Dennis Broeders and Bibi van den Berg, eds. *Governing Cyberspace: Behavior, Power, and Diplomacy*: 1-18. Lanham (MD): Rowman & Littlefield.

Budnitsky, Stanislav. 2020. Russia’s Great Power Imaginary and Pursuit of Digital Multipolarity. *Internet Policy Review* 9 (3): 1-25.

Chiappetta, Andrea. 2019. The Cybersecurity Impacts on Geopolitics. *FormaMente* 14 (1): 61-74.

*Chinadaily.com*. 2021. The Right Path to Overcoming ‘Westlessness’ Anxiety. 22 February. <https://global.chinadaily.com.cn/a/202102/22/WS6032f0c3a31024ad0baaa0c9.html>.

Deibert, Ronald J., and Crete-Nishihata, Masashi. 2012. Global Governance and The Spread of Cyberspace Controls. *Global Governance* 18 (3): 339-61.

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

Drissel, David. 2006. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs* 19 (1): 105-20.

Ebert, Hannes, and Maurer, Tim. 2013. Contested Cyberspace and Rising Powers. *Third World Quarterly* 34 (6): 1054-74.

Erskine, Toni, and Carr, Madeline. 2016. Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace. In Anna-Maria Osula and Henry Rõigas, eds. *International Cyber Norms: Legal, Policy and Industry Perspectives*: 87-109. Tallinn: NATO CCD COE Publications.

Fehl, Caroline, and Rosert, Elvira. 2020. It’s Complicated: A Conceptual Framework for Studying Relations and Interactions Between International Norms. *Working Paper*. Frankfurt am Main: Peace Research Institute Frankfurt. <http://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/PRIF_WP_49.pdf>.

Fendorf, Kyle, and Miller, Jessie. 2022. Tracking Cyber Operations and Actors in the Russia-Ukraine War. *Council on Foreign Relations*, 24 March. <https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war>.

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 S. 2020. Authority Conflicts in Internet Governance: Liberal vs. Sovereigntists. *Global Constitutionalism* 9 (2): 364-86.

Glen, Carol M. 2014. Internet Governance: Territorializing Cyberspace? *Politics & Policy* 42 (5): 635-57.

Hofmann, Jeanette. 2016. Multi-stakeholderism in Internet Governance: Putting a Fiction into Practice. *Journal of Cyber Policy* 1 (1): 29-49.

Jayawardane, Sash, Larik, Joris, and Jackson, Erin. 2015. Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. *Policy Brief* 17*.* The Hague: The Hague Institute for Global Justice. <https://thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf>.

Kello, Lucas. 2017. Cyber Security: Gridlock and Innovation. In Thomas Hale and David Held, eds. *Beyond Gridlock*: 205-28. Cambridge: Polity.

Komaitis, Konstantinos, and Sherman, Justin. 2021. US and EU Tech Strategy Aren’t as Aligned as You Think. *Brookings*, 11 May. <https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/>.

Kuehl, Daniel T. 2009. From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds. *Cyberpower and National Security*: 24-42. Dulles (VA): Potomac Books.

Lantis, Jeffrey S., and Bloomberg, Daniel J. 2018. Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace. *International Relations* 32 (2): 149-72.

Legarda, Helena. 2020. Will China be a Driver of ‘Westlessness’? *Mercator Institute for China Studies*, 12 February. <https://merics.org/en/press-release/will-china-be-driver-westlessness>.

Liaropoulos, Andreas. 2016. Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics. *Journal of Information Warfare* 15 (4): 14-26.

Loader, Brian D. 1997. The Governance of Cyberspace: Politics, Technology and Global Restructuring. In Brian D. Loader, ed. *The Governance of Cyberspace: Politics, Technology and Global Restructuring*: 1-19. London-New York: Routledge.

Mačák, Kubo. 2017. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law* 30 (4): 877-99.

Margulies, Peter. 2017. Global Cybersecurity, Surveillance, and Privacy: The Obama Administration’s Conflicted Legacy. *Indiana Journal of Global Legal Studies* 24 (2): 459-96.

Maurer, Tim. 2020. A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague Journal on the Rule of Law* 12 (2): 283-305.

Morse, Julia C., and Keohane, Robert O. 2014. Contested Multilateralism. *The Review of International Organizations* 9 (4): 385-412.

Mueller, Milton. 2017. Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. *Digital Policy, Regulation and Governance* 19 (6): 415-28.

Mueller, Milton, Mathiason, John, and Klein, Hans. 2007. The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance* 13 (2): 237-54.

Munich Security Conference. 2020. Munich Security Report 2020: Westlessness. <https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf>.

Munich Security Conference. 2021. Beyond Westlessness: Report from the MSC Special Edition 2021. Accessed 10 November 2021. <https://securityconference.org/en/news/full/beyond-westlessness-a-report-from-the-msc-special-edition-2021/>.

New Statesman. 2020. Leader: The New Age of Westlessness. 2 June. <https://www.newstatesman.com/politics/2021/06/leader-new-age-westlessness>.

Nye, Joseph S. 2014. The Regime Complex for Managing Global Cyber Activities. *Paper Series* No. 1. Waterloo (ON)-London: Centre for International Governance Innovation-Chatham House.

Nye, Joseph S. 2020. The Dangers of Westlessness: Are the Origins of ‘Westlessness’ to be Found Closer to Home? *The Diplomat*, 8 March. <https://thediplomat.com/2020/03/the-dangers-of-westlessness/>.

Rebello, Katarina. 2017. Building Walls with ‘BRICS’? Rethinking Internet Governance and Normative Change in a Multipolar World. *Working Paper* 1 (1). St. Andrews: Centre for Global Constitutionalism. <http://cgc.wp.st-andrews.ac.uk/files/2017/03/CGC-Junior-Scholar-WP-Series-2017-FINAL.pdf>.

Strickling, Lawrence E., and Hill, Jonah F. 2017. Multi-stakeholder Internet Governance: Successes and Opportunities. *Journal of Cyber Policy* 2 (3): 296-317.

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

Tække, Jesper. 2002. Cyberspace as a Space Parallel to Geographical Space. In Lars Qvortrup, ed. *Virtual Space: Spatiality in Virtual Inhabited 3D Worlds*: 25-46. London: Springer.

Taylor, Emily, and Hoffmann, Stacie. 2019. EU-US Relations in Internet Governance. *Research Paper*. London: Chatham House, <https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf>.

West, Sarah M. 2014. Globalising Internet Governance: Negotiating Cyberspace Agreements in the Post-Snowden Era. *Conference Paper from the Telecommunications Policy Research Conference*. Fairfax, Virginia, 11-13 September.

1. This Special Core is the result of a call for thematic Special Cores on the notion of Westlessness open to early-career scholars under 35 years of age that was issued by *The International Spectator* in November 2020. [↑](#footnote-ref-2)