Routledge
Taylor & Francis Group

Review of International Political Economy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rrip20

Governing cyberspace: policy boundary politics across organizations

Stephanie C. Hofmann & Patryk Pawlak

To cite this article: Stephanie C. Hofmann & Patryk Pawlak (2023) Governing cyberspace: policy boundary politics across organizations, Review of International Political Economy, 30:6, 2122-2149, DOI: 10.1080/09692290.2023.2249002

To link to this article: https://doi.org/10.1080/09692290.2023.2249002

Published online: 01 Sep 2023.

REVIEW OF INTERNATIONAL POLITICAL ECONOMY
2023, VOL. 30, NO. 6, 2122–2149
https://doi.org/10.1080/09692290.2023.2249002

Routledge
Taylor & Francis Group

SPECIAL FORUM ON INTERNATIONAL REGIME COMPLEXITY

Governing cyberspace: policy boundary politics across organizations

Stephanie C. Hofmann[a] and Patryk Pawlak[b,c]

[a]Department of Political and Social Science & Robert Schuman Centre of Advanced Studies, European University Institute, Florence, Italy; [b]EU Institute for Security Studies, Brussels, Belgium; [c]Robert Schuman Centre of Advanced Studies, European University Institute, Florence, Italy

ABSTRACT

Policy boundaries and issue interdependence are not a given. The stakes they imply—*who* governs, *how,* and *where* a policy domain is—become institutionalized over time, often first by the Global North. We know little about how these stakes are presented and institutionalized within and across organizations. We tackle this lacuna by asking how, and to what effect, an emerging policy domain is situated in a densely institutionalized environment. We argue that new policy domains such as cyberspace or artificial intelligence prompt resourceful governments to forum-shop policy frames by clustering promising issues in new and existing organizations in pursuit of coalition-building. Initially, resonance is more likely to be established in organizations with like-minded countries, leading to partially differentiated non-hierarchical regime complexes. In the long-term, competing adjustment pressures, particularly felt in the Global South, help trigger a regime-shift to an orchestrating general-purpose organization. Key actors must reconfigure their frames thereby reducing differentiation. In today's geopolitical world, this hardens intra-organizational political differences. We examine three propositions in the case of cyberspace and show how the proliferation of competing frames across organizations led to shifting the policy debate to the UN, where only piecemeal policy adjustments are possible. Our analysis is based on primary sources and immersion strategies.

KEYWORDS

Global governance late comer; regime complex evolution; policy frame; frame resonance; issue-splitting; issue-linking

Introduction

Cyberspace is a late comer to global governance. How it is used and governed carries multifaceted social and political implications: From influence operations targeting elections in Brazil to ransomware attacks on a Belgian port, financial

CONTACT Stephanie C. Hofmann stephanie.hofmann@eui.eu

inclusion in Kenya, and improved farming practices in India. These examples show how cyberspace can crosscut many existing policy domains (e.g. security, trade, development, and human rights) whose policy content and policy boundaries are negotiated in existing organizations.[1] Since the internet and internet-enabled technologies that cyberspace encompasses are not only about productivity gains and economic growth but also about authority and control, actors try to govern the rapidly expanding cyberspace[2] through standards, treaties, algorithms, and protocols.

Given the late arrival of cyberspace and its potential to crosscut different policy domains, debates about where and how to define and govern it unsettle inter-organizational relationships. These debates not only occur in many existing international (IO) and regional (RO) organizations, such as the United Nations (UN), the World Trade Organization (WTO) or the European Union (EU), but also in new multistakeholder or informal organizations, such as the Paris Call for Trust and Security in Cyberspace or the Prague 5G Security Conference.

Despite broad agreement among scholars and policymakers that regime complexes characterize global governance in general (Henning & Pratt, 2023) and cyberspace in particular (Nye, 2014), we know little about the regime complex dynamics that emerge around new policy domains. Most scholarship takes policy boundaries—and consequently, regime complex boundaries—as given. We question the assumption of stable, consensual policy boundaries and investigate their contested content over time. How and to what effect do new policy domains, such as cyberspace, enter a densely institutionalized environment in which they have no obvious focal or host organization? In line with this special issue, we pay particular attention to inter-organizational differentiation and hierarchy when analyzing the evolution of regime complexes.

We argue that in our contemporary world, a new policy domain possesses crosscutting potential—both in terms of policy content and organizational host—and its introduction triggers fights between actors over who, how, and where to govern the policy domain; policy boundaries have not settled, and organizational fit and resonance still have to be determined. As there is no obvious main contender among the many organizational options, we expect a competitive process to be unleashed that can be divided into two stages.

In the first stage, we argue that policymakers will introduce governance proposals to existing and new organizations in accordance with their core preferences. In regime complexity parlance, this corresponds to forum-shopping, regime creation and seeking regime-shifting. If actors do not all share the same understanding of the domain and agree on its stakes (which is very likely), then actors will link and split issues into issue clusters that inform their policy frame's content in search of coalitions that help them not only carry the proposal forward but also ratify it. Not all proposals are equally likely to resonate with potential coalitions. Consequently, heterogenous (in membership or tasks) organizational hosts are likely to reject contested proposals, while more homogenous organizations with like-minded actors (such as regional or possibly task-specific organizations) are more likely to ratify them. This explains why we expect to first find a regime complex that is partially differentiated and nonhierarchical.

In the second stage, we argue that these overlapping and competing institutionalized policy frames in a partially differentiated and non-hierarchical regime complex create a feedback loop. We specify under what conditions we expect to observe

a move from such a regime complex to a more hierarchical and less differentiated one. Given overlapping and competing frames in a partially settled policy domain, we argue that it is likely that adjustment pressures rooted in inconsistent regulatory and normative frameworks lead to calls for orchestration over the long-term. When exactly these pressures arise is hard to predict. However, dissatisfaction will mount that cannot be addressed solely in regional or task-specific organizations. This growing dissatisfaction will prompt disadvantaged Global South actors, in particular, to turn to general-purpose and inclusive decision-making bodies and request orchestration over how to govern the new policy domain, thereby essentially contributing to regime-shifting. This shift relocates authority to one organization and reduces institutional differentiation. However, by design, general-purpose organizations have many venues where political debates can take place. These venues enable actors to continue building coalitions and debating over how to govern the new policy domain, potentially hardening major cleavages. These cleavages inhibit comprehensive policy solutions, such as a general treaty. Instead, they feed into task-specific customary practices.

Our theoretical framework is a corrective to existing scholarship that takes issue interdependencies for granted at all stages of issue emergence and focuses on technocratic solutions to manage them (Johnson & Urpelainen, 2012). It also addresses analytical gaps left by functional approaches that understand major international actors as acting in the interest of reducing turf wars and providing global public goods (Gehring & Faude, 2014; Jupille et al., 2013). We argue that there are no inevitable policy solutions since policy problems are not necessarily commonly perceived and defined. This is particularly so when new policy domains emerge. Instead of observing a functional expansion of institutional mandates triggered by new issues, policymakers intentionally seek out issue connections, introducing them to/across IOs. Linking and splitting issues is a political act that responds more to political coalition building than functional imperatives. While adjustment pressures leading to more institutional and authority orchestration can seem at first sight to be functional responses to strategic inconsistencies, the particular regime shift that such pressures trigger (namely, the shift to a general-purpose global organization) aggravates the search for common policy responses by hardening political cleavages.

By looking at who introduces cyberspace, and how and where it is introduced, we seek to contribute to our understanding of the malleability of policy domains in densely institutionalized environments, as well as of the benefits and risks entailed for global trade and other policy domains. First, we draw on and add to international relations scholarship on regime complexity and global governance. Regime complexity scholars have emphasized various strategies of contestation (Hofmann, 2019; Morse & Keohane, 2014). We add issue-linking and issue-splitting to this set of strategies.[3] We show that to understand inter-organizational relations, it not only matters *where* actors pursue authority claims (e.g. through forum-shopping or regime-shifting), but also *how* they do so (e.g. through issue-linking or issue-splitting).

Second, we build on public policy, communications, and social movement scholarship that demonstrates the malleability of policy problem construction and solutions to *specify one condition* under which we should observe these processes on the international level (namely, when a new policy domain emerges), and to theorize the *processes that unfold across organizations*. Our focus on discursive policy

framing and coalition building helps account for an important source of power in global (economic) governance not solely rooted in material or institutional power (Farrell & Newman, 2019; Krasner, 1976; Odell, 2018) but also in ideational and discursive power. Scholarship addressing these sources of power has demonstrated how hegemonic and epistemic imposition of a definition (Allan, 2017; Branch, 2021; Knaack & Gruin, 2021) or vetting (Carpenter, 2011) can settle policy domain boundaries over time. We add discursive policy framing and frame resonance across organizations to this list, combining insights from regime complexity and framing scholarship.

We also contribute to debates on cyberspace governance and its implications for global economic governance. Existing studies have provided valuable insights into the power of metaphors (Branch, 2021) and spatial debates (Lambach, 2020) but have otherwise focused on various parts of the cyberspace regime complex, such as internet governance (DeNardis, 2014), disinformation (Rid, 2020), or cybersecurity (Calcara & Marchetti, 2022). Our analytical framework helps to show that governments value cyberspace differently as they link and split cyber with other issues to build coalitions, consequently pursuing different policy solutions through international law and norms (Finnemore & Hollis, 2016). Even a powerful actor like the United States (US) must face alternative frames presented by actors such as Russia, China, Brazil, India, Iran, Egypt, and the EU, and can fail to create frame resonance. In addition, by demonstrating cyberspace's growing importance as a digital marketplace, global information outlet, and theatre of conflict, we point to adjustment pressures and dissatisfaction that eventually led Global South countries to support Russia's call to negotiate cyberspace governance in the UN—effectively making the UN the cyberspace orchestrator. This turn to the UN consolidated many frames into an accountability-sovereignty cleavage cutting across UN venues.

Our analysis is based on official documents from organizations, national position papers and other actors' formal submissions, joint proposals, informal consultations, speeches, and commentaries, particularly those from the UN's First Committee's Open-Ended Working Group (OEWG). Analysis is also informed by a Goffmanian sensibility and immersion strategies, namely hanging out (Nair, 2021), participant observation, and participation in multilateral cyber processes (Müller, 2013) such as the 2019–2021 UN Group of Governmental Experts (GGE), the OEWG in 2019–2021 and 2021–2025, the Global Forum on Cyber Expertise (2015–2021), and informal engagement with government and IO officials since 2017. Immersion in these various discussions helped us contextualize document analysis and thematize policy frames.

Emerging policy domains and regime complex evolution

Investigating how actors understand and want to regulate emerging policy domains while navigating a densely institutionalized environment requires a theoretical discussion of three interrelated concepts: Policy frames, policy frame resonance, and frame (mis)alignment. Framing is a process of discursive construction that is indispensable to actors, where policy content and goals are in flux and others must be brought on board. Policy frames concern the supply side of policy content and solutions. The question of frame resonance concerns the demand side: Governments

look for partners willing to accept their agenda as worthwhile within and across organizations. A focus on frames and frame resonance therefore helps us unpack how and where policymakers make strategic choices, especially discursive choices of how to frame their preferences and where to forge support. This relates to frame (mis)alignment and related adjustment pressures after competing and overlapping policy frames have been introduced across organizations. Misaligned contested policy boundaries and their related governance mechanisms produce adjustment pressures, which trigger a regime shift to an orchestrating organization. To spell out each theoretical step below, we build on public policy, communications, and social movement scholarship, which has mainly focused on actors within one country (often the US) and/or single IOs when examining policy frames (Baumgartner & Jones, 1993; Chong & Druckman, 2007; Snow & Benford, 1988). We build on these insights to investigate how policy frames align, overlap, and compete (or not) with other frames *in* and *across* organizations.

Multiple policy frames

Before organizational claims to govern policy domains can be recognized, these policy domains must be defined. What many perceive as established policies (e.g. liberal market economy, sustainable environment, human security) consist of issue clusters. The policy domain of human security, for example, clusters issues pertaining to poverty eradication, conflict prevention, arms control, humanitarianism, and human rights (Carpenter, 2011).

Framing policy content and boundaries fulfills the discursive tasks of identifying problems and prescribing solutions (e.g. binding regulatory frameworks like treaties, non-binding instruments like codes of conduct) (Entman, 2004, p. 5), each of which can be contested by others. Through framing, policymakers craft meaning for collective governance action and construct its boundaries, making it politically consequential (Baumgartner & Jones, 1993). Policy frames can therefore change the stakes for actors in organizations. For example, attaching an issue to development might increase some actors' access to funding while obliging others to pay, while linking it to fighting crime might support calls for additional regulation while threatening access to markets.

One instance where policy framing is likely to be prevalent in global governance is when a new policy domain emerges. Actors will try to make sense of this new domain and how it relates to the existing organizational environment. In line with the special issue, we focus on governments as the main actors and concede that while governments are not the sole caretakers of global governance, they arguably have the most access to organizations where global governance is decided upon (Andonova, 2017; Pouliot & Thérien, 2018). At this stage, it is unlikely that actors will agree on the opportunities, challenges, and stakes that a new domain can entail—or share an understanding of domain-specific functional characteristics—particularly if actors diverge in their material and ideational preferences (Allan et al., 2018; Voeten, 2021). Functional narratives first must be created and institutionalized (Allan, 2017). It is likely that some will pursue diverse liberal agendas (Acharya, 2016) while others 'privilege state security, civilizational diversity, and traditional values over liberal democracy' (Cooley, 2015, p. 50; Flonk et al., 2020),

for example. Based on these different preferences, actors cluster issues into policy frames and propose them to organizations for adoption and implementation. Already the written language of policy proposals is 'a fundamental part of the construction of organizational reality' (Phillips et al., 2008, p. 771). The existence of a multitude of policy frames across organizations demonstrates the politics of policy boundaries and their implications for regime complexes. As governments identify and label policy problems and advocate for policy solutions across organizations, they also frame distinctive and possibly competing or contradicting authority and differentiation claims, transforming the framing process into a fight for recognized claims to govern (Adler-Nissen & Zarakol, 2021; Hofmann, 2013; Princen, 2011, p. 931). These diverse frames together form the nascent regime complex.

Proposition 1: If a new policy domain emerges, key actors are likely to frame and claim authority over it differently in and across new and existing organizations, instead of sharing a common understanding of domain-specific functional characteristics.

Forging frame resonance through issue-linking and issue-splitting

For authority and differentiation claims to become meaningful, they must be recognized as claims to govern (Adler-Nissen & Zarakol, 2021). Recognition by others is achieved when policy frames resonate with a coalition of actors that can dominate an organization (Snow & Benford, 1988). The goal of frame resonance requires strategizing by governments. Policymakers do so by constructing policy frames in which they link or split their preferred cyber-specific issues with issues that are important to other actors, which are often already governed by existing organizations. These issues can be costly to add or to drop. For example, adding development aid to a cyber-related issue incurs additional financial expenditures, just as adding investment screening mechanisms implies greater economic costs, and adding or dropping human rights can have political consequences. To create competitive coalitions, policymakers re-organize their frames as others challenge and dismiss their agendas and strengthen their leverage in negotiations.

These two resonance-creating framing strategies—issue-linking and issue-splitting—should be further elaborated as they are crucial to understanding *how* and *where* a policy domain is governed. Through *issue-linking,* governments and their policymakers strategically construct interdependencies between their core preferences and incidental issues 'making it appear common sense to regulate or govern them together and in a particular way' (Muzaka, 2011, p. 761). This strategy has been primarily examined in international trade, where policymakers combine 'multiple issues to change the balance of interest' (Davis, 2004, p. 153). Issues pertaining to environment have been successfully linked to trade, for example. Policymakers that pursue a green economy (Jinnah & Morin, 2020) argue that this is 'a political necessity for free traders' (Esty, 2001, p. 116). But we can also find issue-linking in the security realm, where policymakers have linked security issues with migration or the environment (Buzan et al., 1998). Through *issue-splitting,* governments and their policymakers strategically negate and deconstruct the functional interdependencies constructed by others to regulate or govern issues separately. Although not much discussed in the literature, this strategy has major

repercussions on inter-organizational differentiation and authority. As governments strategically detach an issue from existing issue clusters, they also 'change the balance of interest' and present the new streamlined cluster as 'intrinsically linked'. Empirical examples include the Chinese government's intentional issue-splitting of peace and security on the one hand, and human rights on the other. The resulting sovereigntist understanding of peacekeeping has found a large following in the UN, challenging the liberal peacebuilding/state-building paradigm.

Governments that pursue issue-linking and issue-splitting tap into organizational repertoires to articulate frames that echo with potential partners. Policymakers leverage IO policy agendas, cultural resources, and organizational capacities as a treasure trove to generate and mobilize support for their policy frames (Goffman, 1974; Nelson & Weaver, 2016; Swidler, 1986). As Princen (2011, p. 933) observes in the EU context, governments try to tie 'in with established overall values that are held to be central' or 'in with stated policy priorities and commitments'. New and established organizations can help governments create resonance.

Frame resonance is not a given, however; pursuit for frame resonance can lead to either IO acceptance or resistance. Studying parties and public opinion, Chong and Druckman (2007, p. 113) observe 'when an issue is new to the agenda, the public is uncertain of its stakes and of how competing positions relate to their values. In the formative stages of an issue, opposing sides may each contend that its position is consistent with the core values and priorities of the voters it is targeting'. The same can be said about governments and their potential coalition partners. Member-states and IOs will interrogate new frames for their applicability and 'suitability for interpreting and responding to their environment. Consequently, they often … will either filter out these items they consider inappropriate or they will use them as standards' (Price & Tewksbury, 1997, pp. 187–88). On the one hand, if governments have chosen an IO that does not align well with their policy frame, then resistance is likely, which weakens their capacity to promote and push for the adoption of their frame and capture the organization. This is particularly the case in general-purpose IOs with large and heterogenous memberships or when the frame consists of issues that have 'low hierarchical salience within the larger belief system, [then] the mobilizing potential is weakened' (Snow & Benford, 1988, p. 205).

On the other hand, if policymakers seek out an organization that aligns with their frame—which is probable if they chose an organization where they are a member and members are relatively ideologically homogenous (e.g. regional)—then frame acceptance is likely. Between these two types of organizations are task-specific organizations where actors share a common outlook on a particular policy issue and do not need to assess the proposed policy frame *vis-à-vis* all other possible options. While existing organizations lend themselves to mobilize support, new organizations might be added to meet the needs of policymakers, who find their frames too far removed from existing ones (Tallberg, 2003, pp. 8–10). To pursue their frame and gather support from others, it is therefore likely that policymakers will invest in new forums, which has been called (competitive) regime creation, and/or reform existing ones (regime-shifting) (Morse & Keohane, 2014).

By linking or splitting issues and creating resonance for their frame, actors shape institutional differentiation and (re)allocate authority (Schattschneider, 1957, p. 937). Each newly introduced frame 'shape[s] political debates by redefining the

object of conflict, the actors involved in it, as well as the end goal and strategy to be pursued' (Bocquillon, 2018, p. 341), as well as designates winners and losers. '[E]ach institutional venue is home to a different image of the same question' (Baumgartner & Jones, 1993, p. 131) as policymakers will not agree on how and where to discuss the new domain. Different frames will challenge each other's problem definition, scope, legitimacy, and/or alignment with a forum. Powerful actors are unlikely to be able to impose their policy frame, as the multitude of potential host organizations provides other actors the possibility to pursue their preferences. Given differentiated organizations and at least in the short-term, no immediate policy adjustment pressures or dissatisfaction is likely to arise, as proposed in the framework paper.

> *Proposition 2*: In the first phase of domain institutionalizing, policymakers are likely to be more successful in creating frame resonance in regional and task-specific organizations, or in creating new ones, than to capture global general-purpose organizations. This supports differentiated and nonhierarchical inter-organizational relations.

Frame (mis)alignment, adjustment pressures, and organizational orchestration

With time, misaligned, overlapping, and competing policy frames across organizations change the stakes for governments and create policy adjustment pressures for states with membership in several IOs. Some policy frames imply concrete legal obligations or compliance with a broader normative approach (Finnemore & Hollis, 2016), while voluntary and non-binding agreements commit actors to specific coordination and cooperation mechanisms (Fioretos, 2017). Because of these frame misalignments (Snow & Benford, 1988), actors face legal and normative uncertainties bringing substantive and procedural disagreements to the fore (Chong & Druckman, 2007, p. 113) as well as experience increased transaction costs and inequalities among themselves (Raustiala & Victor, 2004). For example, preferential trade agreements (PTAs) with environmental provisions oblige states to reduce their greenhouse gas emissions, which can create tensions between the PTAs, the UN Framework Convention on Climate Change (UNFCCC), and other trade agreements (Baghdadi et al., 2013).

While some actors can exploit regulatory inconsistencies across organizations by forum-shopping, many others must juggle policy adjustment pressures across IOs. On the one hand, actors who most feel the adjustment pressures will start looking for more hierarchical relationships, e.g. an organizational orchestrator, that they can influence as members *via* equal voting rights and other mechanisms (Abbott & Genschel, 2015; Nelson & Weaver, 2016). Scholars have shown that the UN is a likely contender for organizational orchestrator where diverse issues can be linked to each other (Acharya, 2016, pp. 1157–1158; Pouliot & Thérien, 2018). On the other hand, as this shift is likely to go against the preferences of at least some key actors who preferred partially differentiated and competing organizations, those key actors are likely to only accommodate the call for a more inclusive organization if that organization can host all the issues they have attached to the new policy domain. This explains why it is likely over time that actors will move debates about where and how to govern the new policy domain to a general-purpose and representative IO. Because they are hard to capture, such

organizations are unlikely resonance-creating organizations in the early stages of the domain emergence—but once political demands for orchestration arise, their set-up becomes advantageous.

The shift to a general-purpose organization requires governments to reevaluate their policy frames as new organizational repertoires and venues must be captured and inconsistencies addressed. To do so, governments can emphasize broad common denominator issues such as sovereignty or non-interference and coalesce ideologically congruent policy frames around them. If competition among governments prevails, these common denominators are likely to form the core of high-stake issue clusters (Clark, 2021). This is facilitated by the institutional set-up of general-purpose IOs, which contain many venues to discuss policy proposals and counter rival claims. Hence, incentives for forum-shopping and regime-shifting *across* organizations are likely to reduce, but are also likely to be replaced by the same strategies *within* a general-purpose IO. General-purpose organizations become debate orchestrators across their own venues. As contestation and competition persist, comprehensive policy solutions (e.g. general treaties) are hard to find. Instead, governments will try to address at least some adjustment pressures through carefully crafted incremental policy changes that can find majorities. Policy boundaries therefore settle very slowly and not comprehensively.

> *Proposition 3*: If organizations pursue misaligned and overlapping normative and regulatory policy frames over time, calls for adjustments trigger regime-shifting to an orchestration organization rather than competitive regime creation. If disagreements among key actors persist, this orchestration likely leads to hardening of political cleavages rather than comprehensive policy solutions.

The emerging cyberspace regime complex

Cyberspace's crosscutting potential has implications for many policy domains, providing governments with the opportunity to cluster cyber and cyber-related issues in various ways to pursue their preferences. The EU's 'human-centric technology' or China's 'cyberspace sovereignty' policy frames are examples of how policymakers cluster issues to shape cyberspace governance. These clusters not only reveal the unsettled boundaries of regime complexes but also highlight the changing political coalitions that governments create across organizations. We look at how key governments create policy frames around their preferences and seek frame resonance within new and old IOs. We then analyze how policymakers navigate pressures that guide them towards more orchestration through the UN, where accountability and sovereignty are used to link or split policy frames and ultimately create an insurmountable cleavage.

Multiple policy preferences and frames on cyberspace

Governments and their policymakers are divided over the goals and instruments in and through cyberspace (Finnemore & Hollis, 2016; Flonk et al., 2020) and therefore have introduced different issue clusters responding to such questions as: Who should govern cyberspace? What rights and responsibilities do actors have in cyberspace? How do digital risks impact progress towards digital society and

economy? How can national sovereignty be ensured in the borderless digital domain? While early involvement in shaping the internet's development in the 1970s gave the US an advantage in setting the rules for cyberspace governance, subsequent commercialization of the internet introduced new actors. With them came a multiplication of policy frames and the emergence of the cyber regime complex, which is in line with our first proposition. As we discuss key actors, with their preferences and policy frames setting the stage for the subsequent development of the regime complex,[4] we demonstrate that actors are not necessarily motivated by reducing transaction costs or avoiding turf wars. Were this the case, IOs like the International Telecommunications Union (ITU) or WTO would be the 'natural' institutional homes for cyberspace governance. Functional rationales mask the complexity and, arguably, the incompleteness of policies, as well as the degree of contestation between actors.

United States: global internet stability for economic growth

As the *de facto* controller of the internet's critical resources, the US understands cyberspace governance and internet infrastructure control as critical to its economic power. To ensure economic growth, the US prefers the internet's technological and political stability. Al Gore's 'global information society' and Bill Clinton's call for cyberspace as a 'global free trade zone' have packaged this policy frame for global consumption. A functioning infrastructure that ensures the interoperability of protocols and networks is at the core of this policy frame (Mueller, 2009). Given that the infrastructure is shared between public and private actors, the US prefers a multistakeholder approach and recognizes the importance of prescribed roles between different policy communities. For example, the Department of Justice plays a more central role in investigating cybercrime than it does in internet governance, whereas the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC) are significant players. The expanding use of the internet and growing vulnerability to malicious activities by state and non-state actors led the US to link other issues to its core preference. To counter ransomware, cyber espionage, and disinformation campaigns, the US government linked the global internet to economic growth, international security, and human rights issues under the umbrella of cyber stability. The US Cyber Deterrence Initiative (White House, 2018) links economy and security while the Declaration for the Future of the Internet (US Department of State, 2022) links economy, security, and human rights.

European Union: competitiveness to strengthen the rights-based common market

The US-dominated emerging digital economy put the EU under the twin pressures of ensuring economic competitiveness while protecting fair competition between EU member-states. That is why in the 1990s, the EU challenged the US with a proposal for an 'International Charter for Global Electronic Services' and criticized the 'monopolistic oversight of the Internet by one government' as 'no longer a politically tenable solution' (Reding, 2005). Although this view has evolved over time, the objective of protecting European businesses and citizens has not. The EU's competitiveness frame—combining the commitment to open markets with

values-driven regulation—is a cornerstone of its policies. Through its extraterritorial effect, EU regulations transformed it into a global norm setter (Bradford, 2020). The EU's antitrust and data protection laws are used to curb the expanding influence of US-based tech companies. Its competitiveness frame has evolved to address its dependence on technologies produced in third countries, especially China and the US, which became a concern. By clustering competitiveness, security, economic growth, and human rights, the EU has repackaged its core preference for competitiveness in response to pressures from the US and China (Espinoza, 2021). 'Technological sovereignty' and a 'human-centric' approach to regulation became the EU's new mantra, including in relation to emerging technologies such as Artificial Intelligence (AI).

Russia: information security to safeguard sovereignty

Russia's limited connectedness to the global economy in the 1980s reduced its role in shaping early debates about cyberspace. Not until the late 1990s, during debates around asymmetrical warfare, did Russia adopt a frame of information security that highlights the role of the internet as a potential non-military instrument of war (Jonsson, 2019). Russia's policy frame clusters the security of its national information infrastructure and influence operations with sovereignty, territorial integrity, sustainable socio-economic development, defense, and state security (MoD of Russia, 2011). To ensure information security over its national cyberspace, Russia relies on legislative and technical measures such as the 2019 'sovereign internet' law increasing control over online communication networks by isolating RuNet from the global web. The Russian agency Roskomnadzor can also fine foreign companies like YouTube or Twitter if they refuse to remove information banned in Russia. Russia's preference for sovereignty and non-intervention in domestic affairs has consistently guided its policy positions (Allan et al., 2018).

China: cyberspace sovereignty to preserve the regime

Beijing views cyberspace as an amplifier of political, economic, military, social, and cultural problems. Therefore, China's main goal is to preserve sovereignty in cyberspace as a tool to safeguard national regime legitimacy, social stability, and order. Cyberspace sovereignty is constructed around the need for a global internet governance system that gives each state the right to 'independently choose their path of cyber development' and administer cyberspace 'in accordance with their distinct political-cultural contexts and legal frameworks' (Xi, 2015). This frame clusters internet governance issues with sovereignty, sovereign equality, and non-interference. China's Great Firewall that filters information flowing into China is one expression of cyberspace sovereignty. China also invests heavily in its 'indigenous innovation' policy rooted in domestic technology base to support its international ambitions and political influence. Consequently, China's policy frame balances concerns over domestic stability with economic growth. However, accusations of cyber espionage and the close links between Chinese tech companies and the Communist Party (CCP) provoked national security concerns in other countries. As a result, China's frame merges the Russian concept of information security, the US frame of economic growth, and the EU frame of competitiveness, while clearly splitting human rights issues.

India, Brazil, South Africa: access and capacity to stimulate development

Although not an entirely cohesive group, India, Brazil, and South Africa frame cyberspace governance primarily in terms of human development and poverty reduction. They focus on accelerators of economic growth such as internet access, skills, and institutional or regulatory capabilities. Even though all three agree on the importance of sovereignty in cyberspace, they are committed to human rights protection and the multistakeholder model, differentiating them from Russia and China. There are also some differences between their approaches. South Africa champions the issue of access to new technologies as a chance to 'leapfrog' stages in development. India promotes its policy frame of a 'citizen centric' data governance model and 'data sovereignty' as the foundation for free digital trade (Hicks, 2019). Brazil closely links its policy frame to internet governance issues that are shaped through engagement with the multistakeholder community, as was the case for Brazil's Digital Bill of Rights. The three governments also act jointly to propose global governance solutions. The call for internet governance reforms by the IBSA Dialogue Forum challenged the US role in cyber governance and led to significant reforms, including the role of ICANN.

Forging frame resonance for data governance and 5G

Governments link or split their cyberspace preferences to economic growth, development, trade, or security to build competitive coalitions in organizations that best support their frame. When governments got involved in setting the rules for governing and regulating cyberspace in the 1980s and onwards, the US pursued its economic growth frame in the General Agreement on Tariffs and Trade (GATT) and in the ITU, fighting for resonance. EU member-states pursued their frames in the EU while searching for resonance of their common frame in the Organisation for Economic Co-operation and Development (OECD), G8, and the Council of Europe (CoE). Russia tried for resonance in the UN first but failed, and hence moved to task-specific organizations such as the ITU and new ROs like the Shanghai Cooperation Organization (SCO). China joined the debate later. Their attempts differentiated the emerging regime complex with overlapping and competing frames.

Dissecting all issue clusters created over the past 40 years is beyond the scope of this paper. As Figure 1 (below) demonstrates, cyberspace is a policy domain where issues can be clustered in multiple ways with concrete implications for governance. The figure should be looked at like a kaleidoscope, where different issue clusters emerge depending on which intersection one looks at. Governments search for frame resonance in organizations with organizational repertoires corresponding to their frame. We concentrate on two crosscutting and contested policy spaces—data governance and 5G—to demonstrate how governments link or split issues to build coalitions, creating resonance or resistance according to their preferences. Drawing on our immersion in the policy debates, we focus on the major overlapping and competing frames and their potential organizational hosts. The data governance case demonstrates that even powerful actors meet significant resistance to their policy frame, especially if it might lead to reallocation of authority. While the EU created resonance for its human-rights-driven frame in data governance, the US

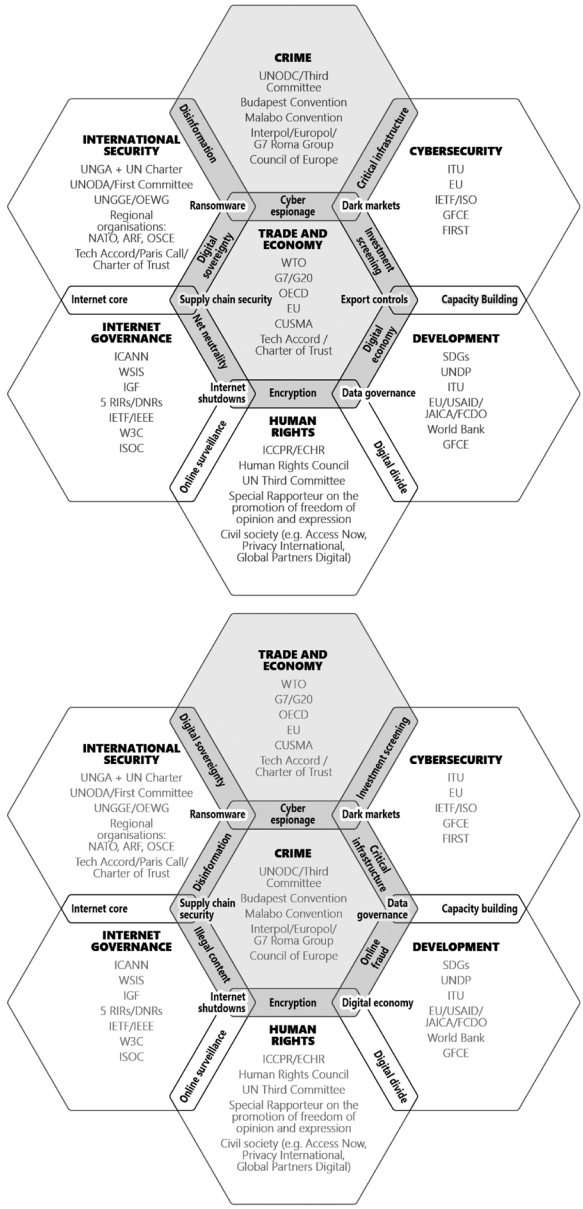

Figure 1. Selective mapping of cyberspace's organizational topography (grey hexagons are those that shifted place). Abbreviations: ARF: Association of Southeast Asian Nations Regional Forum; CoE: Council of Europe; CUSMA: Canada-US-Mexico Agreement; DNR: Domain Name Registrar; ECHR: European Court of Human Rights; EFF: Electronic Frontier Foundation; FIRST: Forum for Incident Response and Security Teams; G8: Group of Eight; G20: Group of Twenty; GFCE: Global Forum on Cyber Expertise; IAB: Internet Architecture Board; ICANN: The Internet Corporation for Assigned Names and Numbers; ICCPR: International Covenant on Civil and Political Rights; IEEE: Institute of Electrical and Electronics Engineers; IETF: Internet Engineering Task Force; IGF: Internet Governance Forum; ISOC: Internet Society; ITU: International Telecommunication Union; NATO: North Atlantic Treaty Organization; OAS: Organization of American States; OECD: Organization for Economic Co-operation and Development; OEWG: Open-Ended Working Group (UN); OSCE: Organization for Security and Co-operation in Europe; RIR: Regional Internet Registry; SCO: Shanghai Cooperation Organization; UNGA: United Nations General Assembly; UNGGE: UN Group of Governmental Experts; UNODA: United Nations Office for Disarmament Affairs; UNODC: United Nations Office on Drugs and Crime; WSIS: World Summit on Information Society; WTO: World Trade Organization; W3C: World Wide Web Consortium.

failed to do the same with the weaponization of data transfers (i.e. the proposed ban of TikTok) and instead was met with Chinese resistance in the WTO. In the 5G rollout, we observe how governments adjust their frames when confronted with resistance within their preferred task-specific IOs (EU and the North Atlantic Treaty Organization, NATO) and attempt competitive regime creation (US-led 5G Prague Conference, 5G Club of Democracies). We also see how issue-linking enables China to bring 5G to task-specific organizations like the WTO or attempt competitive regime creation through the Global Initiative on Data Security (GIDS).

While these cases represent only a small fraction of the broad landscape of overlapping and competing policy frames, where machine learning, quantum computing, or disinformation are also debated, their multiplication shows that cyber has no obvious organizational home where potential conflicts over competing framings can be addressed. Instead, policymakers have used issue-linking and -splitting to introduce and cluster cyberspace in a multitude of organizations. The chances that issue clusters resonate with the organization's membership are highest in relatively homogenous organizations, thereby confirming our second proposition. Contrary to the expectations of functional approaches, we observe a growing density of IOs, without efforts of inter-organizational coordination.

Data governance: linking and splitting privacy, security, and digital economy

The growing importance of personal data for digital trade or national security makes data governance a core issue in cyberspace. Governments do not value the diversification of data uses in the same way, pursuing different policy frames and strategies. The growing automation of data processing and the absence of a global data governance regime or an IO with authority to adopt binding rules resulted in a patchwork of national legislations and multiple frames—which resonate with regional and task-specific organizations in particular but also frustrate governments that have to navigate across organizations.

Concerns about proliferation of national legislation (e.g. in Austria, Denmark, France, Germany, and Sweden) that could undermine individual rights or disrupt important sectors of the economy (banking, insurance) have prompted the European Commission to develop data protection laws. Germany's strong data protection safeguards played a critical role in shaping these legal rules, which resulted in an EU frame linking market competitiveness, fairness, and fundamental rights. This frame found its expression in the 1995 Data Protection Directive and the 2016 General Data Protection Regulation (GDPR). It was also enshrined as a fundamental right in the EU Charter of Fundamental Rights and the 2009 Lisbon Treaty. The European Commission became a central player on behalf of EU member-states, conditioning EU market access by introducing an equivalence scheme (i.e. adequacy decisions) as one of the mechanisms to sanction non-compliant companies. The EU used overlapping memberships in the OECD and CoE to further externalize this frame, for instance, through modernization of the OECD Privacy Guidelines and the CoE Convention 108 on Data Protection. Linking competitiveness to human rights also allowed the EU to create resonance for this frame though courts, like the European Court of Human Rights.

The US focused on strengthening its economy in the 1990s and underplayed the impact of the EU whose internal market rules were in nascency. Later, the clash

between the US frame of economic growth and the EU frame rooted in human rights made it difficult to build coalitions (Fefer & Archick, 2021). The situation got more complicated after 9/11 when the US linked data governance to national security and externalized this frame through a system of national rules with extra-territorial implications (e.g. the obligation imposed on airlines to transfer passenger name records). This led to conflicts with the EU, which described the US approach as 'unbalanced and unsustainable' and called for the creation of a multilateral framework for Passenger Name Record Data Transfer within the International Civil Aviation Organization (ICAO) (European Commission, 2003). Reports in 2013 of widespread US online surveillance practices and the potential involvement of some US tech companies further undermined the US frame. In response, Brazil and Germany (whose leaders were targeted) linked data governance more clearly to human rights and introduced this frame as the right to privacy in the digital age at the UN.

China is a latecomer to the discussion about data governance. The success of Chinese tech giants like Tencent and ByteDance (respective owners of WeChat and TikTok) is built on the government-sanctioned commercial use of data with little protection for privacy or human rights online. The expansion of these companies to new markets, including the US and EU, is used by China to promote its cyber-space sovereignty frame. The US challenges this frame, accusing Tencent and ByteDance of collaborating with the CCP to obtain proprietary information and carry out disinformation campaigns to China's benefit (White House, 2020). However, the US linking of privacy and national security through 'weaponization of data' brought limited results. The EU's frame rooted in human rights and competitiveness dictated its approach to the governance of online platforms like TikTok—but also Facebook and Twitter. Instead of using bans as a policy solution as proposed by the US, the EU's Digital Markets Act and Digital Services Act imposed universally applicable conditions and obligations on these companies. Although India banned more than 170 Chinese applications as threatening the 'sovereignty and integrity of India' (Press Information Bureau, 2020), this move was motivated by border skirmishes with China rather than the resonance of the US frame. China countered the US frame by splitting data governance from national security and instead linking it to development and free trade. It called US and India's actions 'discriminatory practices violating WTO rules' and 'economic bullying' (MFA of China, 2020a) that violate the basic principles and objectives of the multilateral trading system (Embassy of China in India, 2020). Although China raised the issue in a closed-door WTO Council for Trade in Services meeting in October 2020 (Bermingham, 2020), it did not formally contest US national legislation, fearing the implications for its own sovereignty frame embodied in the Great Firewall.

While we observe that the EU frame resonates not only among its membership but also across other countries and organizations, no hierarchal inter-organizational or inter-regulatory relations have been established. Instead, we observe steps aimed at regime-shifting and competitive regime creation (see the special issue framework paper). The US continues to challenge the EU's human-rights-driven frame of data governance (Slaughter & McCormick, 2021) for 'creating significant risks for public safety' (US Mission to the EU, 2020), stressing the negative implications of GDPR for the fight against cybercrime by undermining the functioning of the WHOIS

database governed by the ICANN. The US is also using the UN Ad Hoc Committee on Cybercrime (AHC) to build a coalition against the EU data governance frame, which carries significant political costs (impact on national security) and financial costs (sanctions for non-compliance).[5] China, on the other hand, proposed the multilateral Global Initiative on Data Security on the basis of 'universal participation by all parties' and 'a balanced approach to technological progress, economic development and protection of national security and public interests' (MFA of China, 2020b). By linking and splitting issues from both EU and US frames, China created a frame that resonates with other ROs, leading to new competitive cooperation platforms such as the China-League of Arab States Cooperation Initiative on Data Security (MFA of China, 2021).

Capturing task-specific organizations with diverse and universal membership has proven more difficult. More than 80 countries are engaged in WTO e-commerce negotiations launched in 2017. Key players have expressed competing and overlapping frames. The US favors an agreement with 'meaningful trade rules' that support global economic growth and development (WTO, 2019a). China is unwilling to make any formal commitment that would undermine its cyberspace sovereignty frame (WTO, 2019b). The EU is open to a deal on cross-border data transfers but proposes exceptions linked to data protection (WTO, 2019c). At the G20 summit in Osaka, Japan tried to bridge these gaps and proposed a Declaration on the Digital Economy that linked the digital economy to intellectual property rights, protection of personal information, and cybersecurity (Ministry of Foreign Affairs of Japan, 2020). India, Indonesia, and South Africa refused to sign the document, as these Global South countries had no opportunity to express their views (Haidar, 2019).

Ultimately, in the densely institutionalized cluster of data governance, the frames have multiplied and resonated across specialized IOs (OECD, G20, CoE, ICAO), ROs (EU, AU) and regional trade arrangements (APEC Cross-Border Privacy Rules System). This growing density of IOs raises costs for governments with limited resources and creates adjustment pressures within task-specific organizations like the WTO.

5G rollout: linking and splitting national security, digital trade, human rights, and development.

5G networks are designed to connect machines, objects, and devices. Due to their capacity, reliability, and efficiency, the technology is critical for digital transformation of the economy and public services, from remote access to healthcare, precision agriculture, or safer transportation networks. As such, it increasingly attracts government attention.

As a leading supplier of the 5G systems—with Sweden's Ericsson and Finland's Nokia—the EU and its member-states have linked their competitiveness frame to digital transformation, research, and innovation. The EU promoted this frame through bilateral cooperation agreements with other market leaders, namely South Korea and Japan. Considering 5G as a technological issue for standardization bodies, the EU split it from the human rights dimension of its core frame and opened the way to a partnership with China, despite a clear clash with China's cyberspace sovereignty frame (European Commission, 2015). This move also allowed the EU to

create resonance in standardization bodies like the 3rd Generation Partnership Project (3GPP).

In the 2010s, the US started linking 5G rollout to stability, national security, and human rights in an effort to curb China's technology-enabled growth as a global power (Gallagher, 2022). The Trump administration tied Huawei and ZTE—Chinese champions in 5G technology—to the CCP and China's military, presenting them as a threat to global security and democracy and calling for their blockage from foreign markets (US House of Representatives, 2012). In practice, this meant undermining the Chinese frame of cyberspace sovereignty. The US frame linking economic growth to national security and cybersecurity was too distant from the organizational repertoire of the *technical* standardization bodies, such as ITU, 3GPP, and the Internet Engineering Task Force (IETF). Hence, the US tried to create resonance for its frame around 5G in NATO and through NATO allies also in the EU. Using its NATO membership, the US introduced its frame, for instance through the NATO Communications and Information (NCI) Agency. In the EU, it built coalitions with allies like Poland, the Czech Republic, and Estonia to alter the EU's common frame. There, this frame met with resistance from European governments with significant economic ties to China (Nietsche & Rasser, 2020).

Since NATO and the EU provided only limited opportunities for creating frame resonance, the US moved to create new platforms. The 2019 Prague 5G Security Conference started as a new channel to promote the US national security frame, resulting in the non-binding Prague Proposals on 5G security. Furthermore, by including 5G in a broader cluster of infrastructure, the US proposed a new policy frame linking sustainable growth and resilient economic recovery that was also discussed in G7 and G20 (e.g. G20 Principles for Quality Infrastructure Investment). Finally, the US attempted to gather broader support by splitting economic development from security and linking the former to human rights and democratic values instead. These efforts have led to the calls for new platforms such as a '5G club of democracies' bringing together Australia, South Korea, India, and the G7, or T-12 as a platform to address the rise of 'techno-autocracies' and economic competition from those countries (Fisher, 2020).

The Chinese government denied any influence over Huawei or ZTE. But as US accusations persisted and more countries started reviewing their policies towards Huawei (including big markets in Europe, India, Australia, and Canada), China's cyberspace sovereignty frame was challenged. Chinese authorities described Huawei technology bans as undermining market economy principles and WTO free trade rules (Global Times, 2020). China challenged the US frame by splitting economic growth and competitiveness from national security and instead linking it to access, free trade, fairness, and development, which it knew would resonate better with developing countries representing a sizeable market for Chinese tech products. In a position paper to the UN General Assembly (UNGA), China framed 5G as a technological issue that 'belongs to mankind and should be used to benefit all' (MFA of China, 2020c). China used bilateral cooperation with Asian and African countries under the Digital Silk Road (Cheney, 2019) to create resonance for this frame and signaled the possibility of bringing the issue to the WTO to investigate potential US abuse of the WTO national security exception. Also, to support its frame without recourse to Western-dominated financial organizations, China used the Asian Infrastructure Development Bank (AIDB) to fund its digital investment projects.

The case of 5G technologies confirms that capturing IOs with new frames is difficult, especially if costs to members are high. In case of the 5G roll-out, the cost of upsetting economic and political relations with China was clearly too high for many governments. In the case of NATO, the 2019 Leaders Meeting in London stressed the importance of 'the security of communications, including 5G' but was not followed by any concrete decisions impacting the whole Alliance (Gilli & Bechis, 2020). In the 5G cybersecurity toolbox, EU member-states split economic growth from national security and instead linked it to risk management. Compared to the ban of Huawei and ZTE equipment adopted by the US, this frame gave EU governments more flexibility and carried lower costs for countries unwilling to upset their relations with China (e.g. Germany, France), even though such an approach risked undermining the EU's human-rights-centric frame (European Court of Auditors, 2020). To foster infrastructure investment (including the 5G rollout), the US, Australia, and Japan launched the Blue Dot Network and requested technical support coordination from the OECD. But national security and human rights frames around 5G did not manage to create resonance among developing countries, many of whom preferred China's linking to development and open markets. The African Union (AU), for instance, concluded a Memorandum of Understanding with Huawei to strengthen cooperation on broadband, cloud computing, and 5G. Nonetheless, China's efforts to capture the general-purpose UN with this frame have also failed.

The multiplication of frames and organizations for discussing 5G—especially the number of new regional or task-specific platforms established—suggests partially overlapping but non-hierarchical inter-organizational relations. With national decisions about 5G rollouts, we are likely to observe further fragmentation of the markets, which will ultimately increase pressures on the existing ROs for harmonization through binding commitments (EU, NATO) or clarification of the existing trade rules (WTO). As the Global South becomes an important market in new technologies, we also see the growing importance of ROs like the AU. The US focus on decoupling from China and the EU's human-centric digital transformation put pressure on other countries to choose between the US, EU, and China for access to technologies, resulting in increasing political and economic costs.

Adjustment pressures and bifurcated orchestration at the UN

The multiplication of cyber-related policy frames and organizations has become resource-intensive for many actors navigating different formal and informal obligations. Regulatory and legal uncertainties, driven by inter-organizational competition and growing inequalities resulting from states' limited capacities to effectively participate in multiple concurrent cyber processes (Rothstein, 2022), have pushed many governments to pursue their grievances at the UN. Gradually, the volume of submissions and increasing participation of Global South countries in cyber-related debates at the UN made ignoring the UN's role impossible.

This shift is driven by development-oriented countries that see the UN as the only IO where they can seek resonance for their own cyber policy frames centered around the building of cyber-related capacities.[6] Ironically, the adjustment pressures driven by those countries also worked to the advantage of Russia and China, who

from the beginning favored greater UN involvement in cyberspace governance due to their privileged UN Security Council position. The EU and US have long resisted attempts to advance a state-centric and central cyberspace governance approach at the UN, since the nonhierarchical and differentiated regime complex allowed them to navigate different organizations and link/split issues according to their

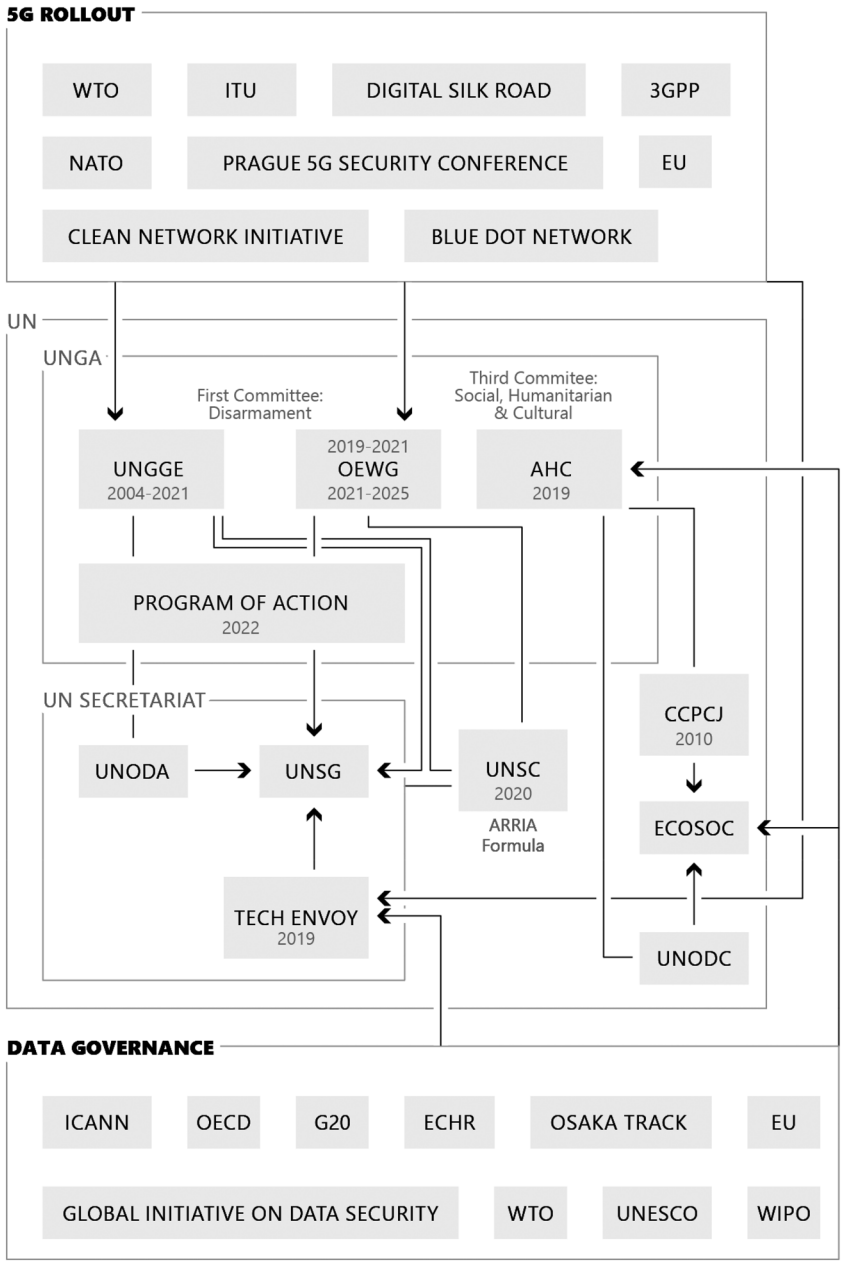

Figure 2. Orchestration of data governance and 5G at the UN.

preferences. At the UN, the EU and US are forced to invest significant resources in building cross-regional coalitions without any guarantee of policy frame success.[7]

With cyber-related policy frames proliferating across the UN, the question became not whether the UN is the right place, but which venue(s) within it should be prioritized. Figure 2 (below) illustrates how 5G and data governance were increasingly moved to different venues at the UN strengthening its role as an orchestrating IO. Governments engage different venues within the UN to bridge frames previously discussed elsewhere. A Russia-sponsored resolution made the UN Third Committee the home of an Ad Hoc Committee tasked to draft a new cybercrime convention until 2024, which includes elements of data governance debates that took place in organizations such as the UN Office on Drugs and Crime (UNODC), CoE, and Interpol (UN, 2019). Russia also succeeded in turning the OEWG in the UN First Committee into a central place for discussions about international security in cyberspace, which includes 5G, supply chain security, and critical infrastructure. Those issues were previously central to the work of task-specific IOs like the ITU, WTO, OECD, and the G7.

Not only did cyberspace find institutional homes in two different UN Committees, but once government attention focused on the UN, the First Committee split—for the first time in its history—into two parallel processes with identical mandates to further clarify rules applicable to cyberspace: The US-sponsored GGE and the Russia-sponsored OEWG (UN, 2018a, 2018b). From 2019–2021, both processes ran in parallel until the OEWG mandate was renewed in 2021 while the GGE's was not. Both processes were approved by the UNGA but states like Russia, China, or Iran criticized the GGE (whose membership has increased from 15 to 25 members over the years) for lacking the legitimacy to set norms and rules for the entire UN membership. Hence, GGE consensus reports establishing the framework for responsible state behavior (RSB)—including 11 norms reaffirming the applicability of the existing international law and proposing confidence-building measures in cyberspace—became a subject of contestation in the OEWG. Russia and China portray the OEWG, which is open to all states, as the main venue for a universal and democratic debate and use it to pursue policy frames with sovereignty claims at their core.[8] While the US and EU initially opposed the OEWG, they were forced to engage in the process to defend and 'universalize' the GGE's RSB *acquis* (UN, 2021a). The OEWG produced a report in 2021 that replicated many GGE conclusions but also included additional proposals by Russia, China, and Iran. We focus here on the debates within the GGE and OEWG, which epitomize how governments coalesced around major cleavages linking or splitting issues around sovereignty or accountability.

A cleavage emerged within and across these two processes, whereby Russia and China reinforced coalitions around sovereignty while the US and EU did the same around accountability. As long as policy frames have accountability—broadly understood as agreement on the application of *existing* international law and norms among states—the US and EU have not objected to issue-splitting and -linking. They propose multilateral cooperation frameworks that promote accountability (cyber deterrence, collective public attribution).[9] They supported framing around accountability proposed by South Africa, Thailand, Turkey, and Egypt, which linked it to their preferred frames of capacity-building as a precondition for the implementation of the norms and the application of international law (UN, 2021a). Such

linking was later reflected in an Australian and Mexican proposal for a survey on UN cyber norm implementation (now accepted as part of the OEWG). To limit the potential burden of implementing RSB norms, international law, and confidence-building measures, the Caribbean Community (UN, 2021b) and Egypt (UN, 2021c) linked accountability to cyber capacity building (CCB), economic growth, and development, arguing for 'common but differentiated responsibility' that conditions state obligations and responsibilities in cyberspace on their level of development. The US and the EU oppose Russia-orchestrated calls for policy tools like a new treaty or code of conduct, describing them as 'futile' and a 'remendous distraction' (UN, 2021a).

Sovereignty lies at the core of the frames created by Russia and China who have supported issue-linking accordingly in the OEWG (UN, 2021d). They supported Iran who (subject to trade sanctions) has used sovereignty to split capacity-building from export controls and human rights, arguing that CCB should disarm 'unilateral digital sanctions' (UN, 2021e). Struggling with market access limitations for its tech companies, China proposed formulating 'objective international rules and standards' on supply chain security (UN, 2021f) and linked cyber espionage and mass surveillance frames to undermine the US in forging coalitions targeting China (UN, 2021 g). At the same time, Russia and China spearheaded efforts to split issues proposed by Canada and the United Kingdom (UK), such as social aspects, human rights, and gender equality, which they view as potential threats to sovereignty in cyberspace. Russia and its allies (China, Iran, Cuba, and Venezuela) repeatedly called for a new legally binding instrument as the only policy tool to guarantee respect for sovereignty and non-interference (UN, 2015).

With the GGE's mandate ending in 2021, Australia, Canada, and the EU, among others, did not want to accept that the OEWG would become the sole venue to orchestrate how to govern cyberspace, fearing that sovereignty would become the dominant policy frame. To minimize this risk, France—with support from Egypt and 40 other countries—pushed for a UNGA resolution establishing a new permanent regulatory dialogue, the Program of Action (PoA) to advance responsible state behavior in cyberspace, which will replace the OEWG in 2025 (UN, 2022). Having learned from the success of the Russia-sponsored resolution establishing the OEWG and recognizing the importance of access and capacities for developing countries, CCB is central to the PoA proposal. This proposal further increases the UN's orchestration capacity among regional (EU, COE, OAS, ASEAN, ECOWAS) and task-specific IOs (ITU, UNODC, Interpol) engaged in CCB and reinforces the state-centric model of cyberspace governance preferred by China and Russia (UN, 2018a). The US remains ambivalent about UN-led processes as their outcomes, although voluntary in nature, increase scrutiny of the US's unilateral actions, making weaponization of interdependencies more complicated. The PoA will add to, and potentially further consolidate, the existing framework documents and acquis from both the GGE and the OEWG.

As the UN has become the orchestrating IO where governments debate and decide the contours of cyberspace, other IOs have acknowledged the centrality of the GGE and OEWG in their own work. In 2017, the Organization of American States (OAS) established a 'Working Group on Cooperation and Confidence-Building Measures in Cyberspace' to prepare a set of confidence-building measures for the region, building on the consensus reports of the GGE (OAS, 2017). The following

year, the Association of Southeast Asian Nations (ASEAN) agreed in principle to GGE norms and focus on regional capacity-building to implement these norms (ASEAN, 2018) and the SCO Expert Group on International Information Security referred to the OEWG and GGE (SCO, 2019). Other IOs, including the Organization for Security and Co-operation in Europe (OSCE), the G7, AU, or the Global Forum on Cyber Expertise (GFCE) also have committed to working towards the implementation of the cyber-related UN norms.

In line with proposition 3, while adjustment pressures led to a regime shift to the UN, it also hardened political cleavages and expanded the number of UN venues for debating cyberspace. As a result, governments agree only narrowly on technical, normative, and legal documents, if at all. What looks at first sight to be a functional spillover to the UN reveals itself as a politicized process that used to occur across many organizations and now also happens within an orchestrating one.

Conclusion

By taking the politics of policy boundaries seriously, we gain important insights into the architecture and development of regime complexes, as well as into actors' behavioral adjustments. When new issues emerge in a densely institutionalized environment that crosscut already institutionalized policy domains, we observed that neither policy domains nor their organizational homes are set in stone. There are no immutable rules determining which IO will help govern them or how. We have shown how cyberspace unsettles existing policy boundaries and how governments contest emerging policy boundaries around cyberspace. Economic issues are thereby often at the forefront of the political debate, but are linked to and embedded in issues around national security or development.

Strategic framing through issue-linking and -splitting and the search for frame resonance have major implications for regime complexes. As the special issue has postulated, framing and successful frame resonance help explain the origins of regime complex structures. Through the lens of framing strategies, we showed that regime complexes do not simply emerge and remain static over long periods of time. While regime complexes can constrain actors in the short-term, contesting frames and their associated compliance pressures trigger a process that demonstrates the malleability of regime complexes in the long-run, as successful framing changes their scope and size and makes them more or less differentiated and hierarchical. Existing scholarship has emphasized that actors search for the IO that best serves their preferences within a given policy domain. Such scholarship focuses on the impact of strategies *for* actors *within* regime complexes. Studying policymakers in search of frame resonance shows that strategies also can *create* and *change* regime complexes, as well as change the stakes of cooperation.

Our findings are likely to travel to other emerging policy domains such as artificial intelligence, blockchain technologies (Beaumier & Kalomeni, 2022), or issues that can be framed as crosscutting and consequently unsettle existing organizational and inter-organizational configurations. For example, actors have linked issues such as trade with security or the environment to form policy nexuses such as trade-peace or trade-environment. We have argued that a major factor likely contributing to regime complex development over time are governments who (re)frame policies

and look for frame resonance in organizations, thereby impacting authority and differentiation dynamics as well as policy adjustment and dissatisfaction. In times when scholars and pundits point to dramatic changes in global order-making and harsh geoeconomic and geopolitical differences across governments, disagreement over *how* and *where* a particular issue or issue cluster should be governed is likely. Even if we observe that debates eventually consolidate within a single global and representative organization, we should not expect comprehensive multilateral policy solutions. But as long as actors continue to debate within organizations, incremental solutions and adjustments are likely to emerge that alleviate some dissatisfaction.

Notes

1. We use organization as an umbrella term for formal, informal, state-led, or multistakeholder organizations.
2. Cyberspace has almost four billion users, with a third living in the developed world and a digital economy estimated to represent between 4.5 and 15.5% of world gross domestic product (GDP) (UNCTAD, 2019).
3. Issue linkages have mainly been discussed in national or IO trade policy analyses (Davis, 2004); they have hardly been discussed in the context of regime complexes and how different economic policies are embedded in larger issue clusters.
4. These policy frames are derived from participation in global and bilateral cyber policy processes and are cross-referenced with official documents.
5. Based on exchanges with government officials and participation in AHC meetings.
6. Based on exchanges with government officials during OEWG meetings.
7. Ibid.
8. Ibid., and interventions by Russian and Chinese officials at the OEWG.
9. Based on participation in informal GGE sessions and OEWG sessions.

Acknowledgements

The authors are very thankful for comments and suggestions from Daniëlle Flonk, Miles Kahler, Xymena Kurowska, and the participants at two (virtual) regime complexity workshops (in particular Randy Henning and Tyler Pratt). Farrah Hawana did a fabulous job editing this paper and Christian Dietrich helped us with the figures.

Disclosure statement

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

Funding

Stephanie C. Hofmann's research for this article was supported by the Swiss National Science Foundation [grant number #100017_172667].

Notes on contributors

Stephanie C. Hofmann holds the Joint Chair in International Relations between the Department of Political and Social Science and Robert Schuman Centre of Advanced Studies at the European University Institute and is director of the Europe in the World research area. Her research revolves

around densely institutionalized spaces, multilateralisms, national preference formation on foreign and security policy issues and global ordering processes.

Patryk Pawlak is a visiting scholar at Carnegie Europe and a visiting fellow at the Robert Schuman Centre of Advanced Studies at the European University Institute (Florence). He has extensive research and policy experience in international cyber issues, including at the EU and the UN. His research focuses on accountability, coercive diplomacy and capacity building in cyberspace.

ORCID

Stephanie C. Hofmann http://orcid.org/0000-0003-0045-8356

References

Abbott, K., & Genschel, P. (2015). *International Organizations as Orchestrators* (Snidal, D., & Zangl, B., Eds.). Cambridge University Press.

Acharya, A. (2016). 'Idea-shift': How ideas from the rest are reshaping global order. *Third World Quarterly*, *37*(7), 1156–1170. https://doi.org/10.1080/01436597.2016.1154433

Adler-Nissen, R., & Zarakol, A. (2021). Struggles for recognition: The liberal international order and the merger of its discontents. *International Organization*, *75*(2), 611–634. https://doi.org/10.1017/S0020818320000454

Allan, B. (2017). Producing the climate: States, scientists, and the constitution of global governance objects. *International Organization*, *71*(1), 131–162. https://doi.org/10.1017/S0020818316000321

Allan, B., Vucetic, S., & Hopf, T. (2018). The distribution of identity and the future of the international order: China's hegemonic prospects. *International Organization*, *72*(4), 839–869. https://doi.org/10.1017/S0020818318000267

Andonova, L. (2017). *Governance Entrepreneurs. International Organizations and the Rise of Global Public-Private Partnerships*. Cambridge University Press.

ASEAN. (2018). Chairman's statement of the third ASEAN *Ministerial Conference on Cybersecurity*. https://asean.org/asean2020/wp-content/uploads/2021/01/AMCC-2018-Chairmans-Statement-Finalised.pdf

Baghdadi, L., Martinez-Zarzoso, I., & Zitouna, H. (2013). Are RTA agreements with environmental provisions reducing emissions? *Journal of International Economics*, *90*(2), 378–390. https://doi.org/10.1016/j.jinteco.2013.04.001

Baumgartner, F., & Jones, B. (1993). *Agendas and Instability in American Politics*. University of Chicago Press.

Beaumier, G., & Kalomeni, K. (2022). Ruling through technology: Politicizing blockchain services. *Review of International Political Economy*, *29*(6), 2135–2158. https://doi.org/10.1080/09692290.2021.1959377

Bermingham, F. (5 October (2020). TikTok, WeChat bans by US and India broke WTO rules, China says. *South China* Morning Post. https://www.scmp.com/economy/china-economy/article/3104239/china-says-us-and-indian-bans-tiktok-wechat-broke-wto-rules

Bocquillon, P. (2018). (De-)Constructing coherence? Strategic entrepreneurs, policy frames and the integration of climate and energy policies in the European Union. *Environmental Policy and Governance*, *28*(5), 339–349. https://doi.org/10.1002/eet.1820

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Branch, J. (2021). What's in a name? Metaphors and cybersecurity. *International Organization*, *75*(1), 39–70. https://doi.org/10.1017/S002081832000051X

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner.

Calcara, A., & Marchetti, R. (2022). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*, *29*(4), 1237–1262. https://doi.org/10.1080/09692290.2021.1913438

Carpenter, C. (2011). Vetting the advocacy agenda: Network centrality and the paradox of weapons norms. *International Organization*, *65*(1), 69–102. https://doi.org/10.1017/S0020818310000329
Cheney, C. (2019). China's digital silk road: A strategic technological competition and exporting political illiberalism. Issues & Insights, 19, WP8, July 2019 Working Paper. https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf
Chong, D., & Druckman, J. (2007). Framing theory. *Annual Review of Political Science*, *10*(1), 103–126. https://doi.org/10.1146/annurev.polisci.10.072805.103054
Clark, R. (2021). Pool or duel? Cooperation and competition among international organizations. *International Organization*, *75*(4), 1133–1153. https://doi.org/10.1017/S0020818321000229
Cooley, A. (2015). Authoritarianism goes global: Countering democratic norms. *Journal of Democracy*, *26*(3), 49–63. https://doi.org/10.1353/jod.2015.0049
Davis, C. (2004). International institutions and issue linkage: Building support for agricultural liberalization. *American Political Science Review*, *98*(1), 153–169. https://doi.org/10.1017/S0003055404001066
DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
Embassy of China in India. (2020). *Response to media query by Spokesperson of Chinese Embassy in India Counselor Ji Rong on the Government of India's Decision of Blocking 118 Chinese Mobile Apps*, 3 September. http://in.china-embassy.org/eng/embassy_news/t1811909.htm
Entman, R. (2004). *Projects of Power: Framing News, Public Opinion, and U.S. Foreign Policy*. University of Chicago Press.
Espinoza, J. (2021). EU tech policy is not anti-American, says Vestager. Financial Times, June, 20. https://www.ft.com/content/d00fb0f3-b542-438f-9d7a-8b83e1d3630f
European Commission. (2003). *Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*. COM/2003/0826 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0826:EN:HTML.
European Commission. (2015). *5G Vision*. https://digital-strategy.ec.europa.eu/en/policies/5g-research-standards
European Court of Auditors. (2020). 5G Roll-out in the EU: Delays in Deployment of Networks with Security Issues Remaining Unresolved. Special Report. https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/en/.
Farrell, H., & Newman, A. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351
Fefer, R., & Archick, K. (2021). *U.S.-EU Privacy Shield and Transatlantic Data Flows*. Congressional Research Service. 22 September. https://crsreports.congress.gov/product/pdf/R/R46917
Finnemore, M., & Hollis, D. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/S0002930000016894
Fioretos, O. (2017). *International Politics and Institutions in Time*. Oxford University Press.
Fisher, L. (2020). Downing Street plans new 5G club of democracies. The Times, May, 29. https://www.thetimes.co.uk/article/downing-street-plans-new-5g-club-of-democracies-bfnd5wj57
Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, *9*(2), 364–386. https://doi.org/10.1017/S2045381720000167
Gallagher, J. (2022). U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests. Congressional Research Service. 5 January. https://www.everycrsreport.com/files/2022-01-05_R47012_65c5c54827b8fef912a19079f10e144b3b88d009.pdf
Gehring, T., & Faude, B. (2014). A theory of emerging order within institutional complexes. *Review of International Organization*, *9*(4), 471–498. https://doi.org/10.1007/s11558-014-9197-1
Gilli, A., & Bechis, F. (2020). NATO and the 5G challenge. NATO Review, September, 30. https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html.
Global Times. (2020). Great Britain cannot be 'Great' without independent policies toward China: Chinese envoy. *Global Times*, August 16. https://www.globaltimes.cn/content/1197901.shtml
Goffman, E. (1974). *Frame Analysis. An Essay in the Organization of Experience*. Harper.
Haidar, S. (2019). At G20, India Stands with Developing World—Not U.S., Japan—on 5G and Data. The Hindu, June, 28. https://www.thehindu.com/news/national/on-5g-and-data-india-stands-with-developing-world-not-us-japan-at-g20/article28207169.ece
Henning, R., & Pratt, T. (2023). Hierarchy and differentiation in international regime complexes: a theoretical framework for comparative research. *Review of International Political Economy*.

Hicks, J. (2019). 'Digital colonialism': Why countries like India want to take control of data from Big Tech. The Print. September, 29. https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/

Hofmann, S. (2019). The politics of overlapping organizations: Hostage-taking, forum shopping, and brokering. *Journal of European Public Policy*, *26*(6), 883–905. https://doi.org/10.1080/13501763.2018.1512644

Hofmann, S. (2013). *European Security in NATO's Shadow: Party Ideologies and Institution Building*. Cambridge University Press.

Jinnah, S., & Morin, J.- F. (2020). *Greening Through Trade: How American Trade Policy is Linked to Environmental Protection Abroad*. The MIT Press.

Johnson, T., & Urpelainen, J. (2012). A strategic theory of regime integration and separation. *International Organization*, *66*(4), 645–677. https://doi.org/10.1017/S0020818312000264

Jonsson, O. (2019). *The Russian Understanding of War: Blurring the Lines Between War and Peace*. Georgetown University Press.

Jupille, J., Mattli, W., & Snidal, D. (2013). *Institutional Choice and Global Commerce*. Cambridge University Press.

Knaack, P., & Gruin, J. (2021). From shadow banking to digital financial inclusion: China's rise and the politics of epistemic contestation within the Financial Stability Board. *Review of International Political Economy*, *28*(6), 1582–1606. https://doi.org/10.1080/09692290.2020.1772849

Krasner, S. (1976). State power and the structure of international trade. *World Politics*, *28*(3), 317–347. https://doi.org/10.2307/2009974

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022

MoD of Russia. (2011). The Concept on the Activities of the Armed Forces of the Russian Federation in the Information Space.

MFA of China. (2020a). Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference, 14 September. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1814845.shtml

MFA of China. (2020b). Global Data Security Initiative, 8 September. https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm

MFA of China. (2020c). Position Paper of the People's Republic of China on the 75th Anniversary of the United Nations, 10 September. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1813751.shtml.

MFA of China. (2021). China-League of Arab States Cooperation Initiative on Data Security, 29 March. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1865098.shtml

Ministry of Foreign Affairs of Japan. (2020). Osaka Declaration on Digital Economy, 28 June. https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/special_event/

Morse, J., & Keohane, R. (2014). Contested multilateralism. *The Review of International Organizations*, *9*(4), 385–412. https://doi.org/10.1007/s11558-014-9188-2

Mueller, M. (2009). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. The MIT Press.

Müller, B. (Ed.). (2013). *The Gloss of Harmony: The Politics of Policy-Making in Multilateral Organisations*. Pluto Press.

Muzaka, V. (2011). Linkages, contests and overlaps in the global intellectual property rights regime. *European Journal of International Relations*, *17*(4), 755–776. https://doi.org/10.1177/1354066110373560

Nair, D. (2021). 'Hanging out' while studying 'up': Doing ethnographic fieldwork in international relations. *International Studies Review*, *23*(4), 1300–1327. https://doi.org/10.1093/isr/viab001

Nelson, S., & Weaver, C. (2016). Organizational Culture. In J. K. Cogan, I. Hurd, & I. Johnstone (Eds.), *The Oxford Handbook of International Organizations*, 920–939. Oxford University Press.

Nietsche, C., & Rasser, M. (2020). Washington's anti-Huawei tactics need a reboot in Europe. *Foreign Policy.* https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/

Nye, J. (2014). The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance. https://www.cigionline.org/static/documents/gcig_paper_no1.pdf

Odell, J. (2018). *Negotiating the World Economy*. Cornell University Press.

Phillips, N., Sewell, G., & Jaynes, S. (2008). Applying critical discourse analysis in strategic management research. *Organizational Research Methods*, *11*(4), 770–789. https://doi.org/10.1177/1094428107310837

Pouliot, V., & Thérien, J.- P. (2018). Global governance: A struggle over universal values. *International Studies Review*, *20*(1), 55–73. https://doi.org/10.1093/isr/vix025

Press Information Bureau. (2020). *Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defense of India, security of state and public order.* 29 June. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206

Price, V., & Tewksbury, D. (1997). News Values and Public Opinion: A Theoretical Account of Media Priming and Framing. In G. Barnett & F. Boster (Eds.), *Progress in Communication Sciences*., 173–212. Ablex Publishing.

Princen, S. (2011). Agenda-setting strategies in EU policy processes. *Journal of European Public Policy*, *18*(7), 927–943. https://doi.org/10.1080/13501763.2011.599960

Raustiala, K., & Victor, D. (2004). The regime complex for plant genetic resources. *International Organization*, *58*(02), 277–309. https://doi.org/10.1017/S0020818304582036

Reding, V. (2005). Privatize Internet Governance. The Wall Street Journal Europe, November, 16. http://ec.europa.eu/information_society/doc/internetgovernance.pdf

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus & Giroux.

Rothstein, S. (2022). Toward a discursive approach to growth models: Social blocs in the politics of digital transformation. *Review of International Political Economy*, *29*(4), 1211–1236. https://doi.org/10.1080/09692290.2021.1895278

Schattschneider, E. E. (1957). Intensity, visibility, direction and scope. *American Political Science Review*, *51*(4), 933–942. https://doi.org/10.2307/1952444

SCO. (2019). *SCO Expert Group on International Information Security meets in Moscow*. Available at: http://eng.sectsco.org/news/20191112/600393.html

Slaughter, M., & McCormick, D. (2021). Data is power. Washington needs to craft new rules for the digital age. *Foreign Affairs*, *100*(3), 54–63.

Snow, D., & Benford, R. (1988). Ideology, frame resonance, and participant mobilization. *International Social Movement Research*, *1*, 197–217.

Swidler, A. (1986). Culture in action: Symbols and strategies. *American Sociological Review*, *51*(2), 273–286. https://doi.org/10.2307/2095521

Tallberg, J. (2003). The agenda-shaping powers of the EU Council Presidency. *Journal of European Public Policy*, *10*(1), 1–19.

UNCTAD. (2019). *Digital Economy Report 2019*. United Nations. https://unctad.org/system/files/official-document/der2019_en.pdf

UN. (2018a). *Developments in the field of information and telecommunications in the context of international security* Resolution adopted by the General Assembly on 5 December. A/RES/73/27.

UN. (2018b). *Advancing responsible State behaviour in cyberspace in the context of international security* Resolution adopted by the General Assembly on 22 December. A/RES/73/266.

UN. (2019). *Countering the use of information and communications technologies for criminal purposes* Resolution adopted by the General Assembly on 27 December. A/RES/74/247.

UN. (2021a). *Compendium of statements in explanation of position on the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, *25*March. A/AC290/2021/INF/2.

UN. (2021b). *Remarks by Egypt at the Informal Meeting on the Zero Draft of the OEWG report*, 22 February. https://front.un-arm.org/wp-content/uploads/2021/02/Egypt-OEWG-Informals-of-18-Feb.pdf.

UN. (2021c). *Russia's remarks/comments on the OEWG Zero draft*, 22 February. https://front.un-arm.org/wp-content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-22.02.2021.pdf.

UN. (2021d). *General comments of the Islamic Republic of Iran at the Informal OEWG*, 18 February. https://front.un-arm.org/wp-content/uploads/2021/02/I.R.Iran-General-Comments-on-zero-draft.final_.pdf.

UN. (2021e). *China's Contribution on the Zero Draft of the OEWG Substantive Report*, 22 February. https://front.un-arm.org/wp-content/uploads/2021/02/Chinas-Contribution-on-the-Zero-Draft-of-the-OEWG-Substantive-Report.pdf.

UN. (2021f). *Chair's Summary. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* Conference Room Paper, 10 March. A/AC.290/2021/CRP.3.

UN. (2022). *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security,* 7 December. A/RES/77/37.

US Department of State. (2022). *Declaration for the Future of the Internet*. Available at: https://www.state.gov/declaration-for-the-future-of-the-internet.

US House of Representatives. (2012). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 8 October. https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

US Mission to the EU. (2020). *U.S. comments on the review of the General Data Protection Regulation (GDPR)*, 20 April. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Data-protection-report-on-the-General-Data-Protection-Regulation/F514088_en.

Voeten, E. (2021). *Ideology and International Institutions*. Princeton University Press.

White House. (2018). *National Cyber Strategy of the United States*. September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

WTO. (2019a). *United States. Joint Statement on Electronic Commerce*. WTO INF/ECOM/23. 26 April. https://docs.wto.org/dol2fe/Pages/FE_Search/ExportFile.aspx?id=252610&filename=q/INF/ECOM/5.pdf.

WTO. (2019b). *China. Joint Statement on Electronic Commerce*. WTO INF/ECOM/19. 24 April. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf.

WTO. (2019c). *European Union. Joint Statement on* Electronic CommerceINF/ECOM/22. 26 April. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=r:/INF/ECOM/22.pdf.

Xi, J. (2015). *Remarks by Xi Jinping, President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference*. Wuzhen, 16 December.