ELGAR INTERNATIONAL LAW AND TECHNOLOGY

Series Editors: Nicholas Tsagourias, Professor of International Law and Russell Buchan, Senior Lecturer in International Law, University of Sheffield, UK

Editorial Board: Duncan Hollis, Temple University, USA, Ashley Deeks, University of Virginia, USA, Marco Roscini, University of Westminster, UK, Zhixiong Huang, Wuhan University, China, Theodore Christakis, University of Grenoble, France, Karine Bannelier, University of Grenoble, France, Uti Korhonen, Turku University, Finland, and Rain Liivoja, University of Queensland, Australia

The aim of the series is to act as a platform to examine the implications of technology such as IT, cyber technology, autonomy, robotics, nano-technology, space technology, geo-engineering, sea-bed technology, and Artificial Intelligence on the practice and theory of international law and to address the challenges that arise. The development of technology and its use across different areas of human and state activity have raised questions about the scope, content, and reach of international law and of existing regulatory regimes as well as proposals for their reinterpretation and readjustment or for the development of new rules and regulatory regimes. This book series will capture the challenges and opportunities that arise from the intersection of technology with different areas of international law such as legal theory, human rights, humanitarian law, international criminal law, security, trade law, environmental law, international responsibility, dispute settlement and many more. It will also capture the challenges that arise when international law intersects with other legal regimes such as national law or regional law such as EU law in regulating technology. The aim of the series is to produce innovative, scholarly, and cross-disciplinary publications to inform scholars and practitioners and to promote knowledge.

For a full list of Edward Elgar published titles, including the titles in this series, visit our website at www.e-elgar.com
Building an International Cybersecurity Regime
Multistakeholder Diplomacy

Edited by
Ian Johnstone
Professor of International Law, The Fletcher School of Law and Diplomacy, Tufts University, USA
Arun Sukumar
Post-Doctoral Research Fellow, The Hague Program on International Cyber Security, Leiden University, the Netherlands
Joel Trachtman
Professor of International Law and Henry Braker Professor of Commercial Law, The Fletcher School of Law and Diplomacy, Tufts University, USA

ELGAR INTERNATIONAL LAW AND TECHNOLOGY

Cheltenham, UK • Northampton, MA, USA
Contents

List of contributors vii

PART I INTRODUCTION

1 Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects
   Ian Johnstone, Arun Sukumar and Joel Trachtman 2

PART II THEMATIC ISSUES

2 The geopolitics of multistakeholder cyber diplomacy: A comparative analysis
   Arun Sukumar 20

3 Multistakeholder characteristics of past and ongoing cybersecurity norms processes
   Josephine Wolff 59

4 Developing multistakeholder structures for cybersecurity norms: Learning from experience
   Joel Trachtman 85

5 Implementing cybersecurity norms: The design of international institutions
   Ian Johnstone 111

PART III COUNTRY PERSPECTIVES

6 U.S. multistakeholder engagement in cyber stability issues
   Christopher Painter 143

7 Russia’s participation in multistakeholder diplomacy for cybersecurity norms
   Andrey Shcherbovich 165

8 Rethinking Chinese multistakeholder governance of cybersecurity
   Jinhe Liu 185
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>India’s “passive” multistakeholder cyber diplomacy</td>
<td>Arindrajit Basu</td>
<td>201</td>
</tr>
<tr>
<td>10</td>
<td>Brazil and multistakeholder diplomacy for the Internet:</td>
<td>Carlos Affonso de Souza and Christian Perrone</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>Past achievements, current challenges and the road ahead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Taking stock of Estonia’s multistakeholder cyber diplomacy</td>
<td>Marina Kaljurand</td>
<td>238</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PART IV</td>
<td>CONCLUSION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>The way ahead for multistakeholder cyber diplomacy</td>
<td>Ian Johnstone, Arun Sukumar and Joel Trachtman</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contributors

Arindrajit Basu is Non-Resident Research Fellow at the Centre for Internet and Society, India.

Ian Johnstone is Professor of International Law at The Fletcher School of Law and Diplomacy, Tufts University.

Marina Kaljurand is an Estonian politician and Member of the European Parliament. She was previously the foreign minister of Estonia.

Jinhe Liu is Assistant Professor at the School of Journalism & Communication, Peking University.

Christopher Painter is President of the Global Forum on Cyber Expertise Foundation. He was previously the Coordinator for Cyber Issues at the US State Department.

Christian Perrone is Head of Rights and Technology and GovTech at Instituto de Tecnologia e Sociedade do Rio de Janeiro.

Andrey Shcherbovich is O’Brien/IIE-Scholar Rescue Fund Research Fellow at McGill University.

Carlos Affonso de Souza is Director of Instituto de Tecnologia e Sociedade do Rio de Janeiro and Professor of Law, Rio de Janeiro State University.

Arun Sukumar is a post-doctoral fellow at The Hague Program for International Cyber Security, Institute of Security and Global Affairs, Leiden University.

Joel Trachtman is Professor of International Law and Henry J. Braker Professor of Commercial Law at The Fletcher School of Law and Diplomacy, Tufts University.

Josephine Wolff is Associate Professor of cybersecurity policy at The Fletcher School of Law and Diplomacy, Tufts University.
PART I

Introduction
1. Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects

Ian Johnstone, Arun Sukumar and Joel Trachtman

In many areas of international life, governance is no longer the exclusive preserve of governments. As international affairs has encompassed subject matters with increasing technical and social complexity, it has been necessary to expand participation from pure state-to-state diplomacy to include more direct input, action and accountability from other actors: intergovernmental organizations, not-for-profit organizations, businesses, experts and transnational networks that encompass some or all of the above. This has long been the case for environmental law and policy and, increasingly, in the realm of global health.

The domain of cybersecurity is no different. Although governments lead in the regulation of cyberspace, the private sector owns and controls critical internet infrastructure, and much of the relevant expertise resides in the private sector. Non-governmental organizations, too, hold considerable technical and policy expertise and may act as checks on the approach and power of governments, and of private companies. Recognizing the important role of non-state actors in securing digital networks and infrastructure, intergovernmental forums have gradually opened the door for multistakeholder participation in the formulation, articulation and implementation of cyber norms. As a result, the secretariats of organizations such as the United Nations (UN), European Union (EU), International Telecommunications Union, Organization for Security and Cooperation in Europe (OSCE) and Shanghai Cooperation Organization have become active players in helping to steer cyber diplomacy and regime-building.

What is multistakeholder diplomacy? In many societies, the private sector, civil society actors, technical experts and interest groups participate in domestic policymaking arrangements. In such cases, the government represents their “stakes” abroad in its diplomatic efforts as that term is traditionally understood. What distinguishes multistakeholder diplomacy from traditional diplomacy is...
Building cybersecurity through multistakeholder diplomacy

the conscious structuring of mechanisms to establish input, action, or accountability from any or all non-governmental actors at the transnational level. In that sense multistakeholder diplomacy is a critical component of “transnational governance.”

More specifically, the difference between multistakeholder diplomacy and traditional diplomacy is threefold. First, the scope of issues addressed in international relations has grown significantly in the past 80 years. No longer is diplomacy confined to issues of war and peace. Instead, diplomacy now addresses every activity of the modern state, which itself is far more active than the state of 80 years ago, regulating and acting in many different spheres of life. Second, the formal mechanisms and institutions of diplomacy are no longer sufficient to manage the deeper and more pluralistic forms of cooperation that this new diplomacy requires. For example, the European Union, which has been grappling with this type of diplomacy at least since its 1989 Single Market program, has found that institutional adaptation is required to redress the “democracy deficit.” But there also have been criticisms in international governance of the unaccountable role of experts, of the excessive influence of the private sector, and of the opaqueness of their roles.

Third, multistakeholder diplomacy often produces or occurs within “regime complexes,” defined as “an array of partially overlapping and nonhierarchical institutions that includes more than one international agreement or authority.” The regimes in a “complex” address a common issue and may converge, but are often contradictory and lack an authoritative mechanism for resolving conflicts among them. Moreover, these regimes may operate at multiple levels of governance, adding another level of complexity. The multilevel regime complex for managing the entire range of transnational cyber activities includes international law on the use of force and human rights, as well as international and regional organizations that regulate telecommunications, intellectual property and trade regimes, industrial standards, and more. This volume focuses on a narrower set of cyber governance issues, namely cyber attacks that amount to the use of force and politically motivated cyber opera-
tions that fall short of war. However, platforms set up to address those issues may often discuss cyber operations or cyber norms that do not fall within the remit of this book.

Of course, national governments are often central to transnational governance, because of their regulatory power, and because of their presumptive authority. However, national governments may not always be necessary to or sufficient for transnational governance, because according to subsidiarity, in limited circumstances some combination of non-state actors may constitute the appropriate mechanism for such governance. To complicate this even further, the relevant government representatives may not be traditional “diplomats” perse – they could, and increasingly will, be representatives of parts of government beyond the ministry of foreign affairs.

There have been many examples of multistakeholder diplomacy. Article 71 of the United Nations Charter explicitly authorizes the UN Economic and Social Council (ECOSOC) to “make suitable arrangements for consultation with non-governmental organizations which are concerned with matters within its competence.” Other international organizations have formal mechanisms for consulting or working with non-state actors as well, including the EU, OSCE, World Bank and World Intellectual Property Organization. The International Labour Organization grants employee and employer organizations a vote. In the environment sphere, non-state actors have long been active players – either on the sidelines through non-governmental organization forums at global conferences, or more directly through institutions like the Intergovernmental Panel on Climate Change. Global health institutions have gone further. The board of Gavi (the Vaccine Alliance) is composed of governments, intergovernmental organizations, industry representatives, civil society representatives, a philanthropic organization (the Gates Foundation) and individuals with expertise in different aspects of vaccine delivery.

The cybersecurity realm has seen multiple processes for generating cyber norms, most of which have multistakeholder elements. In December 2019, the United Nations Open-Ended Working Group (OEWG), tasked with articulating cyber norms, hosted the “first ever UN multi-stakeholder meeting on addressing cyber threats in the context of international security.” Organized in the manner of an “informal, intersessional consultative session” with over 100
technology companies, research institutions, and civil society organizations, the OEWG’s meeting was not mandated by the UN General Assembly: it was held at the initiative of the Group’s Chair. In November 2021, the Chair of the second OEWG (2021–2025) suggested to states that it would be the “acceptable and prudent course of action […] to maintain the precedent” of the first Group with respect to multistakeholder participation.8

Outside the intergovernmental bodies, multistakeholder cyber diplomacy has thrived. Since 2017, no fewer than five global multistakeholder initiatives have been created to articulate and implement cyber norms. Some initiatives (elaborated on below), such as the Global Commission on the Stability of Cyberspace, Let’s Talk Cyber, and the Paris Call for Trust and Security in Cyberspace, have been co-sponsored by states. Others, such as the Cybersecurity Tech Accord and Community Talks on Cyber Diplomacy, are industry-led initiatives. The COVID-19 pandemic has, in fact, catalyzed greater activity within these initiatives, with some of them hosting four to five meetings a year. The virtual format of the meetings has elicited robust and more diverse stakeholder participation, with the result that multistakeholder diplomacy has become an integral part of discussions on what constitutes acceptable state and non-state behavior in cyberspace.

**DOES MULTISTAKEHOLDER CYBER DIPLOMACY MATTER? EVIDENCE FROM THE UN**

As noted previously, the 2019–2021 OEWG offered for the first time a multistakeholder platform at the UN to discuss matters of international cybersecurity. The evolution of multistakeholder cyber diplomacy during the term of the first UN OEWG, and its impact on the second (2021–2025) OEWG points to its growing influence. The 2019–2021 OEWG had limited avenues of participation in its substantive sessions for non-governmental organizations (NGOs). NGOs with “consultative status” at ECOSOC received OEWG accreditation, whereas requests from other NGOs – the vast majority of private actors interested in contributing to cybersecurity discussions at the UN did not have ECOSOC recognition – were considered by the OEWG states on a “no-objection basis.” Eighteen NGOs without ECOSOC consultative status applied for accreditation to the OEWG’s first substantive session in September

---

Building an international cybersecurity regime

2019, and the requests for all 18 were denied.9 Even upon accreditation, NGOs could only attend meetings “other than those designated closed,” and the extent of their participation was confined to permission to be “seated in the public gallery and [to] receive documents of the conference.”10

The OEWG’s first brush with multistakeholder diplomacy – the informal, intersessional meeting of December 2019 – while notable, did not appear to change fundamentally the participation of NGOs in this process. The applications of most NGOs without ECOSOC recognition who sought to attend the second substantive session of the OEWG in February 2020 – by one count, nearly 30 organizations11 – were once again rejected summarily. The onset of the pandemic soon after the second session meant intersessional meetings with NGOs scheduled for March and May 2020 had to be canceled. If rules of procedure of the OEWG already limited multistakeholder participation, NGOs were confronted with the possibility that virtual meetings would further restrict whatever informal opportunities they had to interact with negotiators, such as meeting them on the margins of closed sessions, or at conferences, regional consultations and seminars organized around the world in tandem with UN negotiations.

Such concerns did not come to pass, as the pandemic instead provided a major stimulant to multistakeholder cyber diplomacy. Beginning in late 2020, several NGOs independently organized virtual multistakeholder dialogues – some of which functioned as feeder discussions for concurrent OEWG and UN Group of Governmental Experts (UN GGE) negotiations – that drew in states as well as a significantly larger and more diverse group of private actors than the ones who had sought OEWG accreditation. Let’s Talk Cyber, an initiative led by the foreign ministries of Australia and Canada, alongside Microsoft, EU Cyber Direct, and the NGO Global Partners Digital, was perhaps the most consequential effort at multistakeholder diplomacy. Held over two days in December 2020, the sessions of Let’s Talk Cyber mirrored the six agenda items of the OEWG mandate and promoted robust discussions on some of

Building cybersecurity through multistakeholder diplomacy

the Group’s more contentious issues. Notable features of these interactive sessions included the presence of a “chat” facility that allowed participants to ask written questions, as well as real-time translation of the discussion into French, Spanish and Arabic. In a reflection of the genuine demand for inclusive and participatory discussions on international cybersecurity, Let’s Talk Cyber sessions attracted between 150 and 300 attendees for each session. The detailed reports submitted by the co-hosts of each session were finally included on the UN OEWG’s website and highlighted among reports of its formal and informal sessions – although there is no indication that the governments of Australia and Canada were formally tasked, as Singapore had been in relation to the December 2019 intersessional meeting, by the OEWG chair to engage in multistakeholder diplomacy on behalf of the Group.

During the same period, Russian cybersecurity company Kaspersky organized a series of discussions titled “Community Talks on Cyber Diplomacy.” Prominently featuring a number of technical experts, including Kaspersky’s own cybersecurity analysts, “Community Talks” was a multistakeholder dialogue that hosted cyber diplomats and OEWG/GGE negotiators from Germany, the UK, Australia, Switzerland, and Canada. Despite being organized by a Russian technology company, the topic of Russian cyber operations did not appear to be a taboo topic in these workshops, as participants freely discussed incidents such as the SolarWinds hack, and even appeared to make light-hearted comments about the belligerence of the lead Russian negotiator at the GGE and OEWG. Nevertheless, the Russian government did not participate in “Community Talks.”

If “Let’s Talk Cyber” and “Community Talks” opened the door for greater multistakeholder involvement in processes that articulated and interpreted cybersecurity norms, the virtual working groups of the Paris Call for Trust and Security in Cyberspace deepened further the private sector and civil society’s engagement with the UN meetings. Through a process driven by the French foreign ministry, six working groups were tasked with, *inter alia,* “supporting the UN negotiations with a strong, multistakeholder approach” and “engag-

---

15 Ibid.
ing emerging countries” through capacity building and information-sharing efforts.

The groups themselves were led entirely by private actors, which included Microsoft, Kaspersky, Schneider Electric, the University of Florence, the cybersecurity company F-Secure, and thinktanks like The Hague Centre for Strategic Studies.\textsuperscript{16} To be sure, some of these working groups sought specifically to attract more signatories to the Call, and advance interpretations of the eight Paris Call principles themselves. Yet the work of these groups was unquestionably influenced by developments at the UN GGE and OEWG. For example, Working Group 4, whose mandate was to clarify the scope of Paris Call principles, frequently alluded to UN norms during its discussions, and referred to them in its final report.\textsuperscript{17} The France-backed Programme of Action proposal for “regularized, institutional dialogue” at the UN was the subject of detailed deliberations in Working Group 3 – the French GGE Expert and cyber diplomat himself briefed the group on the modalities of the proposal – which ultimately called for “more robust and formal exchange with non-governmental stakeholders” by UN member states through the Programme of Action.\textsuperscript{18}

Many of the working groups met three to four times over the course of 2021 and submitted their final reports in November 2021. Their discussions routinely featured participation from UN negotiators, before and after the successful conclusion of the OEWG in early 2021, and the GGE later in the summer. With some groups hosting over 150 regular participants in each of its sessions, the Paris Call Working Groups created an environment for sustained multistakeholder cyber diplomacy at a critical moment in the UN negotiations.

Multistakeholder initiatives such as Let’s Talk Cyber, the Paris Call, and Community Talks on Cyber Diplomacy have arguably created an expectation not just of sustained interaction among private actors, but also that negotiators and cyber diplomats will engage those actors in good faith. Indeed, the


success of these initiatives appears to have generated louder calls for greater multistakeholder engagement at the UN. In November 2021, Burhan Gafoor, Singaporean diplomat and the Chair of the second OEWG, informed all delegations that he had “consulted widely with delegations” and “concluded that the most acceptable and prudent course of action [regarding multistakeholder participation] would be to maintain the precedent of the first OEWG.”

Within two weeks of his decision, Gafoor received an open letter from some states, international organizations, and non-state actors calling for “participation modalities” that allowed for “meaningful participation” of non-governmental stakeholders in the OEWG. This letter was signed by 44 states – mostly from Europe and North America – but also endorsed by over 100 civil society organizations and individuals, many of whom were from developing countries.

Notably, the letter sought a “transparent process” regarding states’ objections to the accreditation for NGOs which did not have consultative status with ECOSOC, as well as “channels” for NGOs to express their views even if they were denied accreditation. Additionally, the letter requested the Chair to make “sufficient time available” for NGOs to air their views in “formal and informal meetings,” and specifically recommended a “hybrid format” of participation for states as well as NGOs in light of the pandemic’s continuing uncertainties. The proposals reflected a “minimum level” of arrangements required to sustain effective multistakeholder cyber diplomacy, the letter concluded.

Just as remarkable as the proposals contained in the letter was the manner in which its promoters sought and consolidated support for them. Although the letter itself was transmitted by the governments of Australia and Canada to the OEWG Chair, the process of enlisting signatories was done through the Let’s Talk Cyber initiative. In fact, the open letter was sent out to prospective signatories “on behalf of the Let’s Talk Cyber initiative,” with a representative from Microsoft placed in charge of consolidating the final list of supporters.

This significant act of cyber diplomacy orchestrated by a multistakeholder collective resulted in protracted debate, and eventually, modest change, at the UN OEWG. With a number of states throwing their weight behind the open letter, and equally influential ones resisting any changes to the participation modalities of the OEWG, consensus in the group proved elusive. The first

---


Building an international cybersecurity regime

The substantive session of the 2021–2025 OEWG in December 2021 could not agree on the terms of NGO participation, and the second substantive session was held “informally” in March 2022 since organizational matters of the Group were yet to be resolved. The UK even tabled a resolution at the UN General Assembly to break the deadlock, calling on the UNGA to determine the rules of procedure if “no negotiated solution can be found.” Ultimately, the impasse ended in April 2022, when the Chair published the “agreed modalities” of participation in the second OEWG. The new terms confirmed that NGOs without ECOSOC accreditation would continue to participate on a “no-objection basis,” but called on states to “utilize the non-objection mechanism judiciously, bearing in mind the spirit of inclusivity.” States were required to “make known [their] objection to the Chair of the OEWG, and on a voluntary basis, […] the general nature of [their] objections.” Importantly, the updated modalities also empowered the Chair to “share any information [on objections] with member States” upon their request. The terms specifically highlighted that “negotiation and decision-making” within the OEWG was the exclusive prerogative of States.

While the second OEWG’s updated modalities of participation may seem incremental, they have influenced the application of the no-objection mechanism in a discernible way. The number of NGOs seeking accreditation from the OEWG went up significantly in 2021. If the substantive sessions of the first OEWG attracted approximately 30–40 accreditations from NGOs without ECOSOC consultative status, that number went up to 86 for the second OEWG. Whereas most NGOs without ECOSOC status were rejected in the first OEWG, only 32 accreditation requests were rejected in the second Group. Ukraine rejected the applications of five Russian stakeholders, including Kaspersky. Russia rejected requests from 27 NGOs, including from the US, UK, Australia and the EU. While neither country offered explanations, the prospect of public scrutiny of their objections probably contributed to states refraining from rejecting non-accredited NGOs’ participation altogether, as was the case with the first UN OEWG.

Incremental as the evolution of multistakeholder participation in the OEWG may have been, the diplomacy of private actors and states collaborating through the Let’s Talk Cyber initiative is symbolic and significant. It represents the culmination of nearly two years of multistakeholder initiatives coalescing and consolidating support for greater engagement between states and

25 Ibid.
private actors in norms articulation and implementation processes. Following the OEWG’s decision to ask states to formally disclose their objections to the accreditation process – the Group made it clear that the “modalities in no way created a precedent for any other UN process” – it will be difficult to put the multistakeholder genie back into the bottle. Non-governmental actors have not only got a taste of what it means to remain engaged with states but also an acknowledgment of their own collective bargaining power. They will want more, not less, concessions from states to open up intergovernmental processes involving cybersecurity regime creation. The OEWG experience is therefore a lesson that multistakeholder cyber diplomacy matters and requires rigorous study and analysis, which is the objective of this volume.

BUILDING A CYBER-SECURITY REGIME

This volume aims to deepen our understanding of how multistakeholder diplomacy can help contribute to building norms and institutions in the realm of cybersecurity. It emerged from a virtual symposium on multistakeholder cyber diplomacy held in June 2021 that drew participation from government representatives, prominent internet companies (including cybersecurity service providers), the technical standards community, and academia. Organized by the Centre for International Law and Governance at The Fletcher School, Tufts University, the three-day symposium sought for stakeholders to step back from the frenetic pace of engagements that has come to characterize cyber diplomacy to interrogate more substantially the role and future of private sector actors, NGOs and inter-governmental organizations in these discussions.

The symposium itself was held in the immediate aftermath of UN cybersecurity negotiations that had been ongoing for two years under the auspices of the GGE and OEWG. The symposium attracted diplomats who had been nominated by states to lead national delegations, as well as other individuals who participated in those delegations. These negotiators were at ease sharing their insights in a multistakeholder setting – albeit in a closed format that followed the Chatham House Rule – and “debriefed” other participants about key developments within the GGE. Officials at the symposium included not only those from the US and Europe, who are arguably more accustomed to dialogue with the private sector on cybersecurity norms, but also key “cyber powers” in Asia such as Israel, Singapore, Australia, and Japan, as well as regional powers India and Brazil. They interacted freely with non-governmental participants from China, Russia, Argentina, Brazil, Nigeria, and the US, among others.

As noted above, our focus is on cybersecurity issues narrowly defined, but to the extent that multistakeholder elements in other areas of cyber governance illuminate our understanding of cybersecurity diplomacy, they are addressed in some of the chapters. Our conception of norms encompasses the spectrum
from clearly binding legal obligations to clearly non-binding guides to behavior, with the understanding that the line between the two is blurred. Similarly, our conception of institutions ranges from formal intergovernmental organizations, to less formal groupings of states, to informal networks that have established a pattern of interaction.

We start from three propositions. First, states have diverging attitudes on the value of multistakeholderism. While a multistakeholder approach to cyber governance is the preferred model in parts of the Western world, China, Russia, and a number of other countries see the task as largely one for governments. Yet there is little question that the interests, power and knowledge that reside with non-state actors means they cannot be left out of cyber diplomacy altogether. The challenge for regime-building in this area, therefore, is to accommodate not only the differing authority, legitimacy, power, interests, capacity and expertise (the “stakes”) of the many actors but also differing governmental attitudes on whether and how each actor should be involved at all. Second, actors may combine stakes. For example, a leading technology company may have the general interests of its customers, its own special interests vis-à-vis competitors, substantial market power, and unique expertise. A central question this book addresses is how do different existing MSD structures respond to different constellations of stakes. Our third foundational proposition is that, whatever differences there may be about the actors, scope, and content relevant to a cyber-security regime, there is a general consensus that some international cooperation is needed. Cyberspace does not correspond readily to national geographic boundaries that, under international and domestic law, define the scope of state power. Purely national regulation will probably be incomplete or ineffective, without international cooperation. Similarly, a purely unilateral or bilateral approach to managing cyber-attacks will probably fall short of meeting the threat.

This book poses five central questions:

- How do major cyber powers view multistakeholder diplomacy, and how do their contrasting approaches influence the geopolitics of building a cyber-security regime?
- How can theories of compliance help identify the most promising institutional arrangements and mechanisms for implementing cyber norms?
- How can past cybersecurity-oriented multistakeholder initiatives illuminate the dynamics, constraints, and opportunities for creating institutions that identify and apply cyber norms?
- How can the workings of multistakeholder regimes and institutions in other domains inform the process of negotiating and designing a cybersecurity regime?
Building cybersecurity through multistakeholder diplomacy

• How do the approaches of major cyber powers and digital economies towards multistakeholder engagement on cybersecurity issues shape their diplomacy?

We begin with four thematic chapters, addressing respectively the first four questions listed above, followed by six country-specific chapters – focused on the US, China, Russia, India, Brazil, and Estonia – that answer the final question. These six countries represent influential cyber powers with the ability to influence material and normative outcomes in cybersecurity diplomacy, both regionally and globally. Representing also a balanced mix of advanced economies and emerging markets, the case studies examine how unique domestic considerations shape the cyber diplomacy of these respective states.

In the first thematic chapter, Chapter 2, Arun Sukumar provides an analysis of the geopolitics of multistakeholder cyber diplomacy (MCD), comparing the approaches of Russia, China, the US, France, and the European Union – toward multistakeholder cyber diplomacy. With private actors playing increasingly prominent roles in the articulation and implementation of cyber norms, states see strategic opportunities to instrumentally pursue MCD for their own goals. His comparative analysis reveals that Russia and China, states that have traditionally resisted private participation in cybersecurity regime creation, have begun to tolerate MCD initiatives selectively and even to orchestrate efforts of their own. On the other hand, the US, which has supported multistakeholder models of internet governance, has approached multistakeholderism in cybersecurity regime-building more cautiously, preferring intergovernmental forums. France and the EU see MCD as a buffer against great power capture of institutions that identify rules and norms on international cybersecurity. Even as they engage in MCD, states face a common dilemma: they must strike a balance between entrusting MCD initiatives to competent private actors and exerting control over the latter’s actions. Greater state control over non-governmental entities compromises their perceived independence and credibility, thus undermining the effectiveness of the MCD initiative.

In Chapter 3, Josephine Wolff considers past efforts to formulate cybersecurity norms and asks why they yielded limited progress when it comes to fostering international consensus around cybersecurity norms. Her chapter provides a brief overview of seven different processes that operated under different models for engaging stakeholders: (i) the United Nations Group of Governmental Experts, (ii) the Tallinn Manual, (iii) the Global Commission on the Stability of Cyberspace, (iv) the Organization for Security and Cooperation in Europe’s confidence-building measures for cyberspace, (v) the Cybersecurity Tech Accord, (vi) the Paris Call, and (vi) the UN Open-Ended Working Group. Wolff explores how each model attempted to incorporate some elements of multistakeholder diplomacy into their deliberations,
drawing insights into the potential benefits and perils of different models of engaging diverse stakeholders. She argues, on the one hand, the fact that no clear consensus around a single set of norms for cybersecurity has emerged as a result of all these processes and experimentation can be viewed as a failure of the processes. On the other hand, the very proliferation of these processes and the tremendous effort put into them can be seen as a success in terms of raising awareness about the importance of cyber norms, engaging different stakeholders, and developing alternative sets of potential norms. Ironically, these very successes may have hindered the actual development of a concrete set of norms – that the awareness of how important such norms are and the engagement of so many diverse stakeholders has made it more difficult to reach consensus.

In Chapter 4, Joel Trachtman asks whether models of multistakeholder diplomacy from other fields provide lessons that can guide negotiations in formulating MCD norms and institutions. He argues that each type of norm is formed and applied in a particular matrix of the power and interests of the various stakeholders. He defines power to include not only governmental authority and material capacity but also expertise and market power of private sector or NGO interests. It also includes the ability to confer legitimacy on rules or their implementation. Within that framework, he examines several examples of multistakeholder diplomacy. In areas such as product standards, vaccine distribution, and labor relations, norm-producing and implementation mechanisms have given non-state actors important seats at the table. In areas where a significant public interest is at stake, and may not be sufficiently protected by a national government “backstop” of legislation, such as in the food safety context, government continues to play a significant role. Cybersecurity is distinguished by the fact that this field is more greatly influenced by private sector power and expertise, and interests, and perhaps has greater effects on civil society interests, than other fields of security contention. The infrastructure of digital information and communications is largely created, maintained, and controlled by private persons in liberal democracies. Of course, this phenomenon varies across countries, because countries with more pervasive governmental involvement in the economy will have more pervasive governmental involvement in digital information and communications infrastructure.

Ian Johnstone’s chapter (Chapter 5) is about the implementation of cyber-security norms. He notes that, while there is still work to be done in pushing for wider adoption of existing norms and elaborating their content, attention is turning increasingly to norm implementation. His chapter examines the mechanisms, devices and institutional arrangements that exist or could be devised to induce or compel compliance with cyber norms – binding and non-binding. It begins with a brief review of theories of compliance with international law, focusing on what each suggests about alternative implementing
mechanisms that may be used to mete out rewards and penalties. Johnstone then outlines three broad considerations that necessarily underpin any attempt to build a cybersecurity regime: the distribution of power and ideological differences among governments; diverging capacity and interests among the many stakeholders; and the multiplicity of possible institutional forms a regime could take. The fourth section surveys the range of implementation devices that could be used within those institutional forms and identifies those that hold the most promise in moving forward on cybersecurity. A central thread of the chapter is that the line between implementing existing norms and formulating new norms in any field is blurred: practical experience in the implementation and application of norms contributes to their progressive development. Accordingly, this study of institutional arrangements, mechanisms and devices for cybersecurity norm implementation has as much to say about norm-making as it does about compliance.

The first country-specific chapter, Chapter 6 by Christopher Painter, is about the U.S. government’s approach to multistakeholder involvement in cyber stability issues. The US has a long history of championing multistakeholder involvement in a range of cyber and internet policy issues – particularly with respect to internet governance and technical cybersecurity. This approach is grounded in the realization that the private sector owns and operates the large majority of the internet and computer network infrastructure and that the private sector and civil society often have insight and capabilities that the government lacks. Although the US has been a leader in advancing an international stability framework globally, the acknowledgment of, and participation by, other stakeholders in that process has been less formal and more episodic than in larger cybersecurity or internet governance debates. A wide range of US-based stakeholders have a strong interest in, and have launched initiatives relating to, cyber norm and stability developments. Some of these stakeholders are global entities that seek to influence not just US positions but the global debate. Painter argues that, although there have been many informal interactions between these stakeholders and the U.S. government, more structured engagement can both better inform US positions and respond to stakeholder frustration that their input is too limited. He proposes creating a more formal model of stakeholder engagement, closer collaboration on norm implementation and capacity building, and working together to increase accountability for bad actors.

Andrey Shcherbovich in Chapter 7 examines Russia’s attitude towards and participation in multistakeholder cybersecurity diplomacy. He starts from the understanding that Russia tends to adhere to traditional approaches to diplomacy on all international political issues. While a multistakeholder approach to internet governance is the preferred model in Western countries, Russia takes a different approach, and governments retain a decisive role, especially
Building an international cybersecurity regime

In recent years, the principle of ensuring the security of the Russian Federation in the development and operation of information systems, as well as the protection of the information contained in them is increasingly a factor in the development of Russian legislation in the field of information management and internet governance. To a large extent, this can be attributed to the complex geopolitical situation against which Russian officials are increasingly seeking to assert “digital” or “information” sovereignty.

In Chapter 8, Jinhe Liu claims that the key to understanding China’s multistakeholder diplomacy on cybersecurity is to understand China’s domestic model of cybersecurity governance. Based on interviews with key people in the development of the internet in China, as well as important events and documents, his chapter analyzes the governance processes that led to the articulation of Chinese cybersecurity norms and considers how these have impacted China’s approach to multistakeholder cyber governance at the international level. The paper identifies that there are two historical periods in Chinese cybersecurity governance – a “pre-centralization period” and a “post-centralization period.” It also identifies four models of multistakeholder diplomacy: a government-led model, a private sector-led model, a technology community-led model, and a hybrid model. The multistakeholder approach in the pre-centralization stage was a Western style that was in line with international standards. After further integration with China’s local governance experience, a Chinese-style multistakeholder governance model gradually arose and is still evolving.

In his chapter on the multistakeholder “ecosystem” that has shaped India’s approach, Chapter 9, Arindrajit Basu starts with the observation that Indian diplomacy has always accorded a central role to the state in its approach to regime formulation, although multistakeholder influence has certainly shaped this engagement – including in the digital realm. However, with cybersecurity regime formation, all of the stakeholder groups have been quite passive. Because none has articulated a clearly defined interest in the regime, the government has remained largely non-committal in its approach to cyber norms processes. He describes this state of affairs as passive equilibrium – a multistakeholder diplomacy outcome where an absence of clearly defined “stakes” by stakeholders has resulted in an absence of scrutiny, accountability or influence on the government’s negotiating stances at cyber norms processes. Basu concludes with three recommendations to alter the state of passive equilibrium: better government communication about its positions to the other Indian stakeholders, more media scrutiny of government decisions, and more direct engagement with global processes by civil society groups.

In their chapter on Brazil, Chapter 10, Carlos Affonso de Souza and Christian Perrone argue that, domestically, the country has championed multistakeholderism from the outset, establishing an inclusive organization
to advance internet policy. The “Snowden Revelations” (which revealed that the US National Security Agency had monitored the communications of President Dilma Rousseff) prompted adoption of a similar approach internationally because the government felt compelled to propose a bolder approach to global internet governance, which was based on its own multistakeholder experience. This new approach culminated in the coordination and statement at the NETmundial Conference in 2014. Yet the Brazilian experience illustrates the challenges facing multistakeholder internet governance and cybersecurity diplomacy in terms of maintaining a delicate balance among the participating stakeholders. Domestic and international shifts in power, combined with swings in the perception of how the internet – particularly large technology companies – impacts the information ecosystem have led to a changed scenario for internet governance compared to what it was in 2014. The country study showcases how a multistakeholder regime for internet governance may translate into both an opportunity and a challenge for international cybersecurity.

Estonia has long been a leader in cybersecurity. Chapter 11 by former Estonian Foreign Minister Marina Kaljurand provides an insider’s account of how its multistakeholder approach evolved. Aided by progressive ICT policies, a proactive private sector, and a switched-on, tech-savvy population, Estonia can credibly claim to be one of the most connected digital economies and societies in the world. The adoption of digital platforms and services is part of a longstanding effort to forge a new method of participatory governance in the wake of Estonia’s independence from the Soviet Union in 1991. Because of the robust involvement of market actors, citizens, and NGOs in Estonia’s digital economy and society, it became necessary to develop multistakeholder mechanisms to facilitate their participation in matters pertaining to cybersecurity. The 2007 cyber attacks on Estonia’s critical infrastructure not only underlined the need for urgent multistakeholder cooperation on cybersecurity within the country but also with respect to external actors. As a result, Estonia crafted unique legal and policy instruments to support and regulate domestic public–private partnerships in cybersecurity, while engaging actively in and promoting multistakeholder cyber diplomacy globally.

As noted at the start of this Introduction, the influence of non-state and sub-state actors on multilateral diplomacy is not new. What is new is the push for more formal and systematic inclusion of these actors in multilateral norm-making processes and the implementation arrangements that come out of them. That push is felt strongly in the realm of cybersecurity, precisely because stakeholders other than states possess a great deal of expertise, power, and legitimacy, as well as interests in how the field is governed. Yet the phenomenon is not unique to cyberspace – we see it playing out in different ways in the environment domain, public health, and even in areas long thought to be the exclusive preserve of national governments such as the proliferation of...
weapons of mass destruction. Thus, in exploring the opportunities, challenges and risks associated with multistakeholder initiatives to build a cybersecurity regime, this book hopes to shed light on multistakeholder diplomacy and governance more generally.
PART II

Thematic issues
INTRODUCTION

On November 6, 2018, Microsoft Corporation convened a gathering of lawyers, diplomats, research scholars, and technical experts at the Peace Palace in The Hague. The event, titled “An Evening on Digital Peace,” was itself an exercise in multistakeholder cyber diplomacy (MCD): it was organized jointly by Microsoft, the City of Den Haag, and the Institute for Accountability in the Digital Age, a not-for-profit think-tank. The choice of venue for this event was interesting. The Peace Palace hosts the International Court of Justice (ICJ), the world’s premier judicial body for the settlement of international disputes and authoritative interpreter of public international law. The Statute of the ICJ makes it clear that non-state actors can neither be parties to, nor intervene in, a dispute before the Court. There is also no scope for non-governmental entities to act as witnesses, file independent briefs, or serve as amicus curiae in a dispute, except upon invitation from the Court, or through the state parties themselves. The discretionary powers conferred on the Court to facilitate the participation of non-state actors as experts or witnesses have been seldom invoked.
Microsoft’s selecting the Peace Palace as the venue for the event – Brad Smith, the company’s president and Chief Legal Officer, delivered the keynote speech in the Great Hall of Justice, where the ICJ hears cases – may therefore appear as an act of insurgency, signaling the company’s desire to be treated like, if not at par, with states. This perception is reinforced by Microsoft’s call in 2017 for a “Digital Geneva Convention” that reaffirms the status of the “tech sector” as a “neutral Digital Switzerland” (emphasis added in both instances). Microsoft also announced a “Cybersecurity Tech Accord” (CTA) in 2018, that elicited a pledge from technology companies to protect their users and customers from cyber attacks, irrespective of the “criminal or geopolitical” motive of the attacker. At the time of writing, over 100 companies have “adopted” the CTA. The import of such terms and phrases, and their characterization as akin to legal and political instruments signed by states, is unlikely to have been lost on Microsoft. Not only is Brad Smith, the architect of the company’s diplomatic initiatives, trained in international law, but he has also addressed professional associations such as the American Society of International Law. Nevertheless, in his Peace Palace speech, Smith indicated a more plausible reason for Microsoft’s choice of venue. “We need governments to adopt principles […] and ultimately, to do what has always been done in this very building,” he said, “and that is: move norms and international law forward.” From this formulation, it would appear that Microsoft was relying on spatial, historic, and semantic tools to articulate the state-centricity of the problem of cyber governance. The event itself was held close to the centenary date of the World War I armistice, which Smith’s speech frequently alluded to. Microsoft’s invoking a historic failure of intergovernmental diplomacy to foreground the urgency of rules for cyberspace is ultimately an acknowledgment that multistakeholder initiatives have to be mindful of the geopolitics of this domain.

If the governance of cyberspace is no less susceptible than other aspects of international relations to this competitive dynamic between states, what is the role of non-state actors, and specifically, of MCD in crafting rules for the domain? Do MCD initiatives mirror the same geopolitical fault lines that characterize intergovernmental cyber negotiations? If so, are non-state actors simply proxies, and MCD initiatives a vehicle for states to legitimize

---

their own diplomacy and weaken that of their competitors? If not, do MCD initiatives enable non-state actors who are excluded from closed, intergovernmental negotiations to advance those issues and concerns that are inadequately addressed through traditional diplomacy?

The answers to these questions will probably depend on the specific attributes of an MCD initiative, such as its composition, the issues it seeks to address and its deliberative procedures, as well as the capability of its promoters to exert material and ideational influence over other actors in the domain of cybersecurity. Nevertheless, with the rapid proliferation of multistakeholder initiatives in recent years, it has become important to address these questions to better understand the relationship between state and non-state actors in MCD. Between June 2017, when the fifth United Nations Group of Governmental Experts (GGE) on cybersecurity dissolved without a “consensus report,” and June 2021, when the sixth GGE successfully concluded its discussions, no less than four prominent MCD initiatives were incubated by private corporations and not-for-profit think-tanks. In at least one instance, the precise formulation of a cyber norm adopted by an MCD initiative has found its way to the sixth UN GGE report, albeit as an “additional layer of understanding” to its own norms. These developments indicate MCD initiatives are not only outpacing multilateral diplomacy but also bear the potential to frame the substantive agenda for the latter.

This chapter traces the evolving positions of Russia, China, the US, France, and the European Union (EU) toward multistakeholder cyber diplomacy. Specifically, it examines geopolitical considerations that have led each of these major cyber powers to embrace or reject MCD. As with other chapters in this volume, it examines those MCD initiatives relating to the stability of the domain, i.e. relating to cybersecurity threats and concerns of high severity and sophistication that rise above the level of ordinary criminal activity. The comparative analysis reveals that states increasingly perceive MCD initiatives as strategic tools. Even as non-state actors – private corporations, civil

---

7 They include the Global Commission on the Stability of Cyberspace (2017–2019); Paris Call for Trust and Security in Cyberspace (2018), Let’s Talk Cyber (2020–ongoing), the Charter of Trust (an initiative developed by Siemens in 2018), and Cybersecurity Tech Accord (2018–). For a comprehensive overview of MCD initiatives see Josephine Wolff (2021), Chapter 3 in this volume.

society organizations, the technical community, and academia – seek greater participation and transparency in the creation of cyber stability regimes, states have taken an instrumentalist view of multistakeholder diplomacy, carefully evaluating how it aligns with their pursuit of national and global interests. The chapter argues that Russia and China, which have traditionally been reluctant to support the participation of non-state actors in regime creation, have begun, albeit selectively, to engage in MCD. On the other hand, the US, which has sought greater multistakeholder participation in internet governance, appears less enthusiastic about the involvement of private actors in the creation of rules for cyberspace. France, this paper argues, has championed MCD as a wedge against US–Russia Great Power competition in cyberspace, leveraging multistakeholder diplomacy to strengthen its “strategic autonomy.” Finally, it analyses the EU’s Cyber Diplomacy Toolbox, noting that it may promote a supranational multistakeholder regime that renders private actors essential interlocutors in the creation and implementation of cyber sanctions. The second section draws on theoretical insights from the international relations/international law literature to frame the relationship between states and non-state actors in MCD. The third section presents the approaches of the five major powers toward MCD. The final section presents the paper’s conclusions.

MULTISTAKEHOLDER DIPLOMACY: OPPORTUNITIES AND LIMITATIONS FOR STATES

Global governance regimes have in recent years flattened the relationship between state and non-state actors by allowing the latter “to claim more direct routes to global governance,” either through “direct relations to intergovernmental organizations or multi-actor forms of governance in which states are not the dominant actors.”9 “Multistakeholder governance in international law remains rare,” argues Raustiala, “but it appears to be on the rise.”10 Roger and Dauvergne identify three major factors that have contributed to the rise of

---


“transnational rules,” or rules in whose “emergence, selection, and adoption” non-state actors play a crucial role:

1. greater cross-border mobility of capital and goods, which creates opportunities for market actors for “exit” and “voice,” and simultaneously reduce the ability of states to intervene in markets;
2. increased capacity of non-state actors for “cross-border organization”; and
3. a shift in the “global ideational superstructure” for ideas that support private-led modes of governance.

These factors have certainly played an important role in strengthening multi-stakeholder participation in cybersecurity regimes. Market actors (Microsoft, Kaspersky, FireEye, CrowdStrike, etc.), civil society organizations (Access Now, CyberPeace Institute, Women’s International League for Peace and Freedom, etc.), the technical community (Internet Engineering Task Force, Internet Society, Réseaux IP Européens Network Coordination Centre, etc.), and academia (Harvard Belfer Center, Lomonosov Moscow State University, China Institute of Contemporary International Relations, etc.) are today essential interlocutors in cyber stability discussions, whether in norm articulation or in implementation. Concerned as this chapter is with the geopolitics of MCD, the question remains how these factors have “changed the calculus of interstate cooperation.” In other words, given contemporary political and economic realities, when do states decide to promote, engage, or resist participation in multistakeholder initiatives?

Abbott et al argue that states face a “governor’s dilemma” between “preferring to work with competent intermediaries” and compromising control over those intermediaries so they are able to effectively “mobilize [said] competencies.” The “broader and more ambitious” the state’s goal with respect to regime formation or implementation, the more likely it will be to choose

---


13 Roger and Dauvergne, 433.

a powerful and competent intermediary to achieve its goals. However, powerful intermediaries, whether they take the form of multinational corporations or civil society organizations, are often independent, which may result in the governor losing control over the project of regime creation. In other cases, the perceived independence of the intermediary may be essential to the regime’s credibility. If the state ratchets up control over the intermediary, it may therefore come at the cost of its competence, understood broadly to mean the latter’s ability to galvanize support for the regime in question.

Faced with this dilemma, states may choose between two options: create or promote “low-cost” multistakeholder initiatives that establish “common norms, rules, objectives, and decision-making and implementation procedures” for the prospective regime, or engage in “intermediary orchestration” through an international or regional organization. Low-cost initiatives not only offer flexibility for states to “operate and change” their procedures, but also lower specifically the “sovereignty and exit costs” that are associated with treaty-centric arrangements. In the latter case, the IG/RO is delegated by the state to “enlist and support” private intermediaries that pursue the same goals. Both options present a different set of challenges. The lack of binding obligations makes compliance with low-cost multistakeholder initiatives difficult, whereas in the case of orchestration, the intermediary is susceptible to being manipulated by any state that shares membership in the international/regional organization.

States may also participate in, or promote MCD initiatives, with a view to creating a “Community of Practice” (CoP) around key aspects of the regime. A CoP is a collective of individuals and institutions with a joint identity, who seek to “develop, share, and maintain” knowledge that in turn lays the “normative and epistemic ground for action” in the future. Stakeholders in a CoP do not necessarily agree with each other. CoPs differ from epistemic communities in that they do not share “causal beliefs” about a policy problem.

---

19 Abbott and Faude (2021), 399.
and its prescriptive solutions. Indeed, the only defining feature of a CoP is the routine and meaningful interactions of its members around a common, mutually understood purpose. To states, the utility of a CoP lies in the fact that it helps develop intersubjective understandings about key issues in a regime, especially those issues that may be difficult to develop or even broach through closed, intergovernmental diplomacy. Understandings developed by the CoP subsequently find their way into those closed settings, with states citing their articulations as authoritative treatments of the issue. Alternatively, the CoP’s pronouncements, especially in reference to rules or legal norms, become tools of “lawfare” used to defend state practice. The effectiveness of a CoP depends on its perceived credibility, which may be a factor of its ability to bring in powerful interlocutors, the transparent nature of its discussions, or in other cases, its representative character. Although a state may “endow” the CoP with an institutional framework, there are no spatial or organizational limits to the community. Its members may meet not only through the said state-sponsored forum, but also on the sidelines of conferences, bilateral discussions, professional networks, and so on. Given the loosely held and semi-formal character of this collective, states may find it difficult to steer the CoP’s discussions. If a state sponsor attempts to restrict entry into the CoP or tries to control its agenda, such measures may have the effect of compromising the community’s independence.

States have a particular incentive to incubate CoPs around norm implementation by sponsoring multistakeholder initiatives for capacity building or implementing confidence-building measures (CBMs). These initiatives become nuclei for the CoP, serving not only as institutional repositories of knowledge and practical measures that are adapted across regions but also helping induce compliance from state and non-state actors through rewards and penalties. On the positive side of the ledger, incentives in the domain of cybersecurity may take the form of offers of technical assistance, reputational gains, or enhanced access to intelligence information. As for penalties, multistakeholder initiatives may not all have the ability to directly impose sanctions.

---

22 Adler describes CoPs as comprising three concentric circles: an inner circle that articulates norms or confidence-building measures; an intermediate circle of people who are “experts or normatively committed” to the norms, who help diffuse them; and an outer circle of states or regional organizations that adopt those norms or practices. Emanuel Adler, Communitarian International Relations: The Epistemic Foundations of International Relations, 25 (Routledge, 2005).
23 Etienne Wenger, Communities of Practice: Learning, Meaning, and Identity, 74. (Cambridge University Press, 1999).
24 For a survey of measures to induce norm compliance, see Ian Johnstone (2021), Chapter 5 in this volume.
but can nevertheless engage in “naming and shaming” states and non-state actors that do not adequately implement norms.

States may also delegate powers of regime monitoring and compliance to supranational entities, whose functioning relies partly or wholly on multistakeholder participation. These entities differ from international organizations in that they resemble executive bodies performing administrative actions. Although decision-making in such entities may ultimately be the prerogative of states – particularly those tasked with surveillance and sanctions – the agencies that facilitate such decision-making may be of a “hybrid” nature, with multistakeholder participation. In the cybersecurity domain, several such issues lend themselves to multistakeholder involvement in a supranational entity, including issues of attribution of cyberattacks, maintenance of supply chain integrity, and vulnerabilities disclosures.

Finally, states may also promote multistakeholder diplomacy to create “sham standards,” i.e. a “notional set of global standards with weak or non-existent monitoring or enforcement schemes.” Drezner argues that sham standards ease the pressure on states (from domestic constituencies) to show evidence of global coordination while preserving the room for unilateral action. Multistakeholder diplomacy could offer a façade of legitimacy for such standards. Sham standards are more likely in the event of Great Power conflict over regime creation.

MCD INITIATIVES: WHERE DO MAJOR POWERS STAND?

Russia: A Strategic Turn Towards MCD?

Russia’s opposition toward multistakeholder internet governance is well documented, and follows from the view that key entities responsible for articulating policies or technical standards for the internet are based in the US. The Russian position is that entities like the Internet Corporation for Assigned

27 Kingsbury et al (2005), 22.
29 Drezner (2007), 87.
Names and Numbers (ICANN), Internet Engineering Task Force (IETF), and Internet Society (ISOC) “cannot be classified as international intergovernmental organizations, and [are] therefore not a subject of international law.” In 2012, at the International Telecommunications Union’s World Conference on Information Technology (WCIT-12), Russia introduced, rallied support for, and subsequently withdrew a proposal to bring internet governance strictly within the ambit of the United Nations. The Russian proposal, the response and refusal of the U.S. government to sign the WCIT treaty, and the ensuing political controversy, can be considered to be among the early frames of reference for the “multilateral v. multistakeholder” typology that emerged in internet governance analyses. According to former Russian official and influential analyst of cybersecurity Anatoly A. Streltsov, multistakeholder governance models have led to a lack of “[actors] in the system of international relations that would bear international responsibility for ensuring the stability of global cyberspace.”

Its strident view on multistakeholder internet governance notwithstanding, Russia has engaged in MCD initiatives for several years. The most prominent of these initiatives is the decade-long multistakeholder gathering on cybersecurity, sponsored by Russia, at Garmisch-Partenkirchen in Germany. The initiative, titled the “Forum on the Partnership between State, Civil Society and Business in the Field of International Information Security,” was first convened in 2007, and has since met annually without interruption. The Garmisch Forum, structured partly as a Track 1.5 dialogue, is organized jointly by the Lomonosov Moscow State University and the Security Council for the Russian Federation (RuSC), the country’s top policymaking body on national security issues. Attendees include members of the International Information Security Research Consortium (IISRC), a multistakeholder entity that was itself created at the 2010 Garmisch Forum, and which has since grown in scope and participation. The IISRC comprises academics, civil society institutions, government agencies, and prominent businesses from the US, Russia, the UK,

---

India, China, Japan, Israel, and ten other countries. The Garmisch Forum has also witnessed participation from regional international organizations like the Organization for Security and Cooperation in Europe, as well as non-governmental organizations (NGOs) like ICANN.

In recent years, Russia’s MCD initiatives have witnessed a high degree of consolidation. Whereas the Garmisch Forum previously used to be run by an ad hoc committee, it is now organized by the National Association for International Information Security (NAIIS). The NAIIS was set up in 2018 and is registered as a non-commercial organization under Russian law. The Presidium of NAIIS includes not only representatives from Moscow State University and RuSC, but also prominent Russian companies, as well as the editor of the country’s prestigious journal *International Affairs*. The Charter of NAIIS expressly recognizes the Association’s role in MCD. NAIIS lists among its objectives the following:

1. Promoting the formation of a system for ensuring the sustainable functioning of global and national information infrastructures;
2. Making proposals to Russian and foreign state authorities, non-governmental organizations, and international organizations to facilitate the implementation of state policy in the field of the international information security;
3. Participation in Russian delegations to international organizations (UN, Organization for Security and Cooperation in Europe, Shanghai Cooperation Organization, Commonwealth of Independent States, Collective Security Treaty Organization, BRICS (Brazil, Russia, India, China, and South Africa), Asia Pacific Economic Cooperation, G20, and others), as well as bilateral, multilateral and regional consultations on information security rules.

It would not be strictly accurate to categorize certain key stakeholders involved in the NAIIS and Russia’s MCD initiatives as non-state actors. The Lomonosov Moscow State University is a public research institution, and the two main architects of Russia’s MCD initiatives, Anatoly Streltsov and

---

33 The Consortium also hosts its own, independent conferences: http://www.iisi.msu.ru/Main(eng)/isirc2014-2-infmess1/.
Vladislav Sherstyuk, were formerly officials in the country’s military and intelligence services. Other members of the NAIIS presidium, including its business representatives, have also had long careers in the Russian government. Still, there is little doubt the Garmisch Forum is genuinely multistakeholder in character, attracting participation from major technology companies, renowned technical experts, academics, and even high-level government functionaries. In 2020, on account of the Covid-19 pandemic, the Garmisch Forum moved to Moscow, providing the NAIIS an opportunity to showcase its multistakeholder credentials. It remains to be seen whether future editions of the Forum will continue to be held in Moscow.

Russia’s MCD initiatives recently received a significant endorsement from President Vladimir Putin, who addressed the topic at length in his remarks to RuSC in March 2021. In a meeting to review Russia’s position on international information security, Putin supported “the creation and strengthening of new international discussion venues both in Russia and abroad [to promote Russia’s position].” “This is a very solid resource that has yet to reach its full potential,” Putin declared, calling for “more active use of the opportunities of scientific and expert circles and the business community, including, surely, the NAIIS.”

What explains the heightened attention paid by prominent Russian state and non-state actors to MCD initiatives? In the past, Russia has left open the door for the “possibilities” of a “multistakeholder approach” to tackling international information security but conditioned it on the “reform” of multistakeholder governance. Writing in Russia’s International Affairs, Andrei Krutskikh – Russia’s top cyber diplomat and GGE “Expert” for more than a decade – and Streltsov cautioned against digital capacity-building measures that could be “turned into a tool and disguise for interfering in the internal

affairs of developing countries.” Their argument was premised on the control of critical internet resources by private actors in the West. Internet governance models have not changed fundamentally, but the Russian position on MCD appears to be incrementally changing. What explains this outcome?

A plausible explanation is that Russia acknowledges the importance of MCD with respect to two international projects in which it is significantly invested: the UN Open-Ended Working Group (OEWG), and the country’s own hosting of the Internet governance Forum in 2025. The OEWG was conceived as a Russian initiative that would – in Moscow’s formulation – “internationalize” and “democratize” the discussion on rules and norms for cyberspace by opening it up to all UN member states, in contrast to the GGE, which is confined to a select number of state-nominated “Experts” working under the auspices of the UN First Committee on Disarmament and International Security. In political terms, Russia perceives the OEWG as a potent counterweight to the GGE, where it is outnumbered by the US and its allies. Indeed, the OEWG’s publication of a final report, subsequently adopted by the UN General Assembly, was articulated as a “triumphant success of diplomacy” by Russia. As the OEWG’s work advanced, however, Russia has had to make a number of concessions regarding the participation of non-state actors in this process. In December 2019, the OEWG organized an informal, intersessional meeting in a multistakeholder format: chaired by Singapore, this meeting was the first multistakeholder meeting on cyber norms held under the aegis of the UN. The substantive sessions of the OEWG, too, were opened to

---

attendance for NGOs (after a screening process), including those who did not receive UN ECOSOC accreditation. This was a departure from the traditional method of involving non-governmental entities as observers or participants in UN inter-governmental meetings. The chair of the OEWG, Jürg Lauber of Switzerland, and other representatives from the Group, also participated in a number of informal multistakeholder sessions, whose proceedings have been documented on record. Even substantive sessions of the OEWG elicited multistakeholder participation, by way of briefings by non-governmental experts to the Group. As a result of opening its participation to non-governmental entities, the OEWG also received written inputs from a number of stakeholders on the pre-draft, Zero Draft, and First Draft on the Group’s report. The perceived legitimacy of the OEWG’s deliberations and final report was thus enhanced by the participation of non-governmental stakeholders, although a number of such organizations expressed their dissatisfaction with the outcome.

For these reasons, it would be difficult for Russia to limit multistakeholder participation in future OEWGs, as the Group’s credibility is now intrinsically linked to the openness of its negotiations. In December 2020, the UN General Assembly established a new OEWG for five years (2021–2025), leaving the Group to determine its own “organizational arrangements” but stressing the importance of interactions with “NGOs, businesses, and academia.”
Additionally, the 2019–2021 OEWG’s report takes special cognizance of the proposed “Programme of Action” initiative, an effort led by France, Egypt, and 40 other countries, to bring cyber norms discussions under a permanent, institutionalized, and regular dialogue. The PoA is an effort to “end the dual track discussions” of the GGE and OEWG that can be “counter-productive” and “create redundancies,” and explicitly calls for multistakeholder participation in its proposed dialogue framework.49 If future OEWGs are closed to multistakeholder participation, the PoA proposal could gather momentum and support, putting Russia’s prestige project at a disadvantage. Therefore, Russia is likely to support OEWG-centric MCD initiatives, with a view to using non-state actors as a tool to legitimize the Group’s conclusions. Indeed, Krutskikh and Streltsov argue that “it seems important to actively support the expert community, interested commercial organizations and civil society organizations [to] implement the identified priorities of the work of the Open-Ended Working Group.” They highlight the role of the NAIIS as a focal entity that could “cooperate with foreign expert organizations to contribute to the successful work of the OEWG.”50

The UN’s decision to award the 2025 Internet governance Forum (IGF) to Russia will also play an important role in the latter’s approach toward MCD initiatives. IGF, the world’s premier multistakeholder gathering on internet-related issues, does not articulate cyber norms or rules – however, a number of MCD initiatives leverage the IGF’s visibility to propose their own panel discussions, workshops or roundtables at the event. IGF 2025 will be notable for two reasons. In 2025, the present term of the IGF expires, requiring a fresh mandate from the UN General Assembly. The IGF that year will therefore be crucial to determining the terms of reference and substantive dialogue for the Forum’s new mandate (if it is renewed). Russia may hope to steer those terms before they are finalized at the UNGA, for which its own championship of MCD initiatives is essential. Second, the 2025 IGF would be hosted by Russia after an extended period of circulation in Western Europe, making this a prestige project for the government in Moscow. That its hosting of the IGF is


being taken very seriously by Russia is already clear from official statements. To lay the groundwork for a successful IGF, the state requires the support of non-state entities in business, technical communities, civil society and academia. The NAIIS will likely be an important player in bringing together those actors relevant to global cybersecurity considerations, and could thus emerge as a prominent force in the lead-up to the Forum.

Based on the evidence offered in this segment, it would be reasonable to conclude that Russia sees the benefit of MCD initiatives as a strategic tool to enhance its reputation and engineer favorable outcomes in intergovernmental negotiations. The establishment and rapid rise to prominence of the NAIIS is perhaps an acknowledgment by Russia’s top policymaking bodies that MCD initiatives are not epiphenomenal, and could decisively frame the parameters of debate, especially around norms and international law applicable to cyberspace. In 2018, Russia refused to sign the Paris Call, declaring the “multistakeholder approach to digital space proposed by France provides for putting States and non-State actors on an equal footing, and thus dilutes the key role of States in ensuring cybersecurity.”\(^{51}\) Yet, even as it continues to highlight the “artificially exaggerated”\(^ {52}\) importance of the multistakeholder approach in formal negotiations, Russia may therefore pursue in parallel, MCD initiatives where it can exercise levers of control over deliberations and outcomes.

**China: A “Render Unto” Approach to MCD**

Although the state-centric positions of Russia and China on the governance of cyberspace are often clubbed together in topical analyses, the latter has a perceptibly different approach toward multistakeholder internet governance and MCD initiatives. A crucial point of divergence is the treatment of “information sovereignty” and “cyber sovereignty” by Russia and China, respectively – this distinction is relevant to understanding China’s view of MCD initiatives. The Doctrine of Information Security of the Russian Federation, amended most recently in 2016, conceptualizes an “information sphere,” the protection of

---


whose “sovereignty” is among its paramount objectives. The “information sphere,” according to the Doctrine, includes a “combination of information, informatization objects, information systems and websites.”53 Digital networks and infrastructure are included within the ambit of this definition, but Russian security strategy and diplomacy emphasizes their “informatization,” referring to the qualitative uses to which infrastructure is deployed. Analysts have argued that this formulation obtains from the traditional focus of Russia on the potential weaponization of information and its implications for regime stability.54 In contrast, China’s conception of “cyber sovereignty” takes a more subject-oriented approach, seeking comprehensive control over internet infrastructure and activities within its territory,55 and increasingly, abroad.56 In other words, the Chinese approach inverts the Russian notion.57 To be sure, the Chinese state tightly controls the flow of information to and from the country’s borders, but there is less evidence to indicate that Beijing sees information as a strategic asset, as much as a tool to preserve political stability. The focus of “cyber sovereignty” is primarily on the “network physical facility,” i.e. digital infrastructure, first, and secondarily, on the “cyberspace formed on [those] facilities.”58

Fang Binxing has identified four essential attributes of cyber sovereignty. They comprise:\textsuperscript{59}

1. the right to independence, i.e. the ability of a country’s networks to operate “without being subject to the power of other countries”;
2. the right to equality, i.e. the right to “equal management of network systems” and to fair rules for “interconnection between networks”;
3. the right to self-defense, i.e. the ability of a state to defend its own networks; and
4. the “power to manage […] national network systems.”

Fang interestingly analogizes a state’s jurisdiction over its networks and data to a riverbed and river water, respectively. “If the upstream country exports the polluted river water,” he argues, “the importing country should have the ability to clean up, and have corresponding countermeasures to the exporting country that does not intend to clean itself.” This view, however, does not appear to reflect the Chinese position at cyber norms negotiations.

Consequent to this formulation of “cyber sovereignty,” China appreciates the necessity of engaging multistakeholder internet governance, with a view to articulating favorable proposals concerning the transit and storage of data. China’s reconciliation with the “multistakeholder approach” is an acknowledgment that cyber sovereignty can only be realized if the government maintains working relations with key internet governance and standard-setting institutions. Nodal state agencies such as the Cyberspace Administration of China (CAC) have long been active participants in ICANN meetings and ISOC gatherings.\textsuperscript{60} The former CAC chief, Lu Wei, and the founder of Chinese technology giant Alibaba, Jack Ma, were both on the steering committee of NetMundial, a multistakeholder internet governance forum organized by Brazil in 2015. At the 2018 National Cybersecurity and Informatization Work Conference, President Xi Jinping suggested “international cyberspace governance should persist in multilateral participation and multi-stakeholder participation.”\textsuperscript{61}

China purportedly sees no conflict between the “multilateral” and “multistakeholder” models of internet governance. Even as it engages multistake-
holder forums, China is deeply invested in intergovernmental organizations such as the International Telecommunications Union, having expended considerable diplomatic capital to ensure the selection in 2014 of Houlin Zhao, a Chinese national, as the ITU’s Secretary General. The Chinese telecommunications company Huawei recently submitted its proposal for “New IP” to the ITU, as an upgrade to the existing global internet protocol system. The New IP proposal is in line with China’s efforts to actualize “cyber sovereignty.” Although it is difficult to discern the precise impact of “New IP” given its current status as a high-level policy proposal, at least some security-related elements of the proposal are likely to enhance the control of network operators (and in heavily regulated jurisdictions, that of the state) over data flows. The proposal has invited criticism from multistakeholder institutions like the IETF for its “top-down design,” but Huawei has also courted the IETF, playing host to its first virtual meeting in March 2020.

The “engage-all” approach that underpins China’s multistakeholder internet governance strategy appears thus to be borne by practical considerations, even as it works to strengthen the capacity of states to govern digital infrastructure. Cai Cuihong argues China’s emphasis on multilateralism in internet governance is not in contradistinction to “multistakeholderism,” but a call to avoid “unilateral” actions—a euphemism usually for US policies. Recognizing its engagement with multistakeholder internet governance institutions is equally important to avoiding unilateral actions (on account of policies championed by the U.S. government or US companies in those institutions); China has therefore sustained its participation in them.

However, does this same view also inform China’s approach to MCD initiatives? In 2013, China submitted before the UN First Committee that states have a role to play in “stimulating” multistakeholder initiatives domestically,

---

Building an international cybersecurity regime

and therefore should assume a “leading role” in cyber diplomacy. With respect to the 2019–2021 OEWG, there is both written and oral evidence indicating China’s reluctance to support enhanced multistakeholder participation. Addressing references to multistakeholder participation in the “pre-draft” of the OEWG, and specifically its proposal for regular, institutional dialogue, China acknowledged “multi-stakeholders play an indispensable role in maintaining cybersecurity.” “However, given the fact that OEWG is an intergovernmental process, our discussion should focus on the role played by states and governments, not the opposite,” the statement read. In a podcast discussion conducted by the Centre for Strategic and International Studies after the conclusion of the OEWG, Christopher Painter, former coordinator for cyber issues in the US State Department, suggested China had rejected “formal” multistakeholder involvement in the Group. In response, Michele Markoff, the US GGE Expert, said a proposal for “expansive” multistakeholder participation was “vetoed [by] a non-ally” of the US. From a prima facie assessment of such evidence, it would be reasonable to conclude China prefers a “render unto” approach toward MCD: it will engage both multilateral and multistakeholder initiatives for reasons of practicality, but seeks to retain the closed nature of intergovernmental forums – particularly, the UN – that discuss cybersecurity. In other words, Beijing prefers a strict distinction between both forms of diplomacy, preferring not to dilute the prerogative of states to frame rules or norms for cybersecurity.

Nevertheless, China’s reluctance toward MCD engagement, both within and outside the UN, may change for two reasons. In September 2020, China’s Ministry of Foreign Affairs launched the Global Initiative on Data Security, to promote, among others, an “open, secure and stable supply chain of global ICT products and services.” The announcement reportedly followed a multistakeholder exchange with academia and representatives of internet companies. Foreign Minister Wang Yi suggested China was “looking forward to the participation of […] multi-stakeholders,” and the official summary “wel-

70 Ibid.
As analysts have noted, the GIDS appeared to be a diplomatic counterweight against the “Clean Network Program” that the US had announced in 2020. The Clean Network Program, an initiative by the Trump administration, called for “untrusted” internet companies from China—telecom carriers, apps, app stores, cloud service providers, submarine cable companies—to be delinked from US digital networks in order to safeguard their security and the privacy of Americans. The US initiative, which marshalled support for its principles from a number of countries and market players, appears to have been “retired” by the Biden administration. The future of both CNP and GIDS remains uncertain, but with the US persisting in multistakeholder efforts to set supply chain security standards, it is likely that China too will mount or support parallel, competing MCD initiatives. Both the UN GGE and OEWG have endorsed norms on “supply chain integrity,” as have several other MCD initiatives. China may embrace multistakeholder diplomacy for the limited and strategic purpose of preventing a consolidation of US-led or “unfriendly” normative standards in this issue area.

Secondly, and on a related note, China has expressed its preference for an extended discussion on cyber norms prior to negotiations over a binding, legal instrument for cyberspace. This is amply clear from China’s statements at the OEWG, as well as its support for the Programme of Action initiative. In written and oral comments on the Group’s preliminary and final drafts, China emphasized the importance of placing the section on “Norms, rules, and principles for responsible behaviour of states” above that on international law. This was to ensure the OEWG “did not send an implication to the international community of downplaying the role and significance of norms in one way or another,” the statement read. China also played a key role in ensuring the acquis of the 2015 GGE report was carefully and accurately reflected in the

OEWG report, a fact that was noted by the US Expert.\textsuperscript{75} China’s preference for norms-centric discussions may be an attempt to ensure binding commitments do not prematurely disadvantage it over the superior cyber offensive capabilities of adversaries. With MCD initiatives broadening and deepening global and regional discussions on cyber norms – offering China a wider array of formulations to choose from, regarding its strategic priorities – it may be inclined to orchestrate, or at least tolerate, multistakeholder diplomacy.

**US: Qualified Engagement with MCD**

The U.S. government has consistently promoted multistakeholder models of technical internet governance. If its support for the “informal intersessional” meetings of the 2019–2021 OEWG is any indication, the US is also likely to support multistakeholder participation in the 2021–2025 OEWG. However, direct US engagement with MCD initiatives on cyber stability has largely been limited to domestic forums, with the notable exception of global and regional MCD efforts at capacity-building. Christopher Painter offers a comprehensive survey of US engagement with domestic MCD initiatives in this volume, while acknowledging the lack of formal involvement in similar initiatives abroad. After four years since its announcement, the US in November 2021 endorsed the Paris Call on Trust and Security in Cyberspace, but it has not been involved in recent MCD initiatives co-created by its allies such as the Global Commission on the Stability of Cyberspace (GCSC) (The Netherlands) or Let’s Talk Cyber (Australia and Canada). Additionally, while it has offered informal inputs (like China) to the Tallinn Manual 1.0 and 2.0, it has neither endorsed nor supportively invoked the Manual’s identification and application of international law to cyberspace (unlike its NATO allies such as Germany). Painter offers three reasons to explain the lack of US engagement with global MCD initiatives:\textsuperscript{76}

1. The US GGE Expert’s professional background in disarmament negotiations, and indeed the provenance of cyber stability negotiations in the UN First Committee, he argues, has steered the US approach toward cyber diplomacy. On account of both factors, the US prefers to engage states.

2. The U.S. government may not want to be seen as supporting the MCD initiatives of a few private US companies – notably Microsoft – for reasons of both fairness and practicality. It may be the case that the U.S. government’s endorsement or support of private MCD initiatives

---

\textsuperscript{75} “Discussing the UN OEWG with the Mother of Norms,” n. 70.

\textsuperscript{76} Christopher Painter (2023), Chapter 6 in this volume.
The geopolitics of multistakeholder cyber diplomacy may affect their perceived legitimacy, with private companies seen as proxies of the state. Indeed, the US endorsement of the Paris Call refers only to the “Government of France’s leadership in bringing together a multi-stakeholder group of supporters,” and the announcement itself coincided with a US vice-presidential visit to France.77

3. The lack of a formal, consultative process with respect to stakeholders based outside the US.

In identifying these reasons, Painter therefore suggests the US may be open to MCD initiatives if they were more representative in character, and if the government streamlined or institutionalized its internal framework to engage such initiatives.

Nevertheless, it is worth examining in greater detail the policy considerations or incentives for the US to be formally involved in multistakeholder diplomacy. The U.S. government does not appear to be principally opposed to MCD initiatives involving a select group of private actors. In 2021, nearly three years after it was launched, the US joined the multistakeholder Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online – the Christchurch Call, like the Paris Call, was an initiative led by France and Microsoft, along with other stakeholders such as Facebook, Twitter, YouTube, and New Zealand.78 On the other hand, the US has not supported the Cybersecurity Tech Accord, which as Painter notes, is more inclusive and includes a diverse set of “pledgees” from the private sector. Although the US State Department may not have formal channels to promote MCD initiatives, it has done so for certain types of private efforts on occasion in the US and abroad. It has been a longtime sponsor of the Cyber Norms conference hosted by the Computer Science and AI Lab at MIT, and in 2015 supported “CyFy,” a conference on cybersecurity and norms organized by the Indian think-tank Observer Research Foundation. The US also supported, alongside The Netherlands, a two-day discussion by CSIS and the UN Institute for Disarmament Research in 2016 called “The Future of Norms to Preserve and Enhance International

Cyber Stability” in Geneva. A crucial fact to consider is that these platforms all seek to consolidate and deepen multistakeholder discussion on existing norms. In addition, the US has also used these platforms to offer its views on the future of intergovernmental processes like the GGE, while refraining from addressing the role of MCD initiatives themselves in articulating new norms.

The preponderance of evidence indeed suggests the US remains cautious about formally engaging MCD initiatives that themselves articulate norms or identify existing rules to cyberspace. In 2020, while speaking at a UNIDIR conference, Markoff observed: “I do agree that the function we are talking about – I believe First Committee activities have been the unique and sole province of the focus of prevention of war [sic] – and it ought to remain exactly that, and since states are the key actors in that particular activity, it is states who have to take the steps necessary to prevent war and preserve stability, if that is a mutually held goal.” Markoff also noted that “in the past, some private sector entities have been pretty much solely focused on protecting their own prerogatives and assets, and that’s not an international, normative way of proceedings.” In relation to the Paris Call specifically, US analysts and former officials have speculated that its declaration against “private hack backs,” or the use of offensive cyber capabilities by businesses in self-defense, may have foreclosed the possibility of domestic (including Congressional) debate on the topic. Not wanting to prematurely “limit its use of offensive and defensive cyberweapons,” may explain the U.S. government’s long reluctance to commit to this private MCD initiative. The US statement endorsing the Paris Call notes that it “does not mark a change in U.S. government policy.”

---


84 “The United States Supports the Paris Call for Trust and Security in Cyberspace” (2021), n. 79.
Similarly, the Interim National Security Strategy Guidance released by the Biden administration noted its “commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace” (emphasis added). The formulation is decidedly state-centric, and where collaboration with private sector is envisaged, it is in relation to “managing and sharing [cybersecurity] risk.”

Even in respect to the UN, the US appears reluctant to engage MCD initiatives supported by the UN Secretariat. On the UN Secretary General’s High-Level Panel on Digital Cooperation (HLP), Markoff said: “We the US decided not to […] participate as one of the champions or advisors [of the UN High-Level Panel on Digital Cooperation]. You have a few people with vested interests […] trying to impose their will on 193 states […] Having a report that can comment on the gaps [on capacity building], surely that is useful. But to promote an agenda by a non-expert, that is not useful.” Given its strident opposition to the UN HLP, it seems unlikely, therefore, that the US will engage other UN-based MCD initiatives such as the proposed IGF Multistakeholder High-Level Body.

The US view that states should take the lead in articulating cyber norms appears to be motivated by two geopolitical calculations. The fragmentation of norms-making processes may lead to “islands” of like-minded countries or stakeholders articulating different standards of conduct for actors in cyberspace. Such an outcome would be counterproductive to the global cause of preserving cyber stability. Secondly, the U.S. government is also concerned the proliferation of norms will also lead to calls for an “omnibus treaty” that covers several aspects of cybersecurity such as major cyber crimes or counterterrorism. Since this outcome would play into Russia’s strategy for a comprehensive, binding instrument for cyberspace, the US may be reluctant to endorse independent MCD initiatives that articulate new norms. The US’s longstanding reservations against joining the Paris Call and its declaration against “private hack-backs” speaks to the concern that such a norm could lead to global regulation of such measures. Indeed, Markoff sees the call for development of new norms as “semaphore” for treaty negotiations.

With its emphasis on harmonized and universal standards for responsible state behavior in cyberspace, it would thus seem improbable that the US

---

Building an international cybersecurity regime

steps up its engagement of MCD initiatives or orchestrate new ones of its own accord. The Cyber Diplomacy Act (CDA), a draft of which was recently tabled in the US Congress, appears to confirm this view. The CDA, while recognizing the need to have an (updated) international strategy for cyberspace, and the diplomatic resources to actualize it, focuses mainly on bilateral and multilateral efforts to create cyber stability norms. The head of the proposed Bureau of International Cyberspace Policy has simply a mandate, among other things, to serve as a liaison to MCD initiatives.88 For the reasons listed here, US support for MCD initiatives is likely to be restricted to norms implementation mechanisms like CBMs or capacity-building arrangements.

France: Strategic Autonomy through Multistakeholder Diplomacy

France has been a prolific proponent of MCD, helping craft landmark multistakeholder initiatives such as the Paris Call for Trust and Security in Cyberspace (2018), the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online (2019), the Dinard Declaration on the Cyber Norm Initiative (2019), and the Programme of Action for responsible state behavior in cyberspace (2020). France’s objectives in pursuing MCD initiatives may be categorized into three: leveraging multistakeholder diplomacy to articulate new norms; using MCD initiatives to help build capacity among state and non-state actors toward norms implementation; and promoting multistakeholder participation in otherwise closed intergovernmental discussions.

The Paris Call in particular has been billed as “the first major international initiative which is resolutely part of a multistakeholder approach including states, private companies, and civil society organizations.”89 In 2019, outlining its vision for international cooperation on cyber stability to the UN General Assembly, France argued “mass digitization” has led to “the rise in power of new private actors […] becoming at times a challenge to the sovereignty of States [sic] but also at times essential partners. They are de facto transformers of the power relationships between State actors, non-State actors and the

private sector.”90 In a recent submission to the OEWG, France made the case for “mentioning” the Paris Call principles in the Group’s report, but acknowledged they “are not consensual at this stage.”91 France has also argued the Paris Call reflects a “common vision for the principles that should underpin” state and non-state behavior in cyberspace, and should be “built upon” in UN discussions. Taken together, France’s statements and assertions on MCD initiatives indicate not only that it is fully seized of the implications of treating non-state actors at par with sovereign states, but also that it intends for cyber norms developed through MCD channels to be considered by all states as voluntary guidelines of conduct.

France’s embrace of MCD initiatives was envisioned as early as 2015 in its National Digital Security Strategy. “To assert its influence, France will increase its investment in more informal international forums in which the technical and academic communities and the political decision-makers come together,” the Strategy declared.92 Yet, it is one thing to outline a strategy of promoting MCD initiatives, and another to implement it comprehensively in the manner France has. What factors facilitated France’s orchestration of global MCD initiatives such as the Paris Call? Beyond its broad claim of “asserting influence,” what might be France’s geopolitical compulsions for crafting new MCD initiatives?

The unique professional backgrounds and mandates of French diplomats placed in charge of cyber stability negotiations have arguably facilitated the country’s championship of MCD initiatives. Prior to 2015, the “cyber diplomacy” portfolio within France’s Ministry of Foreign Affairs (MFA) was held by Justin Vaïsse, whose primary responsibility was policy planning for the MFA. Vaïsse’s background as a scholar and historian, as well as his long tenure as research director at the US think-tank Brookings Institution, arguably cast him differently from the mold of the traditional diplomat engaged in international security negotiations. More importantly, Vaïsse has long been a proponent of multistakeholder diplomacy. In an influential 2007 paper on “transformational diplomacy,” Vaïsse argued “diplomacy should be reformed to act not only in the inter-state arena to preserve order between nations, but also on the nature of the units making up the international system in order to

Building an international cybersecurity regime
guarantee order within nations." While at the MFA, Vaïsse founded the Paris Peace Forum, a privately organized initiative which has emerged as France’s pre-eminent multistakeholder gathering on global governance. Indeed, the Paris Call was announced by French President Emmanuel Macron at the first edition of the Paris Peace Forum. At the time of writing, Vaïsse has stepped down from the MFA and serves as the Director-General of the Forum, in which capacity he has continued to champion France’s MCD initiatives abroad. In some respects, the Forum has become the permanent “steward” of the Paris Call – a venue where its principles can be re-negotiated in the future.

In 2015, France created an ambassadorial-level position for “cyber diplomacy” – understood as including cyber stability negotiations – and appointed David Martinon, a career diplomat, to this post. His brief was “upgraded” when President Macron appointed Martinon as “Ambassador for Digital Affairs” in 2017, concurrent to France’s releasing its international digital strategy that sought greater engagement with non-state entities. The wide latitude to engage civil society and the private sector, conferred by the terms of his appointment, allowed Martinon to incubate discussions about the Paris Call, and gather support for the initiative. Brad Smith has highlighted Martinon’s instrumental role in bringing together French officials and Microsoft’s employees to seed discussions on the Call. Additionally, Smith describes Martinon’s brief as similar to that of Casper Klynge, who was appointed in 2017 as Denmark’s envoy to Silicon Valley.

Following Martinon, the post of “Ambassador for Digital Affairs” has been occupied by Henri Verdier, a technical expert who was also an ICT entrepreneur before joining the French government. Verdier’s technical background and professional remit have allowed him to continue the work of his predecessor.

---

sors and deepen the discussions around the Paris Call. In March 2021, Verdier announced the creation of six working groups, that are each co-chaired by supporters of the Call. Their themes and co-chairs are listed below:99

- **Expanding participation** – (co-chairs) Paris Peace Forum, the National Democratic Institute;
- **Involving stakeholders in emerging countries** – Paris Peace Forum, the State of Sao Paulo, and Schneider Electric;
- **Promoting a multistakeholder approach in UN cyber negotiations** – Cybersecurity Tech Accord, AccessCyber.org;
- **Advancing international norms** – Microsoft, F-Secure, University of Florence;
- **Creating a cyberspace stability index** – Paris 8 University, Hague Center for Strategic Studies, CyberPeace Institute;
- **Developing practical tools for supporters** – Cigref network (a French industry body), and Kaspersky.

In addition to hosting discussions around the Paris Call, Verdier has also been an active participant in other state-sponsored MCD initiatives such as Let’s Talk Cyber as well as the proposed Programme of Action initiative. The unique profile and backgrounds of these diplomats have arguably sustained France’s outreach with not only the private sector and technical communities, but also civil society. Their roles have therefore been crucial to facilitating the country’s support of MCD initiatives.

The question remains: what are the geopolitical incentives for France to engage MCD initiatives and create ones of its own? France’s multistakeholder diplomacy in cyberspace appears to be driven by three distinct reasons:

1. the tactical pursuit of three “core” interests in cyberspace, listed in its international digital strategy, and for whose realization the involvement of private sector is essential;
2. enhancing its “strategic autonomy,” understood as the capability of France (and the European Union), to distance its framing of priorities for cyberspace independently from those arising out of Great Power conflict between US and Russia; and
3. leveraging MCD initiatives to advance Europe’s material and normative interests in cyberspace.

---

France’s 2017 International Digital Strategy identifies three areas where collaboration with the private sector is necessary: strengthening the integrity of ICT supply chains; preventing the proliferation or marketing of malicious, “dual-use” ICT tools; and the “supervision” or regulation of “potentially destabilizing practices” like private hack-backs. Notably, all three topics find mention in the Paris Call principles – (Principles 5, 6, and 8, respectively). These three issues, especially the right of private self-defense in cyberspace, have long been raised by France as a cause for concern. In 2017, Martinon argued that “private counter-attacks [or reverse hacking] must stop. Counter-attacks must only be mounted by states.” This is also an issue where France is unlikely to receive any support from the US or Russia: as mentioned above, the US has stayed away from the Paris Call on account of its strong declaration against “hack backs,” while Russia has criticized the formulation as paving the way for legalizing offensive uses of cyberspace. In the absence of state support, France probably sees MCD initiatives as useful to promote the three areas where its interests converge with that of the private sector, albeit on account of the latter’s business considerations.

Related is the leveraging of MCD initiatives to further France’s pursuit of “strategic autonomy.” Arthur Laudrain argues that France seeks, through international cooperation, to maximize both its own and Europe’s “technological and industrial autonomy” as well as “operational autonomy” in cyberspace. While technological autonomy refers to the “hard” capacity of France and Europe’s civilian and military agencies to identify and respond to cyber threats, operational autonomy reflects their ability to “go it alone” or with chosen allies, based on informed decision-making and the ability to “engage in full scope.” A conducive legal and normative environment that allows France to defend its networks or protect its citizens and assets in cyberspace is essential to realizing “operational autonomy.” MCD initiatives like the Paris Call and the Programme of Action – an initiative for regular dialogue under the OEWG, but one that provides for intensive multistakeholder participation – can help create this conducive environment. Through these initiatives, France probably sees opportunities to articulate specific norms on the conduct of private actors

---

102 Ibid.

And finally, France may also see MCD initiatives as a tool to advance a European “vision” of cyber stability. At the launch of the Paris Call in 2018, President Macron spoke of the need to offer an alternative to “the two kinds of internet emerging: Californian cyberspace and Chinese cyberspace.”\footnote{“Five Things You Need to Know About France’s New Cyber Norm Proposal,” New America, accessed February 7, 2021, http://newamerica.org/cybersecurity-initiative/c2b/c2b-log/five-things-you-need-to-know-about-frances-new-cyber-norm-proposal/.} While many elements of a European vision for cyberspace are characterized by its economic aspects – its unique data governance model, state-led efforts to create “European champions” in cyberspace, etc. – there are also security-related dimensions to it, which MCD initiatives could help promote. The joint statement signed between France and Denmark’s cyber ambassadors in 2019 argued Europe could emerge as a “strong, normative voice” in “promoting a multi-stakeholder approach [at a time when the] multilateral system and a rules-based international order is under pressure.” In particular, the statement declared MCD initiatives could pay “special attention” to the digital agenda in UN entities such as the GGE and OEWG.\footnote{“Joint Statement between France and Denmark – a Vision for European Leadership in the Digital 21st Century,” 2019, https://www.diplomatie.gouv.fr/IMG/pdf/joint_statement_between_fr_and_dk_2019_cle8b58da.pdf.}
European Union: MCD to Augment Diplomatic and Coercive Tools

Although the 2015 Council Conclusions on Cyber Diplomacy encouraged the European Union “to [promote] cooperation between the public and the private sectors, as well as research and academic institutions on cyber issues,” the EU approached this mandate cautiously in the early years, orienting its MCD initiatives mainly toward capacity building and the implementation of CBMs in cyberspace. As Patryk Pawlak and Panagiota-Nayia Barmpaliou note, most of Europe’s MCD initiatives in the period between 2013 and 2016 were directed expressly toward helping states tackle cybercrime, or to gather political and institutional support for the Council of Europe’s Budapest Convention. Having sensed the existence of a “normative” roadblock in capacity building – countries with strong cybercrimes laws often wielded them to clamp down on human rights – the EU championed the creation of an “umbrella framework” that would provide precisely such norms-based guidance for capacity building. This effort resulted in the creation of the Global Forum for Cyber Expertise (GFCE), an initiative that emerged from the Hague Conference on Cyberspace in 2015. Although the GFCE’s mandate too was initially limited to capacity building in four areas (cybercrime, e-governance, data protection, and cybersecurity), its terms of reference offered a clear mechanism for identifying non-state partners who can lead capacity building efforts, and recruit expertise.

The GFCE’s capacity building mandate expanded significantly in 2017, when at the annual Global Conference on Cyber Space in New Delhi, it announced the creation of a Global Agenda for Cyber Capacity Building. Known as the “Delhi Communiqué,” the GFCE’s terms of reference for the Global Agenda now crucially included “cybersecurity strategy and policy,” as one of its targets for capacity building. The following year, the GFCE Working Group on this issue created a task force on, among other issues,
The geopolitics of multistakeholder cyber diplomacy, formally embedding MCD initiatives within its remit. The failure of the UN GGE in 2017 to offer a consensus-based outcome document was arguably a catalyst for the GFCE’s expanding its mandate. The Council Conclusions on Cyber Diplomacy had called on member states in 2015 to “strongly uphold” the position that existing international law applies to cyberspace and help build a “global common understanding” on how it applies. However, it is only after the UN GGE’s failure to agree on this very aspect that the EU systematically expanded the scope of its capacity building efforts to include cyber norms, revealing the geopolitical bearings of its MCD initiatives.

The EU in 2017 also unveiled a “Cyber Diplomacy Toolbox” (CDT) with a view toward implementing a “comprehensive EU approach for cyber diplomacy [that could contribute] to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations.” The CDT comprises five “categories” of measures that may be deployed by the EU to meet the above, purported goals:

1. Preventive measures, such as CBMs, capacity building exercises, and public awareness campaigns;
2. Cooperative measures, such as EU-led bilateral and multilateral dialogues, as well as diplomatic demarches, aimed at “the peaceful resolution of an ongoing incident, [assistance to] mitigate the malicious activity, or to ask a third country to join in the response to a malicious cyber activity”;
3. Stability measures, such as statements from the EU High Representative, EU Council Conclusions and diplomatic demarches that serve a “signal- ing function” about a worrisome trend in malicious cyber activities;
4. Restrictive measures in response to malicious cyber activities, namely, sanctions imposed by the European Council under Article 29 of the Treaty of the European Union on states, entities and individuals; and
5. EU support for member states’ lawful responses to malicious cyber activities, which could range from diplomatic steps, countermeasures, or measures taken in self-defence against those activities that amount to an

---

“armed attack” under the UN Charter. To be sure, the “support” envisaged under this measure relates strictly to the previous four categories.

Following the 2017 announcement, the Council in 2019 released “a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect” that posed a threat to the EU, its member states, and third states or international organizations in relation to the fulfillment of the Union’s common foreign or security policy objectives.116 This framework outlined both the kind of cyber attacks that would invite restrictive measures, as well as the nature of those measures, namely, travel bans and asset freezes.

The CDT “regime” is in its nascent stages, and could invite multistakeholder participation in a number of ways. In the category of “preventive” and “cooperative” measures, MCD initiatives could help build capacity and implement CBMs aligned with the EU’s 2020 Cybersecurity Strategy, and additionally convene Track 1.5 dialogues to deepen bilateral and multilateral cooperation.

In the category of “restrictive measures,” multistakeholder participation could even be useful in attributing cyber attacks to individuals and entities, and thus helping implement EU sanctions. A *prima facie* assessment of the 2019 framework indicates a limited role for the private sector in the implementation of coercive measures, although the document covers cyber attacks against both private and state infrastructure. In July 2020, the Council imposed the first sanctions under the framework, targeting individuals and entities responsible for the NotPetya, WannaCry, and Operation Cloud Hopper cyber attacks, as well as the attempted attack on the Organisation for the Prohibition of Chemical Weapons.117 There is no evidence to suggest that private actors offered assistance or evidence in support of the Council’s attributing these attacks to their targets. Nevertheless, the door remains open for future multistakeholder participation in the EU’s cyber sanctions regime. The framework specifically notes “the application of targeted restrictive measures does not amount to attribution [of responsibility for attacks to third States], which is a sovereign political decision taken on a case-by-case basis.”118 This formulation offers flexibility to the EC to solicit multistakeholder inputs on identifying

---


perpetrators of malicious cyber attacks, as long as their legal and political attribution vests with the member states.

Finally, the EU could also rely on multistakeholder diplomacy to move the needle on international cyber law, by promoting deliberation and consensus-building on what constitutes lawful responses to cyber attacks. In particular, MCD initiatives could help consolodate broad-based support within the international legal community on tools such as “collective countermeasures” – the right of states “not directly injured” to apply countermeasures to support the state affected by the cyber attack. Collective countermeasures do not find support in the International Law Commission’s Articles on State Responsibility, but have been endorsed by states such as Estonia and the Netherlands. MCD initiatives akin to the Tallinn Manual consultations with states (organized by the Dutch foreign ministry) could be a strategic tool to strengthen the normative and legal basis of such responses. Indeed, two prominent legal scholars associated with the Tallinn Manual International Group of Experts argue the CDT signals a movement toward treating hostile cyber operations as a “shared concern,” and collective countermeasures as a reflection of collaborative responses.

CONCLUSIONS AND SUMMARY

The preceding comparative analysis reveals how major powers engage in MCD to promote their strategic objectives vis-à-vis norms creation and implementation. Russia, which has relied on multistakeholder diplomacy to engage US and NATO interlocutors through the Garmisch–Partenkirchen Forum, faces a “governor’s dilemma” as it prepares (at the time of writing) to support or host international multistakeholder initiatives such as the 2021–2025 OEWG and the 2025 IGF. As the chapter notes, Russia has sought greater control over the participation of domestic non-state actors in MCD through the creation of the NAIIS. The NAIIS has also emerged as the nodal actor with respect to Russia’s multistakeholder initiatives abroad, with officials seeking a greater coordinating role for it in the OEWG. However, with the Association heavily populated

121 See Johnstone (2023), Chapter 5 in this volume.
by individuals and institutions with longstanding connections to the state and its security apparatus, it risks losing credibility with third parties. Former Western officials have even speculated the NAIIS is a front for Russian intelligence and influence operations because its appearance as an NGO makes it “far less threatening” to, and easier to co-opt or “recruit,” outsiders.\footnote{Pierre Vaux, “Cybersecurity Consultant was Outed for Ties to Moscow, So Why Is He Meeting Top Trump Officials in D.C.?,” The Daily Beast, October 21, 2020, sec. world, https://www.thedailybeast.com/cybersecurity-consultant-was-outed-for-ties-to-moscow-so-why-is-he-meeting-top-trump-officials-in-dc.} In 2020, the German government “distanced itself” from a Berlin-based NGO that had signed an MoU with NAIIS, citing its ties to former intelligence officials.\footnote{Ibid.} Similarly, the arrest in September 2021 of Ilya Sachkov, the founder of the prominent Russian cybersecurity company Group-IB and the sole Russian commissioner of the GCSC, on charges of treason, signals Moscow’s intention to tightly control the activities of prominent private actors in MCD initiatives.\footnote{Tom Balmforth and Anton Zverev, “Russia Arrests Top Cybersecurity Executive in Treason Case,” Reuters, September 29, 2021, sec. Technology, https://www.reuters.com/technology/moscow-office-group-ib-cybersecurity-firm-searched-by-police-company-2021-09-29/.

\textit{Interview with an OEWG Diplomat}, September 17, 2021 [conducted via Zoom].} With the Communist Party of China exerting increased control over domestic and foreign actors in the country’s digital economy, China has indicated...
its limited appetite for MCD initiatives. Even with respect to DNS governance, where Beijing has participated in multistakeholder policymaking institutions such as ICANN, it has sought greater agency for states, as its diplomacy at the ITU and championship of the “new IP” proposal seems to suggest. Nevertheless, the Chinese government is unlikely to abandon multistakeholder diplomacy altogether, realizing as it does the necessity of MCD initiatives to shore up support for its private sector abroad. Sanctions and commercial restrictions imposed by the US and Western allies since 2019 have severely affected the operations of Chinese companies, especially Huawei. As the chapter notes, China’s GIDS proposal was conceived as a counterweight to the now-retired Clean Network Initiative by the US. Ahead of the annual 2021 session of the UN First Committee on Disarmament and International Security, China circulated a similar draft proposal on “promoting global data security.” Notably, the proposal called on states to “handle data security in a comprehensive, objective and evidence-based manner,” and “maintain an open, secure and stable supply of global ICT products and services,” alluding presumably to the discrimination faced by Chinese companies abroad. However, this proposal failed to garner support among states, and China ultimately did not table it before the First Committee. The failure of the UN proposal on data security may force China to take a multistakeholder approach to promote GIDS, involving states and startups across the world in which its state-run businesses and private sector have made considerable investments. It is clear China acknowledges the growing strategic importance of MCD. At the time of writing, Cyberspace Administration of China is slated to organize a multistakeholder discussion at the 2021 IGF – involving Chinese companies as well as experts from Japan, Brazil, France, and the OECD – on “rule-making on Artificial Intelligence.” Other such initiatives on data security may likely follow, but China faces similar tradeoffs as Russia vis-à-vis MCD, namely between retaining control over domestic constituents and risking their perceived credibility as independent interlocutors on cybersecurity.

---


129 “Promoting Global Data Security” (Draft Resolution), ¶1(a).

130 Electronic Correspondence with a Diplomat, October 5, 2021.

On the other hand, the US’s decision to finally join the Paris Call in November 2021 should not be seen as a major shift in its approach toward MCD initiatives. This is clear not only from the accompanying statement put out by the US Department of State, but also the circumstances surrounding the US endorsement of the initiative. The US arguably signed the Paris Call to mollify France, with the bilateral relationship having frayed on account of the US decision in September 2021 to sell nuclear submarines to Australia (an agreement that displaced a France–Australia submarine deal). As long as MCD initiatives seek binding controls on state behavior in cyberspace – among the longstanding demands of pre-eminent private actors such as Microsoft – the U.S. government is unlikely to support them. The US position on international cybersecurity continues to favor voluntary, non-binding norms that are “technology neutral,” i.e. offer clear guidelines for state behavior capable of withstanding advancements in digital technologies. The approach of the U.S. government toward cybersecurity differs from technical internet governance, where it has been an enthusiastic proponent of multistakeholderism. As Raustiala and Becker note, the US “relinquished” contractual oversight of the Internet Assigned Numbers Authority – the body responsible for distributing and assigning domain names and IP addresses – in 2016 to a “global, multistakeholder body” on account of external pressure from strategic adversaries like Russia and China. Rather than allowing other states to have a greater say in DNS governance, the US sought to cede it entirely to private actors, eliciting in the transition process a firm commitment from ICANN (the body that housed the IANA) against future governmental control of those same functions. It remains to be seen whether the US would make such a tradeoff with respect to cyber diplomacy. To begin with, there is a sharp divergence of positions between Russia and China on the need for an umbrella treaty to govern cyberspace; the latter is more skeptical of the utility of binding obligations on states at the present moment. Similarly, the EU and major trans-Atlantic powers are also not in favor of a treaty. Simply put, the US does not face isolation or external pressure to the extent that will compel it toward MCD initiatives, in the same manner as it delegated IANA functions to ICANN. Further, while the IANA transition also implicated security consid-

---


133 Raustiala, Power, Preference, and Delegation in the Governance of the Internet, n. 10.

The geopolitics of multistakeholder cyber diplomacy

operations for the US, the process was led by its Department of Commerce. Any US-led MCD effort aimed at creating rules or norms for international cybersecurity must factor in the role of the US intelligence community, which may be reluctant to participate alongside private actors in a global setting.

France, meanwhile, has been able to create a robust CoP around norm articulation and implementation through the Paris Call. In November 2021, the Working Groups of the Paris Call submitted comprehensive reports detailing their year-long, virtual discussions involving states and private actors. The reports will be presented at the 2021 Paris Peace Forum. This event could conclude multistakeholder diplomacy under the institutional umbrella of the Paris Call, but France will likely want the CoP to also actively participate in the UN Programme of Action (PoA) – of which it is a co-sponsor – for responsible state behavior. The PoA represents a good illustration of “intermediary orchestration,” because France seeks to enhance multistakeholder participation in cybersecurity discussions by creating a “permanent, action-based, and inclusive” forum hosted by the UN. In other words, the PoA attempts to create room, in an otherwise closed setting, for participation of industry and civil society in cybersecurity rulemaking. Indeed, Working Group 3 of the Paris Call, specifically tasked with “promoting a multistakeholder approach in UN cyber negotiations,” published a study exploring different models by which multistakeholder inputs can feed into the PoA. The cyber PoA itself appears to be inspired by the PoA on Small Arms and Light Weapons, which allows for “direct participation” of private actors in assisting states fight the illicit trade in small arms. At the time of writing, the PoA proposal appears to be favorably

received by a number of states as well as private actors, so France’s attempt at orchestrating MCD in the UN through this mechanism could be successful.

Finally, the EU’s Cyber Diplomacy Toolbox offers room for intrusive multistakeholder participation with respect to sanctions and countermeasures in cyberspace. With the 2019 EU Council Framework separating targeted sanctions from legal or political decisions to attribute cyber attacks to third parties, the door remains open for private involvement in this process. The separation gives states the flexibility to support multistakeholder attribution without having to make public the modalities of government–private sector cooperation, which may be expected in a legal or political statement. As a result, potential concerns surrounding the exposure of private parties, especially industry, to possible retaliation, or the sharing of sensitive information by intelligence agencies with third parties, are ameliorated. Private involvement in the application of cyber sanctions via the CDT may take time to materialize, given the internal political dynamics of the EU. Nonetheless, a permissive framework is already in place.

This comparative analysis reveals the changing calculus of states with respect to MCD initiatives. States may have the sole prerogative to set binding rules for cyberspace, but as the analysis suggests, they have increasingly turned to private actors to help further their goals through the articulation or implementation of non-binding norms. The instrumental use of multistakeholder diplomacy for geopolitical ends presents its own set of challenges. With private actors gaining prominence in international cybersecurity discussions, governments will struggle to retain control over them, as the latter’s own interests as well as the agenda of the MCD initiative evolve autonomously over time.

3. Multistakeholder characteristics of past and ongoing cybersecurity norms processes

Josephine Wolff

INTRODUCTION

Surveying the landscape of different efforts to develop global norms for cybersecurity is a surprisingly daunting task for a set of initiatives that, for the most part, spans less than two decades. Have so many concurrent norm development processes ever led to so few concrete, impactful, widely accepted norms? Since the early 2000s, groups of diplomats, private companies, civil society representatives, non-governmental organizations, academics, have convened in a series of different venues, formats, and configurations with the intention of developing some consensus-based, common views on acceptable and unacceptable online activity – the elusive set of cybersecurity norms that would, ideally, enable greater cooperation and coordination across different countries and stakeholders leading to a more secure Internet for all. It was – and remains – an ambitious and worthwhile goal, and participants in the various norm development processes have been tireless in their willingness to experiment with different models and modalities for arriving at norms that incorporated the perspectives of the diverse set of stakeholders involved in cybersecurity. On the one hand, the fact that no clear consensus around a single set of norms for cybersecurity has emerged as a result of all these processes and experimentation can be viewed as a failure of the processes. On the other hand, the very proliferation of these processes and the tremendous effort put into each of them, as well as into formulating new approaches, can be seen as a success in terms of raising awareness about the importance of cyber norms, engaging different stakeholders, and developing alternative sets of potential norms. It is possible that these very successes have hindered the actual development of a concrete set of norms – that the awareness of how important such norms are and the engagement of so many diverse stakeholders has made it more difficult to reach consensus. This suggests that the complexity of the Internet, the
variety of its functions, and the number of different intermediaries involved in its operation and maintenance, may have all contributed to the challenges of setting global norms and establishing functional processes of multistakeholder diplomacy for doing so.

Building from Katzenstein’s definition of norms as “collective expectations for the proper behavior of actors with a given identity,” cybersecurity norms are expectations for online behavior of governments in how they exercise their cyber capabilities, and also, in some cases, expectations for private sector online service providers’ behavior in defending computers and networks and responding to security breaches. In 2016, Finnemore and Hollis wrote of cybersecurity norms processes: “We remain in a period of ‘infinite meetings,’ with nearly every day witnessing an international conference or gathering dedicated to cybersecurity and norms to govern it. The amount of time and attention required to participate in all these projects simultaneously may eventually lead to fatigue, resulting in the cessation or consolidation of various processes.” Five years later, though, the meetings and concurrent norm development processes seem only to have proliferated, and the appetite for cybersecurity norms remains surprisingly robust worldwide. It’s possible that the fatigue Finnemore and Hollis predicted has simply not yet set in, and cybersecurity norms have at least a few more years – or decades – before participants grow tired of such efforts. The continued commitment to establishing norms in this space probably also reflects the extent to which high-profile cyberattacks, as well as cyber-espionage and cybercrime incidents, remain in the news and a constant, if not growing, source of concern and disruption for companies and countries around the world. These incidents can be seen both as clear signs that previous norms-setting efforts have failed to moderate malicious online activity and, at the same time, as equally clear indicators that the development of global cyber norms has never been more necessary or urgent. This is one of the strange ironies of cyber norms development: the less impact previously developed cybersecurity norms seem to have on how actors wield their offensive cyber capabilities, the more determined stakeholders become to redouble their efforts to establish new, more effective, more widely accepted norms to govern this domain.

Given how many such efforts have been undertaken and are currently underway, it is worth revisiting some of the primary cybersecurity norm development processes of the past 15 years and considering what lessons, if any, can

---

2 Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” American Journal of International Law 110, no. 3 (July 2016): 469.
be drawn from their relative successes and failures. To that end, this paper provides a brief overview of seven different processes for developing cybersecurity norms that operated under different models for engaging stakeholders: the United Nations Group of Government Experts (GGE), the Tallinn Manual, the Global Commission on the Stability of Cyberspace (GCSC), the Organization for Security and Cooperation in Europe’s (OSCE) confidence-building measures (CBMs) for cyberspace, the Cybersecurity Tech Accord, the Paris Call, and the UN Open-Ended Working Group (OEWG). These cases were selected to exemplify the different types of leadership and engagement processes that have been attempted in the cybersecurity norms development allowing for examination of the strengths and weaknesses of different modes of multistakeholder diplomacy in this context. Three of these processes – the GGE, the OEWG, and the OSCE – were led by representatives of State governments through international organizations, while the Cybersecurity Tech Accord was championed by a private company, the Tallinn Manual was led by academic researchers, the GCSC was convened by think-tanks, and the Paris Call was led by a hybrid model of government and private industry stakeholders.

All seven of these efforts attempted, to some extent, to incorporate some elements of multistakeholder diplomacy into their deliberations, whether through the inclusion of outside observers, commenters, or signatories, and each therefore offers some insights into the potential benefits and perils of different models of engaging diverse stakeholders in the development of cybersecurity norms. Moreover, since these initiatives have commenced at different points over the span of a decade and, in many cases, existed in dialogue with each other, several of them have been explicitly and self-consciously designed to avoid the pitfalls or drawbacks identified in other processes. Thus, comparative analysis provides an opportunity for reflecting on the ways that these efforts to iterate on multistakeholder cybersecurity norm-development processes have and have not been productive and whether there are additional iterations that might provide more opportunities for global consensus and progress.

Just as discussions of cybersecurity are often muddled by the fact that different States and stakeholders have very different visions for what a secure Internet would look like, so too are discussions of cybersecurity norms processes sometimes muddled by competing ideas about what a successful set of norms should achieve. For instance, private companies engaged in these processes are often focused on trying to drive down digital threats to their customers and data, while States are often more focused on protecting critical infrastructure and their own sovereignty, and academic and civil society participants may prioritize protection of human rights and online freedoms. This makes it not just difficult to arrive at concrete norms that all stakeholders can agree on, but also difficult to assess the effectiveness or value of any individual set of proposed norms, or the associated norm development process from...
which it emerged. Furthermore, as with all norms or security efforts focused primarily on pre-empting certain risks or conflicts, it is extremely challenging to determine whether the existing proposed sets of norms have had any impact on the actual state of cyber conflict – certainly, there continue to be significant and damaging cyberattacks, but whether there would be more (or fewer) such incidents in the absence of the norms-setting processes discussed here is impossible to say. Accordingly, this article does not focus on the question of whether the seven norms development processes it considers have had any impact on the actual state of cybersecurity. Rather, it considers the extent to which these processes have led to the creation of specific norms that could, conceivably, impact cybersecurity, as well as the extent to which they have been successful at garnering broad support from a wide range of stakeholders.

The following sections provide a brief overview of each of the seven case study norms processes in roughly chronological order, outlining the stakeholders involved in each process and the outputs they were able to reach consensus on. Each case study also includes some discussion of the reception of those outputs and processes by outsiders and how those reactions shaped future norms-setting activities. Following the case studies, three analysis sections discuss possible lessons to be drawn from the history of cybersecurity norms development efforts. The first of those sections describes the different models of multistakeholder diplomacy that have been tried in this context and considers how future efforts might further adapt or finetune those models, especially in the direction of encouraging stakeholders to work with smaller groups of “like-minded” allies. The second discussion section looks at the potential for the development of “bottom-up” cybersecurity norms by more technical communities of network operators and system administrators and the strengths and weaknesses of such initiatives. The final discussion section considers the value of having several, concurrent processes for cybersecurity norms operating in parallel and whether these different norms-building processes have helped to reinforce each other and engage a wider swath of stakeholders or instead detracted from the others and split stakeholders among multiple forums and meetings.

THE UN GROUP OF GOVERNMENT EXPERTS

Discussions of cybersecurity at the United Nations date back to 1998 when Russia introduced a first draft resolution in the First Committee of the General Assembly on “Developments in the field of information and telecommunications in the context of international security.” The resolution, adopted without a vote, called on States to “promote at multilateral levels the consideration of existing and potential threats in the field of information security” and inform the Secretary-General of their views on the “Advisability of developing inter-
national principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.”\(^3\) In January 2002, the General Assembly took its first step towards actually developing such principles, asking the Secretary-General to establish the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (or UN GGE). In June 2004, the Secretary-General appointed the first GGE which consisted of 15 members selected for “equitable geographical distribution.”\(^4\) The five permanent members of the Security Council all have seats on the GGE and the other spots are allocated to States who submit official requests to participate by the Office of the High Representative for Disarmament Affairs, which proposes the GGE composition to the Secretary-General. The first GGE, chaired by Russian representative Andrey Krutskikh, concluded its efforts on July 22, 2005, without reaching any conclusions or submitting any recommendations, and the Secretary-General reported that “given the complexity of the issues involved, no consensus was reached on the preparation of a final report.”\(^5\)

Following the failure of the first GGE, the US opposed the establishment of a second GGE in 2009 on the grounds that another group would be unlikely to make any greater progress than the first. But the US was the only country that voted against the resolution proposing a new GGE and so, in 2010, the UN convened a second GGE, and although the US had opposed the second GGE, they were again appointed as one of the 15 members, and Krutskikh was again elected to chair the group (in fact, Krutskikh and the US representative Michele Markoff were the only two experts from the first GGE who were appointed to the second GGE).\(^6\) The second GGE, convened in the aftermath of the 2007 denial-of-service attacks that disabled a considerable portion of Estonian infrastructure, did manage to issue a consensus report in July 2010, and when Russia called for the establishment of a third GGE in 2012 to continue these efforts, the US this time co-sponsored the resolution, which was

---

\(^3\) “A/Res/53/70” (United Nations General Assembly, 1999), 70.


Building an international cybersecurity regime unanimously approved. The third GGE, convened in the wake of the Stuxnet worm that had disabled centrifuges in an Iranian uranium enrichment facility, again had fifteen members. This time, Australia was selected to chair the group, and the final report, submitted to the General Assembly in June 2013, asserted that existing international law and obligations regarding wrongful acts applied to cyberspace but stopped short of establishing what that meant or how principles of international law should be interpreted in the context of cybersecurity. Notably, the third GGE report followed closely on the release of the Tallinn Manual (discussed at greater length in the third section) which similarly affirmed the applicability of international law and the law of armed conflict to the domain of cyberspace but also expanded on that affirmation with more detailed interpretations of how international law applied to cyberspace.

Perhaps reflecting a growing interest in cybersecurity, the fourth GGE, convened in late 2013, was expanded to 20 members and was chaired by Brazil. The fourth GGE submitted a report in July 2015 that made little progress beyond the third GGE report. Already, though, there were signs that the GGE process was faltering. “The 2015 report was able to keep the interstate conversation on the regulation of cyberspace on track but the discussions had not been easy and a number of important issues were notably absent from the consensus report,” Henriksen points out. “Most importantly, despite the vague reference to ‘the principles of humanity, necessity, proportionality and distinction’ … the report did not explicitly state that international humanitarian law potentially applies to cyber-activities.” The fifth GGE, convened in December 2015 with an even further expanded roster of 25 members. The fifth GGE, chaired by Germany, failed to agree on a consensus report in June 2017 after several countries decided not to accept the proposed draft, some because they believed it went too far in applying international law to cyberspace and others because they felt it did not go far enough.

Miguel Rodríguez, the Cuban representative to the fifth GGE, issued a statement about the failed proceedings criticizing the draft final report for trying to apply international humanitarian law to cyberspace, “establish equivalence between the malicious use of ICTs and the concept of ‘armed attack,’” and “convert cyberspace into a theater of military operations and … legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of

---

8 Kane.
illicit uses of ICTs.”

Markoff, the US representative, registered opposite concerns following the failure of the fifth GGE, registering how far apart the participants had been in their views. Markoff said she had “sought clear and direct statements on how certain international law applies to States’ use of ICTs, including international humanitarian law” and ultimately decided that the final draft of the report “insufficiently address[ed]” those issues. In the same statement, Markoff signaled her disappointment with the process and pessimism about continued GGE efforts saying, “Despite years of discussion and study, some participants continue to contend that is it premature to make such a determination and, in fact, seem to want to walk back progress made in previous GGE reports.”

Despite the failure of the fifth GGE, heralded by some as “the end of cyber norms,” the UN convened a sixth GGE in 2019, again with 25 members, and, like the fourth GGE, was again chaired by Brazil. At this point, the GGE faced growing competition from other norms processes, most notably the UN OEWG, established in 2018, which also addressed the issue of cybersecurity norms but, unlike the GGE, allowed participation by all UN member States who wished to join. Several of the norms in the final consensus report adopted by the sixth GGE in May 2021 avoided the contentious topic of how governments might use their offensive cyber capabilities, focusing instead on norms for governments taking appropriate measures to protect their critical infrastructure or facilitating information sharing. However, the sixth GGE report did echo the conclusions of the third and fourth GGEs with respect to articulating a vague commitment to the applicability of international law in cyberspace in relation to attacks on critical infrastructure. The report stated: “a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infra-


structure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."\(^\text{13}\)

Perhaps reflecting the pressures on the GGE to expand its engagement with outside stakeholders, the sixth GGE held consultations to solicit input from several regional organizations (the African Union, the European Union, the Organization of American States, OSCE and the ASEAN Regional Forum) and two additional sessions to solicit input from all UN member States. Despite these consultations, the GGE meetings continued to be held privately, with no summaries or minutes made publicly available, and with no observers from other governments, NGOs, international organizations, or the private sector. The GGE remains the most state-centric of the cybersecurity norms development processes with the fewest channels for outside contributions from and consultations with other stakeholders. Despite that lack of engagement – indeed, quite possibly because of it – the GGE’s “more exclusive and elusive format” continues to be the preferred norms development forum of the U.S. government.\(^\text{14}\) Meanwhile, Russia and other states have pressed for a more inclusive state-centered dialogue on cybersecurity norms through venues like the OEWG, while other stakeholders in civil society, governments, and industry have also sought to initiate alternative norms processes.

THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013)

The Tallinn Manual on the International Law Applicable to Cyber Warfare, first published in 2013, has less explicit governmental support than the GGE, but offers more detailed proposals about how international law should apply to cyberspace than anything agreed upon by any GGE. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) convened the International Group of Experts who authored the Manual, but it did not lead the initiative, or even endorse the final product. Rather, the drafting process was led by Michael Schmitt who was, at the time, a professor of international law at the US Naval War College, and included other academic researchers, technical experts, and international law scholars. Schmitt clarified that “Although numerous


members of the group were serving in senior posts in their countries, all participated in their personal capacity.”

Indeed, the Tallinn Manual itself is full of similar caveats, clarifying that its contents reflect nothing other than the views of its individual authors. Consider, for instance, the following disclaimer included at the beginning of the Manual:

> It is essential to understand that the Tallinn Manual is not an official document, but is only the product of a group of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCDCOE, its sponsoring nations, or NATO. In particular, it is not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers. Finally, participation in the International Group of Experts by individuals with official positions in their own countries must not be interpreted as indicating that the Manual represents the viewpoints of those countries.

The emphasis on the lack of any institutional endorsement of the Tallinn Manual as well as the participants’ insistence that they are merely interpreting existing laws, as opposed to articulating what the laws should be, seems to free the participants to make bolder, more concrete claims about how they think international law applies to cyberspace. At the same time that they insisted they were only interpreting existing laws, some of the more expansive interpretations offered by the group seemed to blur the line between articulating what the laws actually said and what the group believed they should say. Moreover, the role of the NATO CCDCOE in convening the group and providing support throughout the drafting process also left many stakeholders with the impression that NATO was, in some fashion, behind the initiative and supported its outcomes, despite any statements to the contrary. For instance, multiple media reports on the publication of the Tallinn Manual referred to it as a “NATO manual.”

---

17 Ian Johnstone, “Implementing cybersecurity norms: The design of international institutions”, Chapter 5 in this volume.
Further complicating the question of who had developed the Tallinn Manual and endorsed its recommendations was the fact that the International Group of Experts had invited three organizations to serve as observers to the drafting process: NATO’s Allied Command Transformation, the US Cyber Command, and the International Committee of the Red Cross. The first two of these organizations were chosen to offer “the perspective of a multinational user of the Manual” and “the perspective of a relevant operationally mature entity,” respectively, while the Red Cross was invited “in view of the organization’s special role vis-à-vis the law of armed conflict.”\(^{19}\) While representatives of all three observer organizations “participated fully” in the discussions of the International Group of Experts and the drafting process, they did not have to agree to the rules laid out in the Manual, allowing for the final publication to include the additional disclaimer that “Despite the invaluable active participation of the observers in the process, this Manual is not intended to reflect the legal positions or doctrine of any of these three organizations.”\(^{20}\)

In some ways, the Tallinn Manual seems like an attempt for a group of like-minded stakeholders to explore a new forum for cybersecurity norms-setting following the failure of the first GGE. The International Group of Experts was first convened by the NATO CCDCOE in 2009, at the same time that the US was opposing the establishment of a second GGE in the UN, and while the resulting manual was not developed by States or their direct representatives, it clearly aligns with the strong push the US made throughout every GGE to argue for the relevance of international law principles in cyberspace. Shifting leadership for the norms-development process to academics and shifting the convening body from the United Nations to the smaller, more closely aligned set of countries comprising NATO, enabled the drafters of the Tallinn Manual to develop more specific rules for cybersecurity than the GGE had been able to agree to. The rules articulated in the Tallinn Manual are still ambiguous. For instance, the Manual states that “A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful” but it stops short of defining exactly what types of cyber operations directed at civilian infrastructure constitute unlawful cyberattacks.\(^{21}\) Still, by comparison with the inability of some GGEs to even agree on whether international law was applicable to cyberspace, the Tallinn Manual reflects a more concrete and coherent set of norms for cybersecurity than any of the GGE consensus reports.


\(^{20}\) Schmitt, 10.

\(^{21}\) Schmitt.
The Tallinn Manual was later revised and expanded by the International Group of Experts, with a second version, dubbed Tallinn 2.0, released in 2017 and intended to address norms for malicious cyber activity that does not rise to the level of armed attacks or the more disruptive incidents covered by the original 2013 Tallinn Manual. This revision and extension of the initial Manual could be seen as a marker of its success in influencing international conversations on cybersecurity norms and generating demand for further norms development in this same model. Despite all the caveats on the legitimacy of the Tallinn Manual – the lack of any sponsorship or endorsement by an international organization or government, the fact that adoption of its interpretations of the law was entirely voluntary – the Manual received considerable attention and reference in the international community. It suggested an alternative path to the tortured GGE process, one that engaged a group of reasonably like-minded countries and limited set of stakeholders, rather than bringing adversaries together and trying to force them to reach consensus. It also highlighted the potential freedom of creating “unofficial norms” that did not have to be endorsed by government representatives but could instead be disclaimed as the individual views of experts, while still enjoying the legitimacy of close proximity to an international organization.

The primary drawbacks to the Tallinn Manual model were that the proposed interpretations were non-binding and that the Manual did little to bring any new stakeholders to the table who were not already in agreement about the norms they proposed. Perhaps most concerning, though, was the potential for the initiation of this alternative norms-development process to frustrate and discourage non-NATO countries who felt that the US was trying to perform an end-run around the GGE process to impose their own views on what cybersecurity norms should be without going through the appropriate channels. No matter how many times the authors of the Tallinn Manual clarified in the introduction that this work was exclusively their own opinion, given the observer participation of US Cyber Command and NATO and the timing of the process as the US opposed further GGEs, there was no avoiding that the Manual would be widely seen as an articulation of the norms championed by the US and its allies. The sheen of credibility that these organizations’ involvement offered the Manual was a double-edged sword, bringing attention and legitimacy to the Manual but also serving as an irritant to outside States that their UN GGE process had been undermined by a set of unofficial norms masquerading as a “NATO manual.” The Tallinn Manual was released just

---

months before the third GGE submitted its consensus report agreeing that international law and the UN Charter apply to cyberspace. The Tallinn Manual could be seen as having laid the groundwork for the further exploration of those principles that the fourth GGE was intended to undertake, but it could also be viewed as having aggravated some of the non-NATO members of the later GGEs, leaving them to feel that their work had been pre-empted or that some members had already determined norms for cybersecurity without their input, possibly contributing to GGE failures later on.

OSCE CONFIDENCE-BUILDING MEASURES FOR CYBERSPACE

In December 2013, at the end of the same year when the Tallinn Manual was published, and the third GGE submitted its most successful consensus report, OSCE issued a set of cybersecurity CBMs intended to “reduce the risks of conflict stemming from the use of information and communication technologies.”23 The OSCE CBMs were self-consciously not dubbed norms, or rules, unlike the GGE and Tallinn Manual outputs. Instead, they were a set of more modest agreements among OSCE States primarily aimed at sharing information with each other about their own domestic views on and approaches to cybersecurity. As compared with previous efforts in this arena, the CBMs were much less prescriptive. Instead of prohibiting certain types of online behavior they encouraged participating States to “voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet” and “provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term” in hopes of ultimately being able to “produce a consensus glossary.”24 Despite these relatively tepid (and entirely voluntary) commitments, the Russian delegate to the OSCE requested that a statement be appended to the CBMs affirming its belief in “the principles of non-interference in the internal affairs of States, their equality in the process of Internet governance” and high-


24 “Decision No. 1106: Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.”
lighting that its own agreement to the CBMs “required considerable efforts on the part of many delegations involved in the negotiation process.”  

Like the GGE consensus reports and the Tallinn Manual, the OSCE cybersecurity CBMs would continue to be revised and iterated, with a second set released in 2016. But unlike the Tallinn Manual, the CBMs were explicitly agreed to by the State members of the OSCE, a group of 57 countries in Europe, Central Asia, and North America, that includes several countries that are not NATO members, most notably (for the purposes of cybersecurity norms development) Russia. In this regard, the OSCE CBMs can be viewed as trying to forge yet another path for cybersecurity norms development that combines the legitimacy of the GGE approach by requiring the consensus of government representatives in the smaller group setting of a security-focused intergovernmental organization, not entirely unlike NATO. Perhaps the biggest difference among the GGE, Tallinn Manual, and OSCE efforts, however, is in their ambition. While both the GGE and Tallinn Manual were primarily focused on establishing ground rules for cyberspace in the context of international law and human rights protections, the OSCE CBMs had more modest aims of establishing a common vocabulary for discussing cyberattacks and information sharing efforts aimed at preventing “unintentional escalation.” In this sense, the CBMs can be viewed as a precursor to more heavy-handed norms, trying to address, for instance, the question of what countries consider to be a “cyberattack” – something that the International Group of Experts drafting the Tallinn Manual were unable to agree on – as a first step towards then establishing norms to govern such attacks.

In the wake of the fifth GGE’s failure to submit a consensus report, Grigsby argued that CBMs might be a viable alternative to cybersecurity norms. “Notwithstanding some significant progress over the years on cyber norms, the disproportionate attention given to them has overshadowed an equally important tool that could make cyberspace more stable: confidence-building measures,” Grigsby wrote, pointing out that “CBMs may not be as high-profile or high-stakes as UN negotiations, but they have a long track record of improving stability during the Cold War.” In Grigsby’s view, CBMs may be a more productive path for cybersecurity discussions than full-on norms because “CBMs do not require countries to agree to a predefined and shared set of ideological principles.” But in many ways, the cybersecurity CBMs produced by the OSCE in 2013 and 2016 are just norms by another name, focused on the less controversial aims of establishing shared vocabulary and information

sharing, rather than establishing rules for cyber conflict and self-defense. It is true that these more modest aims require less ideological agreement around issues of international law and human rights than the GGE discussions did, but in many ways the OSCE CBMs seem, at their core, to be intended to serve as a first step towards trying to tackle those larger, harder areas of disagreement.

It is notable that the Russian delegation’s support for such mild commitments in 2013 was so hard won – an indication both of how much the cybersecurity norms environment had already soured by then and how wary Russia was of any proposal that united it with the US and other NATO nations that had already made their stance on cybersecurity norms quite clear through the Tallinn Manual. Still, by the time the second set of cybersecurity CBMs were released in March 2016, Russia was more positive in its assessment of the process, noting in its delegation’s statement that “The fact that agreement has been reached in the OSCE on these confidence-building measures confirms that, regardless of the political situation, consensus can be reached on questions of fundamental importance connected with ensuring international information security. We believe it important to steadily build up international co-operation in this area.”27 The modest aims of the CBMs were presumably crucial to achieving consensus from the Russian delegation. So too, was the decision to develop the CBMs in a forum that engaged State representatives directly (in fact, Russia’s statement also affirmed “the key role of States in facilitating practical co-operation in protecting critical information infrastructures”). While the OSCE engaged stakeholders from civil society and private industry through its series of Cyber/ICT Security Conferences, it was fundamentally a forum for States, like the UN. At a 2019 conference, the OSCE even hosted its first consultations with GGE representatives to coordinate and inform their respective CBMs and norm development processes.28

The OSCE CBMs provide an interesting counterpoint to the GGE and Tallinn Manual process in terms of stakeholder engagement and legitimacy. While the OSCE membership is considerably smaller than the UN’s, it is more than twice as large as the GGE’s, and while it did engage private sector and civil society representatives in its deliberations, the OSCE did not delegate the drafting of its CBMs to external stakeholders as the NATO CCDCOE did with the Tallinn Manual. Ultimately, the relative success of the OSCE CBMs seemed to hinge on the organization’s deliberate choice to steer clear of the most controversial and complicated areas of disagreement about cybersecurity,

---

such as the use of cyberattacks to target civilian infrastructure. This may have allowed for some more productive and concrete agreement around sharing information and definitions, but little progress on the topics of most pressing interest to many of the States involved.

THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

In February 2017, at the Munich Security Conference, yet another cybersecurity norms process was initiated, this time by two independent think-tanks: the Hague Centre for Strategic Studies and the EastWest Institute. The two groups convened a multistakeholder consortium they dubbed the Global Commission on the Stability of Cyberspace, a group of 28 commissioners that included academic researchers, industry representatives, and policymakers from around the world. The Commission’s final report, published in November 2019, laid out eight recommended norms, ranging from a norm “again commandeering of ICT devices into botnets” to a norm “against offensive cyber operations by non-state actors.” These norms were developed in consultation with a Research Advisory Group, consisting of an email list that included more than 200 experts as well as 20 studies commissioned from research institutions and individuals. It also hosted meetings “in the margins of relevant conferences to facilitate input from a wide range of stakeholders,” soliciting input from attendees at conferences including BlackHat, ICANN, Israel Cyber Week, Singapore International Cyber Week, the United Nations Institute for Disarmament Research, and the Internet Governance Forum, among others. The GCSC characterized its deliberations as “bottom-up to top-down,” meaning it first “identified operational norms” and then worked backwards from there to develop a definition of cyberstability and a stability framework.

Eggenschwiler points out that the GCSC proposed norms “exhibit a more technical, implementation-oriented phrasing” than the GGE consensus reports or outputs of the Tallinn Manual or OSCE CBMs process. Indeed, norms focused on botnet mitigation, cyber hygiene, vulnerability mitigation, and non-interference with the public core of the Internet all reference technical measures and infrastructure with much greater specificity and detail than any

---

30 “Advancing Cyberstability.”
Building an international cybersecurity regime

prior efforts at developing general cybersecurity norms in the global community. Eggenschwiler suggests this “may be a by-product of having different stakeholders, including very technical participants” and also perhaps speaks to the desire to generate some more concrete norms than the higher-level proposals generated by the GGE and Tallinn Manual efforts. In terms of their ambition, the GCSC norms fall somewhere between the modest proposals of the OSCE CBMs and the more aggressive aims of the GGE and Tallinn Manual efforts, with more concrete but less controversial proposals like mitigating technical vulnerabilities and enacting measures to ensure basic cyber hygiene. Eggenschwiler describes these as “obvious standards” that “appear to reflect politically relatively uncontentious, lowest-common denominator outcomes” but are still “likely to offer valuable quick-wins (low-hanging fruits), in terms of securing implementation of at least some of the prescriptions issued.”

The GCSC offers yet another variation on cybersecurity norms development in response to the perceived failures of the GGE process – it borrows the Tallinn Manual model of convening a group of independent experts but does so outside the auspices of an international organization, instead relying on two independent think-tanks for operational support. It borrows from the OSCE the idea of avoiding the most controversial and intractable disagreements around cybersecurity norms but does so in a different way, by focusing on more technical norms and solutions rather than information sharing and definitional issues. By avoiding any affiliation with an international organization or the illusion of endorsement and oversight by States, it perhaps managed to sidestep some of the frustration that was directed at the Tallinn Manual, and by focusing on more technical issues of cybersecurity, it also helped justify its own model of relying on independent experts rather than government representatives who may be less well versed in the technical architecture of the Internet.

In terms of its impact, Eggenschwiler points to the inclusion of the GCSC norms in the Paris Call and the European Parliament’s cyber defense report as evidence of the GCSC’s success as a “cooperation incubator and norm leader” and its “capacity to directly influence specific policy actions” but concedes that “so far, the global state of cybersecurity has seen little improvement as a consequence of the Commission’s norm-making undertakings.” Still, she deems the GCSC “partially effective,” not least because it has, in her view, “led to renewed emphasis on the inclusion of civil society organisations and other private stakeholders in global cybersecurity problem-solving efforts.”

---

32 Eggenschwiler.
33 Eggenschwiler.
34 Eggenschwiler.
35 Eggenschwiler.
In some sense, the GCSC efforts can be viewed as a hybrid of the global norms forums like the GGE with the very technical communities of network operators and anti-abuse technologists who convene at regular intervals in regional forums to discuss security mechanisms for operating their own networks and services. While the GCSC proposed norms are far less technical than the kind of work done by the network operator groups (NOGs) or the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) that are composed primarily of representatives from private industry, its focus and recommendations come much closer to the kinds of discussions hosted by those groups than do any of the previous global cybersecurity norms processes hosted by the UN, NATO, or the OSCE. For norms development processes like the GCSC that are primarily run by independent experts or industry representatives, this approach of focusing on more technical issues may be less threatening to the authority of States since governments are rarely involved in the operational logistics of the Internet.

CYBERSECURITY TECH ACCORD

In March 2017, the month following the Munich Security Conference where the GCSC was convened, Microsoft President Brad Smith gave a keynote talk at the RSA Conference in San Francisco calling for a “Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace.” Notably, Smith was not just calling on governments to reach an agreement on cybersecurity norms, he was positioning private industry – and particularly his own company, Microsoft – at the center of that process, calling for the tech sector to take on the role of “a neutral Digital Switzerland that assists customers everywhere and retains the world’s trust.” In April 2018, Microsoft launched a Cybersecurity Tech Accord, together with a group of 33 other companies, calling on other private sector stakeholders to join them in their pledge to “oppose cyberattacks on innocent citizens and enterprises,” “empower users, customers and developers to strengthen cybersecurity protection,” and “partner with each other … to enhance cybersecurity.” This agreement, aimed at companies rather than States, attracted more than 100 signatories from all over the world, though

37 Smith.
European firms seemed especially eager to publicize their commitment to the Accord.39

The Cybersecurity Tech Accord is less ambitious in its aims than the Digital Geneva Convention Smith described in 2017. Rather than calling on States to pledge not to launch cyberattacks directed at the private sector and individual users, the Tech Accord merely asks private companies to pledge to protect their own – and each other’s – customers against such attacks in terms that leave signatories room to interpret the four commitments as they see fit. Despite being a private sector initiative, however, the Cybersecurity Tech Accord took a very high-level, non-technical approach to defining its four norms, rather than focusing specifically on technical risks like bots and core network infrastructure as many of the GCSC’s proposed norms had done.

Gorwa and Peez describe the Cybersecurity Tech Accord as “both performative and flexible, allowing smaller firms to label themselves as meaningful changemakers and innovators, while also potentially allowing larger firms to point to the accord as a token of their goodwill without any meaningful commitments or enforcement mechanisms.”40 They conclude that “the accord offers all the PR potential and heavyweight legitimacy and very little of the normative obligation of the international legal language Microsoft has emulated.”41 Like the OSCE CBMs, the Cybersecurity Tech Accord can perhaps be best understood as a first, exploratory foray into cybersecurity norms development by a stakeholder unsure of how best to iterate on the GGE model without either angering the participants in existing norms processes or emulating the pitfalls of those processes. Smith’s 2017 speech, as well as Microsoft’s later involvement in the Paris Call, made clear from the outset that Microsoft’s aim in casting itself as a “Digital Switzerland” was eventually to be able to engage States on a relatively equal footing in the norms process.

THE PARIS CALL

At the UNESCO meeting of the Internet Governance Forum in November 2018, seven months after the launch of the Cybersecurity Tech Accord, the French government announced its Paris Call for Trust and Security in Cyberspace, an initiative that it had planned and coordinated closely with

---

40 Gorwa and Peez, 277.
41 Gorwa and Peez, 277.
Microsoft. The Paris Call includes nine principles, several of which closely mirror the GCSC norms (including one on the importance of cyber hygiene and another on protecting the public core of the Internet) and others which clearly echo the Cybersecurity Tech Accord (“protect individuals and infrastructure”) as well as Smith’s earlier call for Digital Geneva Convention (including a principle on “non-proliferation” of malicious software and practices). Unlike any previous cybersecurity norms efforts, the Paris Call was not directly aimed at any particular group of stakeholders; rather, it called for supporters from States, private companies, non-governmental organizations, and representatives of civil society all at once. According to Ruhl et al., the Paris Call’s “chief strength” lies in this “multistakeholder orientation” as well as its self-conscious design to complement other cyber norm processes rather than competing with them. And yet, in going after a broad base of diverse stakeholders, the Paris Call has also failed to garner some crucial signatories, including China and Russia (although, in late 2021, the United States finally joined the Paris Call).

Lété argues that the Paris Call’s “legitimacy and value will stand or fall with the extent of its community,” positing that “The more numerous and diverse the signatories, the better the Paris Call community will be able to credibly engage the UN or other groupings on cyber norms.” But if the measure of success for a norms process like the Paris Call is the extent to which it can credibly engage the UN, that reinforces the notion that these other processes that have emerged alongside the GGE are fundamentally vehicles for trying to provide input to the GGE and other UN cybersecurity norms processes. In fact, following the launch of the Paris Call, France and Egypt proposed a new UN Programme of Action for Advancing Responsible State Behavior in Cyberspace that would replace the parallel GGE and OEWG efforts with a more flexible process that enabled UN members to divide cybersecurity norms issues among several subtopics and discuss each separately. This proposal faltered when the US and Russia both submitted alternative, competing proposals for the way forward on discussing cybersecurity norms within the UN.

The multistakeholder model of the Paris Call is in some ways reminiscent of the Tallinn Manual in that it combines an international organization and its State members with independent stakeholders but the genesis and leaders

42 Gorwa and Peez.
of the Paris Call are far murkier than those of the Tallinn Manual. That could work to the advantage of the Paris Call by making it more palatable to stakeholders who believe their interests have been more thoroughly represented in its drafting, but it could also engender distrust in the process through which the nine principles were developed and uncertainty about who, exactly, is behind them. Unlike the GCSC or the Tallinn Manual, both of which were developed explicitly without the agreement of governments, the Paris Call comes closer to achieving a blended multistakeholder process that makes it difficult to discern who, precisely, led the drafting of the Paris Call principles, although general consensus seems to lean toward the idea that Microsoft developed it in collaboration with the French government, and the French government later worked to own the initiative more directly.

THE OPEN-ENDED WORKING GROUP

If the Tallinn Manual, the OSCE CBMs, and the Paris Call are all attempts to iterate or improve on the GGE process, none of those efforts has ever been quite so directly a rebuke to the GGE as the establishment of the UN’s OEWG in December 2018, chaired by Switzerland. Like the GGE, the OEWG is convened by the UN and consists of member States, but unlike the GGE, any UN member may participate in the OEWG, and the group holds consultative, intersessional meetings with industry, NGOs, and academic researchers. The establishment of the OEWG was part of a push by Russia to move towards creating a forum for “formal, standing discussion” about cybersecurity norms within the UN, rather than the recurring, temporary GGE sessions limited to a select set of members. Korzak notes that “Such a development would undoubtedly be in the interests of states such as Russia and China that have long been advocating institutionalized discussions at the U.N. and, ultimately, the negotiation of an international treaty on information security. The U.S. and other like-minded states have always resisted such efforts, preferring the more exclusive and elusive format of GGE discussions to advance the normative framework for responsible state behavior in cyberspace.”

The two competing cybersecurity norms processes within the UN highlight just how poorly the previous efforts have served to bring together stakeholders with different views. Rather than making progress on reaching consensus, the US and Russia have each essentially championed their own group within the UN for putting forward their respective perspectives. In light of that deadlock, it’s not surprising that France and others called for the establishment of the

46 Korzak, “What’s Ahead in the Cyber Norms Debate?”
47 Korzak.
Past and ongoing cybersecurity norms processes

Programme of Action, intended to be an entirely new UN entity to oversee cybersecurity norms. Nor is it surprising that the US and Russia both quickly moved to advance their own alternative plans for the GGE and OEWG, respectively.

One of the challenges to the multiple parallel norms processes within the UN is that many of the outside norms efforts, including the OSCE CBMs and the GCSC, have tried to position themselves in dialogue with the UN processes. The OSCE held consultative meetings with GGE representatives at its 2019 conference, for instance, while the GCSC organized a consultative meeting with OEWG in December 2019 at the United Nations. The less clarity there is about which UN body oversees cybersecurity norms, the more complicated it becomes for outside groups to figure out who they should try to work with or how to plug into the UN process. More generally, this makes it harder for vague norms to crystallize, since there is no single place for the norm-creating actors to coalesce. The OEWG shows some signs of being more open to multistakeholder consultation than the GGE, but the future for both groups is unclear, and the existence of both serves not just to duplicate efforts in this space and confuse outside stakeholders but also, ultimately, to undermine each other’s legitimacy and the potential for any agreement on substantive cybersecurity norms when the key stakeholders cannot even agree on a forum for those discussions.

MODELS OF MULTISTAKEHOLDER DIPLOMACY IN CYBERSECURITY NORMS DEVELOPMENT

The existing cybersecurity norms processes have spanned a wide range of multistakeholder models, from the most exclusive, state-run formats, like the GGE, that allow for limited inputs from non-state stakeholders, to more inclusive models of state-run norms processes, like the OSCE CBMs and the OEWG, all the way to industry-run models like the Cybersecurity Tech Accord, independent expert groups like the GCSC, and hybrid combinations of independent experts and international organizations (the Tallinn Manual) as well as industry actors and States (the Paris Call). It’s worth noting this diversity of approaches because criticisms of the GGE have often led to calls for more varied norm-building processes that rely less on the strictures of the UN GGE format. In particular, critics of existing cybersecurity norms efforts have, time and again, suggested that rather than working through larger forums, “like-minded” countries and stakeholders should organize themselves and develop their own norms for cyberspace. But this seems to have been exactly the model whereby the Tallinn Manual, the OSCE CBMs and the Paris Call – and perhaps to a lesser extent also the GCSC and the Cybersecurity Tech Accord – were developed. And while these processes have sometimes
yielded more specific, concrete outcomes than the UN processes that engage less like-minded stakeholders, they often, ultimately, lead back to the UN forums through consultations and input processes. Similarly, predictions that “various non-state actors will begin to take on a greater role in the regulation of ICT”\(^ {48}\) and calls for the private sector to “take the lead in developing codes of conduct” for cybersecurity have not gone unheeded or unfulfilled with industry-led efforts like the Cybersecurity Tech Accord, but neither have they clearly turned out to contribute to more effective overarching norms development processes.\(^ {49}\)

In 2014, Nye predicted “It is unlikely that there will be a single overarching regime for cyberspace any time soon” and suggested that “rather than global agreements, like-minded states may act together to avoid destabilizing behaviour, and later try to generalize such behaviour to a broader group of actors.”\(^ {50}\) To date, the cybersecurity norms processes have largely made some progress towards the first part of that suggestion – organizing like-minded states – but largely failed at the second part, namely generalizing their norms to a broader group. Similarly, Henriksen predicted at the close of the failed fifth GGE that the group’s failure would “likely lead to a shift away from ambitious global initiatives and towards regional agreements between ‘like-minded states’” and the “gradual emergence of a fragmented international normative structure for ICT.”\(^ {51}\) But as more norms processes have emerged around cybersecurity, it’s not clear that they’ve necessarily fragmented the international normative structure so much as they have created additional forums for generating streams of input into the GGE and OEWG processes. The resilience and dominance of these UN structures, even in the face of repeated failures to achieve consensus, is remarkable and perhaps reflects the interconnectedness of the Internet and stakeholders’ recognition that a coalition of the like-minded is unlikely to be able to achieve much in the context of a global network where they will be forced to share infrastructure with those they disagree with and distrust.

There is no clearer illustration of the limitations of working with like-minded stakeholders than the extent to which this range of different multistakeholder

\(^ {48}\) Henriksen, “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace.”


\(^ {51}\) Henriksen, “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace.”
models for norms development and discussion seems increasingly removed from actual cybersecurity incidents in the news. Grigsby posited that the “largest problem” with the fifth GGE “may have been that the discussion among diplomats in UN conference rooms looked increasingly divorced from the operational reality of state-sponsored cyber actions.”\(^\text{52}\) Indeed, many of the norms developed through the processes described in the previous sections reflect behavioral expectations that no longer seem realistic in light of current cyberattacks and sabotage efforts directed at critical infrastructure. Fostering agreement from stakeholders who already do not engage in these efforts to continue not to do so seems of limited value in the context of ongoing cyber conflicts that violate these norms.

Despite the different forums and formats in which these norms have been developed, many of them return to the same set of themes: limiting collateral damage to civilian infrastructure, preventing especially destructive cyberattacks, encouraging strong security controls and protections. Finnemore and Hollis contend that “how cybernorms are constructed will shape the content and character of the norms that emerge,” but so far, it’s not clear that the diversity of processes for developing norms has given rise to norms of very diverse content or character.\(^\text{53}\) This makes it all the more striking that there continues to be so little agreement among stakeholders in the UN settings. The alternatives to those processes – including variations led by independent experts, international organizations, researchers, industry stakeholders, and combinations thereof – have yielded relatively consistent outcomes, but it remains unclear what exactly can or should be done with those outcomes beyond bringing them back to the UN.

DEVELOPMENT OF MORE TECHNICAL CYBER NORMS

Beyond encouraging coalitions of like-minded stakeholders to formulate norms on their own, critics and observers of the existing cybersecurity norms processes have also at times advocated for more involvement by technical stakeholders and the development of more technologically focused norms. Grigsby, for instance, suggests that diplomats should consider “the inclusion of cyber operators – those in the intelligence community and military who actually do the hacking – in existing bilateral dialogues” in order to “bring an element of operational reality to discussions that are often dominated by diplomats and policy wonks who may know very little about how a cyber operation

\(^{52}\) Grigsby, “The End of Cyber Norms.”

\(^{53}\) Finnemore and Hollis, “Constructing Norms for Global Cybersecurity,” 429.
Building an international cybersecurity regime is actually carried out.” Tikk makes a related assertion that “technical-level cooperation – be it between computer emergency response teams, law enforcement entities or judicial authorities – is likely more efficient than politicized formats” and Sabbah suggests that “a bottom-up process … would likely result in a more technical set of standards based on the perceived needs of national CERT officials, which could then percolate upwards with the assistance of cyber diplomats.” Here, again, the challenge seems to be not with the development of more technical standards but the process whereby those standards “percolate upwards.” The GCSC which focused on more technical standards than any of the other processes described here had some success in refocusing the conversation about norms on specific technical protections and principles. But it has so far had much more limited success at injecting those principles into other, more diplomatic discussions.

Another recommendation, slightly different from an emphasis on technical operators and norms but similar in its effort to focus such processes on narrower areas of greater agreement, is to fragment cybersecurity norms discussions into smaller subtopics that allow for stakeholders to reach agreement on some issues even if they cannot achieve consensus on everything. For instance, Hurwitz writes that “efforts to establish a state-led comprehensive regime for cyberspace will not succeed, notwithstanding the illusion that it could provide a more stable order and block fragmentation of the Internet. Efforts to promote international norms in specific issue areas, such as cyber crime and supply chain integrity, are more likely to gain traction and thereby increase the prospects for security in cyberspace.” Nye alludes to a similar goal, writing of cybersecurity norms development that “Progress in some areas need not wait for progress in others.”

Efforts to divide and conquer cybersecurity-related topics through separate norm development processes have met with some success, particularly when it comes to cooperation on cybercrime, but these different areas are so intertwined that such discussions are often challenging to cleanly separate. For instance, any discussion of supply chain integrity cannot avoid a discussion of cyberespionage in incidents like the SolarWinds compromise, and similarly, cybercrime norms governing incidents like ransomware naturally lead to

---

54 Grigsby, “The End of Cyber Norms.”
58 Nye, “How Will New Cybersecurity Norms Develop?”
questions around the states that harbor such cybercriminals and, in some cases, even rely on them for intelligence and access. Separating out individual strands or subtopics of cybersecurity to discuss and develop norms for is therefore challenging and attempts to do so can, again, lead to discussions that appear to be thoroughly divorced from the reality of how interconnected these different elements of cybersecurity are on the ground.

VALUE OF MULTIPLE, PARALLEL PROCESSES AND CROSS-POLLINATION

Perhaps the defining characteristic of the past decade-and-a-half of cybersecurity norms development has been the sheer variety and diversity of different parallel processes that have been undertaken to hold these discussions in different forums involving a wide array of stakeholders. This diversity of forums has both benefits and disadvantages. On the positive side, it can be seen as offering different processes that appeal to and address the concerns of different stakeholders and allowing for the formation of different coalitions of like-minded actors across government, industry, and civil society. But there are also significant potential drawbacks to exploring so many different norms processes simultaneously, among them the risks of fatiguing and frustrating stakeholders who feel there are either too many such forums or that others are trying to exclude them from side processes. Ruhl et al. note:

Great powers have fundamentally diverging views on core concepts like sovereignty in cyberspace that often underlie their different positions on specific norms. If fragmented norm processes begin to map onto these deeper fault lines – rather than provide bridges across them – it may lead to increasingly irreconcilable stances between competing blocs of states. Correspondingly, there is a need to both facilitate cooperation and manage potential points of conflict between existing norm processes. For example, although cross-pollination is clearly occurring, neither states nor other stakeholders appear to have given much attention to whether and how such interactions occur, let alone what value they have to the processes involved.59

It can be difficult to assess whether the multiple, parallel cybersecurity norms processes in progress have done more to bolster each other and include diverse groups of stakeholders than they have to divide key stakeholders and leave them – and, by extension, their favored norms forums – in competition with each other. Certainly, the different norms processes described here have borrowed from each other, and several of the individuals and groups involved have consulted across these processes or participated in multiple forums. Ruhl

et al. describe a “class of ‘cyber norm professionals’” that they view as connecting the “otherwise disparate processes.”

The cross-pollination of norms across these processes can be seen as a sign of progress and consensus building or as an indication of the repetitive and stagnant nature of these discussions. If the ultimate goal of cybersecurity norms development is consensus, however, it is hard to identify concrete ways in which the cross-pollination of these processes has contributed to any progress on that front. It is especially difficult to view the emergence of the rival GGE and OEWG processes within the UN as a sign of progress when they seem to so clearly embody the tensions between the US and Russia on this issue. Perhaps some of these processes – particularly those that don’t involve direct sponsorship by states like the GCSC and the Cybersecurity Tech Accord – can be viewed as complementary to the UN efforts, but those like the Tallinn Manual, the OSCE CBMs, and the Paris Call, that either explicitly or indirectly suggest some state sponsorship pose a clearer form of competition to the UN forums and complicate the idea that fostering multiple processes can be valuable as a means of enabling greater cooperation or soliciting more diverse stakeholder contributions. The number of norms-development processes around cybersecurity do indicate, though, that stakeholders around the world, in both the public and private sectors, have considerable respect for the importance of global norms in this domain and are heavily invested in the outcomes of these processes. Governments and companies continue to send representatives to multiple different norms-related forums with little sign of fatigue or unwillingness to continue. Having so many concurrent processes that engage so many different stakeholders may not make it easier to reach consensus on global cybersecurity norms – indeed, quite possibly the opposite is true – but it does suggest that there is at least fairly widespread agreement about how critical these norms are. Perhaps that recognition of the importance of these agreements will mean that the ongoing consensus-building processes, as incremental and slow-moving as they sometimes seem to be, will ultimately yield a more thoughtful and nuanced set of cybersecurity norms that more stakeholders will actually be wary of violating.

60 Ruhl et al.
INTRODUCTION: THE POLITICAL ECONOMY OF MULTISTAKEHOLDER DIPLOMACY FOR CYBERSECURITY NORMS

There appears to be a consensus that further specification of norms, and further steps to implement norms, will be useful to ensure the global utility of cyberspace, and to reduce the possibility of significant adverse events. While existing international law is widely understood to apply to cyberspace, and while it provides important primary rules relating to limitation of use of force and protection of civilians, it leaves many questions unanswered. For example, the degree to which cyberattack short of “use of force” is prohibited, or can be the basis for countermeasures, and the extent to which private actors may be conscripted to participate in governmentally controlled attacks, is underspecified. UN Group of Governmental Experts Norm 13 (a) calls on states to engage in further action.

Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs [information and communications technologies] and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

This chapter focuses on a narrow definition of cybersecurity, prioritizing protection from geopolitical cyberattack (“cyberattack”), including damage to networks and physical harm at magnitudes that would have national security consequences. Thus, it excludes, for simplification purposes, important issues, including privacy, consumer protection, and ordinary cybercrime. In particular, and recognizing that other areas of cybersecurity remain important,
binding rules of law, non-binding rules, or perhaps institutions seem to be needed in the following five general areas:

1. protecting the public core of the Internet;
2. protecting other critical infrastructure;
3. attribution of attacks;
4. supply chain integrity;
5. vulnerability disclosure.

It is apparent that these goals involve some existing rules of international law applicable to states, as debated and described, inter alia, in the Tallinn Manual and in United Nations Group of Governmental Experts (UN GGE) reports. They also involve some areas where (i) new rules of international law may be proposed, (ii) greater specification of existing or new rules may be desirable, and (iii) rules applicable to private sector actors may be necessary. It is not clear where these additional norms will be developed.

There has already developed a somewhat fragmented regime complex for cybersecurity norms. Relevant norms are being developed in multiple fora, including several dedicated to cybersecurity, such as the UN GGE, the UN OEWG, the Paris Call, the Global Commission on the Stability of Cyberspace, and the Cybersecurity Tech Accord, as well as a number of other cyber domains or non-cybersecurity-focused fora, such as the International Standards Organization (ISO), the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU), etc. Some of this proliferation of fora seems to be an attempt at strategic forum-shopping, in order to advance particular kinds of norms. While a hundred flowers may bloom, the point may be coming when it will be appropriate to focus diplomatic, industry, and civil society attention on a single, multistakeholder forum.

It is worthwhile briefly to sketch the international political economy dynamics of interaction among different groups in the governmental, non-governmental, and international contexts in connection with cybersecurity, in order to begin to assess the political context and dynamics of multistakeholder diplomacy. This international political economy sketch is based on the distribution of power and interest among different relevant actors.

---


Interests in Cybersecurity Diplomacy

Each government wishes to protect its military capabilities, infrastructure, industry, and civilians from cyberattack. Each government will be accountable to these groups for this protection. Many governments will also have offensive cybersecurity interests, in which they desire the capability to attack foreign military capabilities, infrastructure, industry, and civilians, and perhaps to counterattack. Between states with attack capability (“powerful states”), this can be understood as a collective action problem in which each government will be politically better off if it retains attack capability while denying that capability to others. It may be a prisoner’s dilemma in which each powerful state’s best move is to seek to retain cyberattack capability, rejecting effective primary norms and secondary norms that may reduce its capability. However, with sufficient ability reliably to observe the behavior of other powerful states, and to modify the incentives of those other states through effective sanctions or response, effective norms may be produced. States that lack attack capabilities may still be vulnerable to attack by others, but will not be able to offer valuable reciprocity within the cybersecurity norms field.

Leading firms whose business models depend on the growing use of these technologies will seek to protect their robustness and security. Platform companies like Ali Baba, Amazon, Apple, Baidu, Facebook, Google, Microsoft, and Tencent have been active in this area. Other firms involved more directly in cybersecurity, or sectoral firms in the finance or health sectors, are also involved. The interests of these various firms may, in important but incomplete ways, be congruent with those of the citizenry as a whole. Incomplete congruence may be due to many factors, including a failure of firms to internalize the full social cost of cyberattack. To the extent of congruence, public welfare would benefit if these types of firms were represented in connection with negotiations toward cybersecurity norms.

Home governments and host governments compete to control the cybersecurity and cyberattack capabilities of these firms. The firms will often seek independence, and independence may allow them to operate across borders without special security restrictions due to their foreign character. However, in order for firms to achieve this trusted status, they would have to show their independence, through a history of behavior, policy, structure, or other satisfactory evidence. The ability to achieve trusted status may be jeopardized, on the other hand, where they decline to assist host or home governments with their security or other investigation efforts, especially under circumstances where national interests differ. Clear rules about the circumstances in which cooperation is appropriate, and when it is not, would allow firms to maintain their trusted status.
For example, Article 46 of the European Union’s General Data Protection Regulation (GDPR) allows for transfers of data outside the EU, subject to specified types of safeguards, including “binding corporate rules” and “standard contractual clauses” under Article 47. These types of arrangements are more suitable for protection against violations of individual privacy but less suitable for protection against more geopolitical forms of cyberattack, where the firm may be subject to stronger coercion by its host government.

There is also a burgeoning industry in hacking technology, which would presumably have opposing interests. These firms would ordinarily lobby against cybersecurity cooperation, to the extent that cooperation would diminish the value of their hacking technology. The developing cybersecurity industry would have a different set of interests.

NGOs will also represent particular interests. Some will represent business, but many will represent civil society interests in privacy, free expression, democracy, consumer protection, and other values. The role of NGOs in a democratic political system relies on their ability to fill gaps in expertise, the otherwise dispersed nature of individual interests, and legitimacy. While NGOs may themselves have interests or “stakes,” their main role is often to represent those of others.

Power in Cybersecurity Diplomacy

Components of material (hard) power include military capabilities, economic size, and technological prowess. Interests include both defensive and offensive interests. We focus on defensive interests relating to defense against geopolitical cyberattack. Similarly, offensive interests include potential to attack others, diametrically opposed to the defensive interests of others. Finally, actors are not hermetically separate from one another. States control firms and firms influence states. It is important to recognize, though, that different governments have different domestic political economies. For example, most governments have no domestically based companies that are significant suppliers of software systems.

Firms hold important capabilities in prevention, detection, attribution, remediation, and response to cyberattack. These capabilities can be used defensively or offensively. States that host powerful firms, and these states are not confined to the locations of headquarters, will seek to leverage their regulatory power and/or access to their markets to require that they be granted access to the relevant software or devices.
To the extent that “code is law,” firms, as software producers, retain significant power, because norms may be embedded in code. Indeed, the software architecture can define what can and cannot be done in cyberspace. Conversely, law can require code to follow specified requirements.

Legitimacy in Cybersecurity Diplomacy: Transparency, Accountability, Reasonableness, and Industry Capture Risks

Of course, neither traditional diplomacy nor MSD is normatively benign. Governments have no exclusive, or conclusive, claim to legitimacy in international diplomacy. They may not represent their citizens well, and some may view sovereign equality as inconsistent with individual equality.

While in many areas of diplomacy, the private and broader civil society sectors participate informally from the outside, in some contexts it may be more efficient for them to participate on the inside through formal arrangements, either as observers or as more authoritative participants. Within some national governments, there are formal arrangements to consult with industry or NGO advisory groups.

On the other hand, firms are designed to represent their own interests, however enlightened, and NGOs often focus on narrower social goals. Furthermore, MSD may further narrow industry or social interests, at the expense of the broader public interest. Finally, firms and NGOs may disproportionately channel wealthy state interests. Thus, it is not possible to assume that MSD that includes private firms and NGOs will be more legitimate in this sense than ordinary legislation or treaties.

“Legitimacy” may be defined in a variety of ways. One division is between input legitimacy and output legitimacy. Input legitimacy may be viewed in normative or in descriptive terms. By “descriptive,” I refer to perceptions of constituents and others that a rule or institution has been formulated pursuant to a properly representative and fair process. Output legitimacy refers to a normative evaluation of the rule or institution. I will focus on input legitimacy in descriptive terms. Transparency, accountability, reasonableness, and independence may contribute to input legitimacy, by supporting citizens’ perceptions that particular norms carry legitimacy, and thus make it easier to maintain and enforce the norms.

---


Therefore, it is important that MSD be designed to be appropriately transparent and accountable, and that its decision-making be appropriately representative and supported by cogent, broadly appealing reasoning.

**Expertise in Cybersecurity Diplomacy**

Cybersecurity, like many areas of modern diplomacy and state action, involves expert knowledge. Diplomats seeking to develop or implement norms in this field must have this expert knowledge, or, more accessibly, must be able to engage experts. These experts may be within the diplomat’s own government, or they may come from the private sector or NGO sector or academia/think-tanks. Expertise may include the ability to engage in informed formulation and negotiation of cybersecurity norms and to carry out responsibilities of due diligence, attribution, evaluation of technical data, or remediation. These capabilities may reside in various places within government, and/or within private sector or NGO entities. Government officials assigned to diplomatic tasks may or may not have the ability to marshal these capabilities from within government, and they may not be fully cognizant of the costs and benefits to the private and broader civil society sectors of their decisions.

**Design Elements of MSD**

In a sense, all diplomacy, like all other government activity, is multistakeholder. Multiple stakeholders always participate through their national governments or other vehicles. What distinguishes MSD, then, is the formal or at least systematic direct role of non-governmental stakeholders.

MSD is thus a variant of traditional diplomacy. Diplomacy has a default design and a variety of sectoral designs for specific issue areas or contexts. The default design involves intergovernmental negotiation and agreement, utilizing normative instruments such as international law or non-legal rules, and utilizing the United Nations or other global organizations as a universal forum for diplomacy. There are myriad sectoral designs. We need only mention a few of them to illustrate what is meant here: free trade agreements, regional security arrangements, bilateral tax treaties, the World Trade Organization, the International Monetary Fund, the G7, the International Labor Organization (ILO), and the International Criminal Court. Some of these, such as the ILO, contain elements of institutionalized MSD.

There are a number of parameters to consider in connection with the design of a MSD process or organization for the production or application of norms:

1. **Internal and external transparency.** To what extent do persons not directly involved in decision-making or application and yet are affected...
Developing multistakeholder structures for cybersecurity norms

by the decisions and their application have the ability to observe and comment on decision-making or application?

2. **Decision-making.** How does the organization make legislative or adjudicative, or other, decisions? Who participates, with what magnitude of influence? (I do not separately consider membership, which is subsumed by decision-making, transparency, and scope of application).

3. **Scope of legislative authority.** What can the organization do? At the limit, in what areas, if any, can it formulate and apply norms or binding legal rules?

4. **Scope of application authority.**
   a. Who is bound by the norms or organization’s decisions?
   b. To what extent does the organization have the ability to monitor compliance with its decisions?
   c. To what extent does the organization have the ability to induce or compel compliance with its decisions?

This chapter examines selected examples of structures for multistakeholder diplomacy from within and outside cybersecurity, in order to provide a set of precedents for evaluation in connection with evaluation of structures for cybersecurity norm development and application.

It would be wrong to consider all norms, and all participants in norm formation and application, homogeneously. Different norms will involve different types of actors, including different types of states, but also different types of firms, and different types of NGOs. These different players will, depending on the type of norm, bring different levels of interest (stakes) and power to the equation. Lending legitimacy to a norm or its application is a type of public relations or political or moral power. Thus, different types of norms, applicable to different types of persons, will require different MSD procedures to achieve appropriate levels of effectiveness and legitimacy.

The research question to which this chapter responds asks, “Can existing models of MSD provide guidance to advance norms and institutions in cybersecurity?” The introduction to this volume defines MSD and describes its relevance and dynamics. This chapter examines existing models to determine how selected existing MSD structures respond to different constellations of general interest, special interest, expertise, and power, as laid out in the introduction. In order to respond to this question, this chapter is divided into the five following sections:

1. **This Introduction,** focusing on the political economy of cybersecurity.
2. **Fragmentation and MSD in Cybersecurity.** Here, I briefly describe the MSD features of the GGE, OEWG, Global Commission on the Stability of Cyberspace (GCSC), and Paris Call.
3. **Learning from Broader Experience.** I have selected (i) ICANN and (ii) ITU, which work on broader topics beyond cybersecurity, as well as (iii) GAVI (the Vaccine Alliance), (iv) the ISO (with special reference to ISO 26000 on social responsibility), (v) Codex Alimentarius, and (vi) the ILO.

4. **Accountability, Legitimacy, and Power in MSD.**

5. **Conclusion.** Moving Forward toward MSD in Cybersecurity

**FRAGMENTATION AND MSD IN CYBERSECURITY**

The international relations and international law system generally is fragmented, with many different sectoral initiatives and organizations addressing many different subjects. Yet the world is integrated, and so each initiative or organization touches upon other subjects and concerns. Cybersecurity in the sense discussed here, for example, touches upon other cyber regulatory issues, including privacy, consumer protection, intellectual property protection, political integrity, and trade liberalization.

Fragmentation, here across different public policy concerns, means that we are often in the position, as an international community, of “doing acupuncture with a fork,” with a need to take account of where the other prongs will land when we design an intervention. However, fragmentation is also an opportunity for linkage, allowing states to make tradeoffs in different areas so that they may make agreements that are, on the whole, reciprocally balanced even if states make compromises that are adverse to them in some components of the agreement.

Within cybersecurity, however, there are several active organizations addressing the same or similar problems. While these different fora may be mutually reinforcing, allowing for a growing consensus and progression of agreement, it will be useful to narrow the focus of efforts in the development of norms for cybersecurity in some contexts or at some point.

The question of norms in cybersecurity is also subject to fragmentation by virtue of subsidiarity: some types of issues are best governed by the private sector, others are best governed by individual states (or on a sub-state level), and still others require international rules. As Laura DeNardis writes:

> It is important to view multistakeholderism not as a value in itself applied universally but as a question of what form of administration is necessary in any particular context. Certain areas of internet governance should jurisdictionally be overseen by national governments or via international treaties. Other areas are effectively admin-

---

5 See Burke and Hollis, “Cyber Norms” (n 2).
istered by the private sector or non-profit institutions. ... Still other areas require the direct involvement of many stakeholders.⁶

In this section, in order to establish a background for my discussion of non-cybersecurity efforts, I discuss the GGE, OEWG, GCSC, and Paris Call. This will establish the context and foil for the subsequent description of MSD in other areas.

**UN GGE**

The United Nations GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security is a UN-mandated working group in the field of information security. The GGE has focused on the application of international law to cyberspace, and the development of further norms relevant to cybersecurity.

The most recent GGE consisted of experts from 25 states working nominally in their personal capacities. The GGE was established by the UN Secretary General on the basis of geographical distribution, according to standard UN processes for formation of groups of governmental experts. The latest membership structure includes individuals chosen by the permanent five members of the UN Security Council, plus individuals chosen by 20 other states selected by the Secretary General. These representatives are generally government officials, with backgrounds in cybersecurity and international affairs, often attached to ministries of foreign affairs or defense.

The GGE itself does not include significant MSD. Private firms are not directly involved, and in terms of NGOs, so far, only the International Committee of the Red Cross has made submissions to the GGE on issues relating to the laws of armed conflict. While private firms are not directly involved in the GGE process, the 2015 GGE norms are referred to and supported by MSD initiatives such as the Paris Call for Trust and Security in Cyberspace and by the Global Commission on the Stability of Cyberspace.⁷ Private sector initiatives such as Microsoft’s Cybersecurity Tech Accord, Siemens’s Charter of Trust, and Kaspersky Lab’s Global Transparency initiative aim to reinforce the GGE norms.

---


GGE norms are adopted by consensus of all GGE members. These norms are not legally binding on states or private persons, although the 2015 GGE report was adopted by consensus of the UN General Assembly. UN General Assembly adoption adds authority and influence, and states may determine to transpose portions of these norms into domestic law, or possibly international law. The 2021 GGE report, which was adopted within the GGE by consensus in May 2021, represents the latest progress in intergovernmentally-produced norms in cybersecurity. It recites that the process by which it was prepared included “consultations with relevant regional organizations and open-ended consultative meetings with Member States.” It also recognizes “the importance of engaging other actors, including the private sector, civil society, academia and the technical community, where appropriate, in States’ efforts to implement these recommendations.”

**OEWG**

The OEWG was established by the UN General Assembly on December 5, 2018, “to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States” developed by the GGE in 2013 and 2015. The OEWG is an intergovernmental process under the UN, and its participants are states. There is also an initiative of 40 member states to merge the GGE and OEWG to create a Program of Action.

Under the OEWG structure, states are expected to create norms through General Assembly resolutions. Private sector entities and NGOs were invited to discussions and to provide input on a pre-draft report. A three-day informal consultative meeting of the OEWG held in December 2019 produced, accord-

---


Developing multistakeholder structures for cybersecurity norms

According to the OEWG, “a rich discussion between States and a wide variety of other stakeholders.”

On March 10, 2021, the OEWG released its “Final Substantive Report.” An earlier Pre-Draft report was released by the OEWG with feedback from some state, NGO and private sector entities. While the Final Report acknowledges the role of the private sector, regional organizations and inter-governmental organizations, the meetings involving the non-state actors were classified as “informal” meetings. Non-state actors provided concrete proposals, written contributions and informal exchanges on the sub-areas of the OEWG. However, these opinions merely informed the Final Report, which reflects the views of the states. Therefore, while discussions included non-state actors, their role in norm formation was limited.

The Final Substantive Report recognizes that non-state stakeholders have a role in implementation: “public–private cooperation may be necessary to protect [critical infrastructure] integrity, functioning and availability.” “It was affirmed that acting together and inclusively whenever feasible would produce more effective and far-reaching results. The value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community, was also emphasized in this regard.”

“The broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment.” However, the recommendations of the Final Report are all framed in terms of actions of states.

---


14 UN OEWG, Final Substantive Report, para. 18 (see n 12).

15 UN OEWG, Final Substantive Report, para. 19.

16 UN OEWG, Final Substantive Report, para. 69.
GCSC

The GCSC represents an important example of MSD in the cybersecurity norms field. Founded by two think-tanks – the Hague Center for Strategic Studies and the EastWest Institute – and funded by governments, international organizations, corporations, municipalities, NGOs, and universities, it utilized broad sectoral representation. The GCSC was formed in 2017 to “develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.” Its recommendations were prepared by 25 non-governmental commissioners, led by chairs Marina Kaljurand, and later Latha Reddy and Michael Chertoff, and supported by several research advisory groups. It produced a final report in November 2019.

The Commission held numerous meetings and consultations alongside cybersecurity conferences and participated in more than 70 conferences and events. It solicited input from a broad range of government, civil society, and industry stakeholders. In addition, it periodically disseminated online requests for consultations, resulting in over 23 submissions. The commissioners were active participants in cybersecurity communities, reflecting input from these communities. On the basis of this process, the GCSC promulgated an influential set of principles, norms, and recommendations for further consideration. For example, the GCSC norms were included in the Paris Call. Further work is required in order to promote further specification and adoption of these principles, norms, and recommendations by states and other actors.

The GCSC process involved a wide variety of stakeholders but did not formally involve governments as such, and did not produce norms that are formally binding on states or other parties. In order to build out the GCSC process, it will be necessary to develop a system of representation of states and other stakeholders appropriate to produce more complete, and perhaps binding, norms. The next step in the process, as envisioned by the GCSC, is to forward its products to decision-making groups.

---


Developing multistakeholder structures for cybersecurity norms

PCTC

The Paris Call for Trust and Security in Cyberspace (PCTC) was initiated in 2018, with the articulation of nine broad principles aimed at both state and private actors and intended to promote trust and security. The ninth principle is to “promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.” It is supported by 81 states, including the US and EU, but these states do not include China, India, Iran, or Russia. It is also supported by a number of municipalities, international organizations, firms and NGOs. It has been the basis for subsequent multistakeholder consultations.

LEARNING FROM BROADER EXPERIENCE

While of course, cybersecurity and relevant norms are developed and applied in a unique context, the development of MSD in this field can benefit from the possible cross-fertilization that may be provided by a survey of MSD structures and techniques in other areas. I selected six organizations that have interesting MSD structures. I begin with two organizations in related fields – ICANN and the ITU, and then turn to four organizations in other fields: GAVI, Codex Alimentarius, the ILO, and the ISO.

ICANN

ICANN regulates important technical aspects of the Internet. It was founded in 1998, with the mission to “ensure the stable and secure operation of the Internet’s unique identifier systems.” ICANN has no power to address other issues. It was established when the U.S. government decided to transfer Internet domain name system (DNS) management to a non-profit corporation with global non-governmental participation in order to de-politicize Internet governance. The transfer was carried out in 2016, importantly transferring governance power from the U.S. government to ICANN itself.

ICANN’s work is carried out through three supporting organizations that develop and recommend policies concerning the Internet’s technical management within their areas of expertise. They are the Address Supporting Organization (ASO), the Country Code Names Supporting Organizations (ccNSO) and the Generic Names Supporting Organization (GNSO). Additionally, there are four formal Advisory Committees: At-Large Advisory

Committee, DNS Root Server System Advisory Committee, Governmental Advisory Committee and Security and Stability Advisory Committee.

ICANN is governed by the ICANN Board, which makes policy decisions by majority vote of its 16 voting members.\(^{20}\) The board composition is a good example of multistakeholder, and in fact non-government dominated, governance. Under Article 8 of the ICANN Bylaws, eight board members are nominated by a nominating committee that is comprised of delegates selected by different functional constituencies of ICANN, including five designated by an At Large Advisory Committee ("AtLAC"), seven delegates selected by different constituencies within the GNSO, and one each selected by the ccNSO, the ASO, and the Internet Engineering Task Force. Nominating committee members are required to be “persons who are neutral and objective, without any fixed personal commitments to particular individuals, organizations, or commercial objectives in carrying out their Nominating Committee responsibilities.”\(^ {21}\)

In addition to these eight directors nominated by the nominating committee, two directors each are nominated by each of the GNSO, the ccNSO, and the ASO, and one by the AtLAC. The president of ICANN is ex officio a member of the board.

The Board answers to a kind of supervisory board entitled the “Empowered Community” or “EC.” The EC is composed of the ASO, the ccNSO, the GNSO, the AtLAC, and the Governmental Advisory Committee (described below). It has several powers, including the power to recall the ICANN Board.

ICANN thus describes itself as a MSD-based organization:

ICANN’s inclusive approach treats the public sector, the private sector, and technical experts as peers. In the ICANN community, you’ll find registries, registrars, Internet Service Providers (ISPs), intellectual property advocates, commercial and business interests, non-commercial and non-profit interests, representation from more than 100 governments, and a global array of individual Internet users. All points of view receive consideration on their own merits. ICANN’s fundamental belief is that all users of the Internet deserve a say in how it is run.\(^ {22}\)

\(^{20}\) ICANN Board/Bylaws Background, accessed October 2, 2022, https://atlarge.icann.org/topics/icann-board-bylaws/background.


Gleckman argues that ICANN was established as a multistakeholder entity in order to avoid international organization governance through the ITU:

[The US Department of Defense, which first created the internet and authorized domain names, and subsequently the US Department of Commerce, were only willing to relinquish control to ICANN (the Internet Corporation for Assigned Names and Numbers), if there was a multistakeholder governance structure led by IT firms in place. The U.S. government’s core concern regarding this requirement was that, if the U.S. government were to hand over the keys to governing the internet, it did not want any other government to be involved, even if an inter-national organization already existed to coordinate multi-country communication systems.]

The Government Advisory Committee (GAC) includes 180 member governments and 38 observer organizations. States are mostly represented by a leading information and communications technology official associated with the relevant national ministry. It also includes regional organizations and functional international organizations as observers.

The GAC’s role is to provide advice to ICANN on issues of public policy, especially where there may be interaction between ICANN’s activities or policies and national laws or international agreements. The GAC is not a decision-making body, but its advice must be taken into account by the ICANN Board. Advice from the GAC to ICANN is determined on the basis of consensus. Advice is conveyed to the ICANN Board, usually in the form of a communiqué issued at the end of each GAC meeting. Each communiqué and the minutes of GAC meetings are made available online. Some have argued that ICANN provides insufficient governmental control of Internet governance.

Private sector interests are represented in a variety of ways at ICANN, primarily at the GNSO. The GNSO is the policy-making body responsible for top-level domains such as .com, .net and .org. Within the GNSO, there are stakeholder groups that function as caucuses, including a Commercial Stakeholder Group, a Non-Commercial Stakeholder Group, a Registrars Stakeholder Group, and a Registries Stakeholder Group.

The commercial stakeholder caucus is the forum where private company interests are represented. Academic and civil society representatives are represented by the Non-Commercial Stakeholder Group.

---


Since ICANN is a multistakeholder group, the organization strives to:

employ open, transparent and bottom-up, multistakeholder policy development processes that are led by the private sector (including business stakeholders, civil society, the technical community, academia, and end users), while duly taking into account the public policy advice of governments and public authorities. These processes shall (A) seek input from the public, for whose benefit ICANN in all events shall act, (B) promote well-informed decisions based on expert advice, and (C) ensure that those entities most affected can assist in the policy development process.25

Thus, ICANN is a multistakeholder entity, with far less governmental control than some of the cybersecurity-focused organizations such as the GGE and OEWG, but ICANN works largely on code and interoperability issues, rather than norms that are external to the Internet. This suggests that the type of rule produced may be correlated with the power of different types of participants, with private sector interests more dominant in connection with the formulation of technical parameters for software.

ITU

The ITU is the United Nations specialized agency concerned with information and communication technologies. It facilitates international connectivity in communications networks and allocates global radio spectrum and satellite orbits.26

The ITU engages in a number of activities, including developing ITU Recommendations in the ITU Telecommunication Standardization Sector for network technical interoperability.27 In the area of cybersecurity, the ITU has been mandated, within the framework of the World Summit on the Information Society, to act as facilitator for the World Summit’s action line C5 on “Building confidence and security in the use of ICTs,” and it has launched several initiatives in this regard, ranging from the Global Cybersecurity Agenda to the Child Online Protection Initiative.

All 193 UN member states are also members of the ITU, and only their representatives vote on decisions, such as the ITU technical standards. In addition, membership is open to businesses in the ICT industry, international

---


and regional organizations (including NGOs) and academic institutions. There are over 400 businesses (mostly telecommunication service providers), around 130 international or regional organizations, and a similar number of academic institutions that are members of some or all of the ITU’s sectors.

Non-state members are permitted to contribute to conferences and meetings, but not to vote, which only states can do. In ITU decision-making, therefore, while non-state actors have voice, they are not involved in formal decision-making, which is purely the province of states, voting according to sovereign equality and a principle of consensus-based decision-making. All decisions of the ITU are publicly available. The ITU secretariat, responsible for managing administration, meetings, workflow and outreach, is led by a Secretary General.

The ITU largely works through its study groups, which each represent a different type of expertise. Study groups produce recommendations for the establishment of technical standards. Many study group experts represent commercial interests, but the ITU seeks to offer a “neutral” platform.

The US and other countries have avoided expanding the mandate of the ITU to include cybersecurity. The ITU is an intergovernmental organization with the power of its member states. It operates on the basis of sovereign equality. Even though it is a specialized agency of the UN, it is independent of the UN. It does not involve non-state actors in its actual decision-making. The ITU structure, with its emphasis on sovereign equality, and with its failure to reflect actual distributions of cyber power, may be insufficiently congruent with the actual terrain of cybersecurity to be an effective approach to norms in this field.

GAVI

I now turn to examples from outside the information and communications technologies field.

GAVI, the Vaccine Alliance, is an international public–private organization formed in 1999 to encourage vaccine manufacturers to reduce prices for the poorest countries in return for long-term, high-volume, and predictable demand commitments. As such, it is not a regulatory initiative, but an action-oriented

---


29 “What does ITU do?” ITU (see n 27).

organization that makes technical and distributive decisions with operational importance. It has improved access to vaccines for children.

GAVI was initially funded by a commitment of $750 million from the Gates Foundation. Partly because of this relatively neutral commitment of funding, GAVI was able to secure a great deal of additional funding from rich country governments, and more saliently, to develop an independent, trusted framework for international cooperation, bringing together multiple international organizations, countries, and non-governmental entities.  

GAVI brings together public and private sectors to improve access to vaccines for children in poor countries. It has a unique governance structure that is led by a board that combines representatives of states, international organizations, NGOs, industry, as well as independent individuals. The United Nations Children’s Fund (UNICEF), the World Health Organization (WHO), the World Bank and the Gates Foundation each have permanent seats on the 28-member board, while five donor countries and five implementing states are accorded rotating seats. One seat each is accorded to (i) the developing country vaccine industry, (ii) the industrialized country vaccine industry, (iii) civil society organizations, (iv) research and technical health institutes, and (v) the GAVI CEO. The remaining nine seats are occupied by independent individuals. Board members are appointed by existing board members.

With this board structure emphasizing independence and utilizing altruistic support from the Gates Foundation, GAVI has been able to bring together a number of stakeholders that would ordinarily have difficulty cooperating. International organizations would ordinarily compete with one another for jurisdiction, developing country governments would seek to appropriate intellectual property-based vaccines, developed country governments would seek to protect their producers, and private industry would seek to promote its own interests. However, with an initial infusion of resources, and a board that requires independent, disinterested parties to confirm decisions, GAVI has been able to develop trust that the institution, and those participating in it, will work together to achieve its more altruistic purposes.

Perhaps one lesson that can be drawn from the GAVI experience is that if the organization can command significant resources to solve a real problem, with independent, mission-focused governance, various contending interests may be able to coalesce to coordinate action.

ISO

The world’s leading standardization organization is the ISO. A standard is defined as “a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.” ISO is a non-governmental organization with 165 members, representing national standards bodies. The members may be governmental or non-governmental. ISO works closely with the ITU. ISO members vote in ISO technical and policy meetings. Members vote first in the ISO General Assembly, but the core governance body of ISO is the ISO Council, which is made up of a rotating group of 20 members, plus ISO officers and chairs of three policy development committees. Technical standards work is supervised by the Technical Management Board, which reports to the ISO Council. The Technical Management Board consists of a chair and 15 member bodies. The Technical Management Board supervises Technical Committees, which develop ISO standards. Technical Committees consist of members that decide to participate in development of the relevant standard.

ISO decisions are non-binding recommendations. Members that choose to participate on a specific Technical Committee are permitted to propose experts to serve on the Technical Committee and are accorded a vote on the development of the relevant standard. Consumers are accorded a voice in the development of ISO standards through an NGO, Consumers International, and the consumer representatives of national members in the Technical Committees.

ISO states that “Developing ISO standards is a consensus-based approach and comments from all stakeholders are taken into account.” Under the IOS/IEC Directives, Part 1, approval occurs if two-thirds of the votes cast by the voting members of the technical committee are affirmative, and no more than one-fourth are negative.

---

34 ISO, ISO Statutes, Art. 4.2.
ISO began to use more deliberate multistakeholder engagement beginning in 2002 with the development of the ISO 26000 standard for social responsibility. The Social Responsibility Working Group included more than 300 experts from 54 countries, plus 33 liaison organizations representing industry, government, consumers, labor, NGOs, and certain others. This initiative represented an attempt to broaden the group of participants in order to strengthen the respect for, or legitimacy of, the resulting standard. Balzarova and Castka observe that stakeholder groups with expertise were more active in the process of formulating the standard, and therefore were more influential.

**Codex Alimentarius**

The Codex Alimentarius, or “Food Code,” is a collection of standards, guidelines and codes of practice adopted by the Codex Alimentarius Commission. The Commission, also known as CAC, is the central part of the Joint FAO/WHO Food Standards Programme and was established by the Food and Agriculture Organization (FAO) and WHO to protect consumer health and promote fair practices in food trade.

The Codex Alimentarius Commission has 189 members made up of 188 member states and the European Union. Most standards at the Codex Alimentarius are formed by committees on specific topics. However, the final adoption of the standards is the prerogative of the Commission. All decisions by the Codex Alimentarius Commission are taken by member state consensus. In situations when consensus cannot be reached, decisions are made by majority vote.

Codex Alimentarius allows for “observers.” Observers are divided into NGOs, IGOs, and other UN organizations. While private sector companies are not directly a part of the organization, they are represented through NGOs such as Food Industry Asia, EuroCommerce and the International Association

---


Developing multistakeholder structures for cybersecurity norms

of Consumer Food Organizations. These NGOs provide important expert contributions and legitimacy for Codex standards.

“The food standards, guidelines and other recommendations of Codex Alimentarius shall be based on the principle of sound scientific analysis and evidence, involving a thorough review of all relevant information, in order that the standards assure the quality and safety of the food supply.” 43 Codex members rely on outside assistance in this regard. There are two standing expert groups that support the Codex process: the Joint FAO/WHO Expert Committee on Food Additives and the Joint FAO/WHO Meeting on Pesticide Residues. On standards not related to these two areas, Codex convenes expert consultations on an ad hoc basis. Both the expert groups and the consultations make recommendations to Committees on proposed draft standards.

All discussions of the Committees and Commission are available on the website. The meetings are also broadcast live on their website for the public to view. Member states have direct access to discussion by virtue of being a member. Any NGO, provided it satisfies certain requirements, may attend any session of the committees or commission.

Within the Codex legal and organizational system, Codex standards and related texts are voluntary in nature. They ordinarily require transposition into national legislation or regulations in order to become enforceable. 44 However, beginning in 1995, as a result of referencing of Codex standards in the WTO Agreement on Sanitary and Phytosanitary Measures (SPS), WTO member states are under an obligation to utilize Codex standards in their domestic standard-setting, except if there is a scientific justification or where the Codex standards fail to achieve their appropriate level of protection. 45 Since 1995, when Codex standards were “hardened” in the WTO SPS Agreement, consensus has sometimes been more difficult to achieve, owing to important distributive impacts of certain contentious standards. 46

It is worth comparing Codex, which is an intergovernmentally-focused organization, with ISO, which is dominated by private entities. Both produce


45 A similar phenomenon has occurred in connection with ISO international standards, which are produced as soft rules, but “hardened” in the WTO Technical Barriers to Trade Agreement.

product standards, but perhaps the food safety standards developed by Codex are more essential to governmental functions to ensure citizens’ safety. In this sense, cybersecurity norms may be growing more similar to food safety standards than to industrial product standards, even though industrial product standards can, in at least some instances, address risks of magnitudes similar to those addressed in food safety standards.

ILO

The ILO, a UN agency established under the Treaty of Versailles in 1919 (as an autonomous agency associated with the League of Nations), is principally concerned with international labor standards.

Its governance includes a system for “tripartite governance” that includes member states, as well as employer and worker organizations. These three constituencies are included in all discussions and decision-making on international labor matters at the international level, and the ILO also promotes a similar tripartite cooperation at the national level. “For this reason, not only does the ILO Constitution provide a clear role for both employers’ and workers’ organizations in relation to the adoption and supervision of international labour standards (i.e. Conventions and Recommendations), but most of these instruments also provide a role for them in implementation at the national level.”

At the international level, the ILO makes major decisions through the tripartite International Labour Conference, which meets annually to set international labor standards as well as broad policy. Each member state delegation consists of two government delegates, an employer delegate, and a worker delegate. Each delegate participates and votes independently. Labor and employer delegates are appointed by their governments, subject to agreement of the most representative industrial organizations. The Conference adopts conventions and recommendations by a two-thirds majority of its delegates. Of course, ratification according to domestic law is required for the conventions to become legally binding on adhering states.

A Governing Body, which meets thrice yearly, acts as the executive body of the ILO. It is responsible for policy, programs, and budgets. The International Labour Office serves as secretariat. “The work of the Governing Body and of the Office is aided by tripartite committees covering major industries. It is also

---


supported by committees of experts on such matters as vocational training, management development, occupational safety and health, industrial relations, workers’ education, and special problems of women and young workers.”

Tripartite governance is also apparent in supervision of implementation of standards. “The regular system of supervision is based on the examination by two ILO bodies of reports on the application in law and practice sent by member States and on observations in this regard sent by workers’ organizations and employers’ organizations.”

A standing committee of the [International Labour] Conference, the Conference Committee [on the Application of Standards] is made up of government, employer, and worker delegates. It examines the report [of the Committee of Experts] in a tripartite setting and selects from it a number of observations for discussion. The governments referred to in these comments are invited to respond before the Conference Committee and to provide information on the situation in question. In many cases the Conference Committee draws up conclusions recommending that governments take specific steps to remedy a problem or to invite ILO missions or technical assistance. The discussions and conclusions of the situations examined by the Conference Committee are published in its report.

At the national level, the Tripartite Consultation (International Labour Standards) Convention, 1976 (No. 144), “requires effective consultation between government, employers’ and workers’ organisations at each stage of the standards-related activities of the ILO, from setting the agenda of the International Labour Conference, ratification of international labour standards, the supervision of the application of standards, to denunciation of ratified Conventions.” The national government is the final decision-maker – consultation does not require negotiation. The national government also determines the form of consultation, although the consultations usually are carried out within a national institutional framework.

The ILO tripartite model reflects the unique circumstances and political power of employers and unions in the context of international labor governance and in connection with internationally required national governance. For


52 ILO, Promote tripartite consultation, 2 (see n 47).
some types of cybersecurity norms, this type of representative governance may be considered attractive in light of its reflection of political power and diverse interests.

**LEGITIMACY, ACCOUNTABILITY, POWER, AND DEMOCRACY DEFICITS IN MSD**

The standard source of political legitimacy, at least in liberal democracies, is elected constitutional government decision-making. This is why the default option for many policy-makers is to rely on (i) national formulation of policy through normal constitutional processes, and (ii) international negotiations in accordance with normal diplomatic practice.

With the rise of international or global governance – greater decision-making beyond the state – concerns have been raised that parliamentary control or other mechanisms of input or accountability are insufficiently available at the stage of international negotiations. This is the basis for the gradual empowerment of the European Parliament, and for suggestions that the World Trade Organization would benefit from a parliament. The claim is that while these mechanisms exist at the national level, they are insufficiently influential when decisions are made at the international level.

Can MSD at the international level be a substitute for parliamentary control, and can it supplement multistakeholder policy formulation at the national level? MSD does not provide the kind of accountability or democratic control afforded by parliamentary control. Rather, it expands the voices, and perhaps the decision-making power, beyond the state itself. This expansion may align decision-making better with the actual distribution of interests and power in connection with cybersecurity norm formulation and application. Firms may represent their customers and may internalize the costs of some types of cyber-attack, more effectively than governments. NGOs may represent interests that would otherwise be under-represented in norm formation or application. Firms and NGOs may provide expertise or information that improves the quality or effectiveness of norms.

Yet these structures are not necessarily attractive from the standpoint of legitimacy, accountability, and effectiveness.²⁵ Both firms and NGOs fail to represent the whole of society. They are participants in interest group politics, which often must be twinned with electoral politics, representing the broader society, in order to provide suitable outcomes. Either may accentuate the

---

²⁵ For a general critique of “multistakeholderism” and structural recommendations, see Gleckman, Multistakeholder Governance (see n 23).
representation and satisfaction of certain interests at the expense of broader societal goals.

In order to make a positive contribution, MSD must be designed to accord appropriate, but not excessive, transparency, voice, and decision-making authority to non-state actors. Some MSD initiatives have been criticized for according excessive influence on firms. Firms can be expected to represent their own interests in MSD, and if they have too much influence, the output of the MSD may be illegitimate, inappropriate, or, if the firms wish to avoid meaningful regulation, ineffective. Influence accorded firms in MSD can be counterbalanced by the power of governments, as well as influence accorded interests that are likely to be adverse to firms, yet otherwise under-represented. It can also be counterbalanced by conflict of interest policies that require relevant disclosures and other rules to limit the effects of conflicts of interests.

With respect to firms, as well as to NGOs, it is important to have an appropriate means to select organizations to represent classes of interests in MSD, and to ensure that those selected will be accountable to others in their class. One selection criterion will be the extent to which the interests of the organization chosen are congruent with those of the class as a whole.

CONCLUSION: MOVING FORWARD TOWARD MSD IN CYBERSECURITY

This review of MSD in a variety of settings reveals great diversity at the international level. Elsewhere in this volume, authors consider non-governmental influence in MSD and in cybersecurity governance at the national level. This review provides a selective inventory of MSD structures that may be considered in designing MSD in cybersecurity.

MSD at the international level has generally not been a part of formation of the international law of use of force, the laws of armed conflict, or other traditional areas of international law. What is different about cybersecurity, and about the modern context of cybersecurity, is the fact that the relevant field of security contention is more greatly influenced by the power, expertise, and interest of private sector interests, and perhaps has greater effects on civil society interests, than earlier fields of security contention. In an important sense, cybersecurity is a field of geoeconomics, in which geopolitical contention shapes economic and market policy.

So it is worth examining other fields in which the power, expertise, interests, and perceived contributions to legitimacy of non-state actors play a significant role. What we find is that in areas such as product standards, vaccine distribution, and labor relations, norm-producing and implementation mechanisms have given non-state actors important seats at the table. Resources, expertise, and interest all seem to influence the role of non-state actors. While non-state actors can be expected to articulate parochial interests, their interests may be sufficiently congruent with broader public interests, or sufficiently important, to provide them with a role in the formulation and implementation of norms. The ability to do so will depend on the ability to avoid the perception or reality of capture by special interests.

In areas where a significant public interest is at stake, and may not necessarily be sufficiently protected by a national government “backstop” of legislation, such as in the food safety context, government continues to play a significant role. We also see in the GAVI case that contributions of resources may serve to coalesce cooperation among other actors. In the ILO tripartite case, large labor interests demanded and were accorded direct representation and power.

In all these contexts in which non-state actors were accorded direct representation at the international level, domestic politics to influence national positions was seen as necessary, but not sufficient. It is a general critique of the way states are organized for international relations that some domestic interests do not feel that mere domestic influence on diplomats is enough: direct international action is seen as needed to redress a “democracy deficit” at the international level.

Each of these distinct contexts has its own history and dynamics, but they provide a suggestive trend, and a proof of concept, that MSD may assist in making and implementing norms in this field. In these varying contexts, actors have had an opportunity to address the problem of veto points and the possibility that MSD may make it more difficult to make and implement norms. They have also had an opportunity to address the conflicts of interest – indeed the, by definition, parochial interests – of non-state actors compared with national governments that at least purport to represent their entire citizenry.
INTRODUCTION

Multiple processes have made progress in articulating norms for cybersecurity. While there is further work to be done in pushing for wider adoption of the norms and in elaborating their content, attention is turning increasingly to norm implementation. Much of that attention has aimed at getting states to internalize the norms in domestic legislation and institutions, and to work informally with other states on implementation measures that require inter-state cooperation. Similarly, the information and communications technology (ICT) industry and other non-governmental actors have begun to collaborate on implementing norms they have agreed to. This chapter looks beyond those nascent efforts to more institutionalized cooperation. What mechanisms, devices and institutional arrangements exist or could be devised to induce or compel compliance with cyber norms?

While this chapter focuses on compliance, it is premised on an understanding that the line between formulating new norms and implementing existing norms is blurry. Norms develop and evolve not only (or even mainly) through negotiations around a table, but through a dynamic process that combines practical experience with discursive interaction (including negotiations, but also contestation over incidents). Experience in the implementation of norms contributes to their progressive development in various ways. It may expose gaps in the normative framework, leading to the creation of new norms. It
gives content and specificity to imprecise norms, leading to their “hardening.”\(^1\) And it reveals flaws in existing norms, leading to their adaptation.\(^2\)

The most widely accepted definition of a norm in international relations theory is “collective expectations for the proper behavior of actors with a given identity.”\(^3\) In the cyber literature, “norms” are sometimes distinguished from law.\(^4\) In the broader political science and sociology literature, law is viewed as one type of norm. Other types are social norms, religious norms, cultural norms, professional norms, and norms of etiquette. In international relations, norms fall on a spectrum from clearly non-binding political commitments to “soft law” to the hardest treaty law.\(^5\) Where a norm falls on that spectrum is often contested, and indeed the very idea of soft law is questioned by some legal scholars. This chapter does not delve into those debates, but starts from the premise that norm evolution entails two distinct but related phenomena. First, what a community determines to be “proper” or appropriate or accept-

---

\(^1\) On the process of hardening the law through the practices of international organizations, see Ian Johnstone, “Law-Making through the Operational Activities of International Organizations,” *The George Washington International Law Review* 40, no. 1 (2008): 87. More generally, the International Law Commission has determined (and the UN General Assembly has endorsed) that in certain circumstances, the practices of international organizations can contribute to the development of customary law. See UN General Assembly, Resolution A/73/10 (2018), Draft conclusions on the identification of customary international law, with commentaries, Part Three, Conclusion 4, paragraph 2, 130–132.

\(^2\) It may simply be adding elements to an existing soft norm, for example, including healthcare systems in the definition of critical infrastructure that ought to be immune from cyberattacks.


Implementing cybersecurity norms

able behavior at one point in time may come to be seen as abhorrent later. Slavery is an example. Second, norms can move along the spectrum from soft to hard (in both directions). For example, international human rights went from being a broad aspiration in the UN Charter, to the soft law of the Universal Declaration of Human Rights, to binding legal commitments in a wide range of human rights treaties. As Martha Finnemore and Duncan Hollis point out, norms grow out of social processes and interactions, and they are extended and amended in that way. International legal norms evolve and crystallize mainly through the practices and discursive interactions of states, but increasingly intergovernmental organizations (and their staff), legal and subject-matter experts, non-governmental organizations, and businesses are involved.

The evolution of norms is not always progressive. Just as soft law can harden, hard law can soften. In principle, one would expect the movement to be in a forward direction if institutional mechanisms are constructed for implementing the norms. This is because the institution and any argumentation that occurs in and around it is tacit acknowledgment that the norm exists and ought to be respected. However, if the push for implementation mechanisms gets too far ahead of what the political context will bear, it can have the opposite effect: a widely accepted “soft norm” can lose support. One can imagine adopting a global cybersecurity treaty with a verification mechanism, perhaps even a dispute settlement body with enforcement powers. However, the attempt to do so could be counterproductive. It may have the effect of reversing the incremental progress that has been made, causing states to back-pedal on their commitments on the assumption that – at least for some states – stronger implementation mechanisms would reduce their willingness to participate in the regime, preferring the flexibility provided by softer norms and institutions.

Thus, rather than seeking to build a unified cybersecurity regime in one fell swoop, it may be better to do it in bits and pieces through a dynamic, iterative process involving multiple state and non-state actors. Indeed a “regime complex” of sorts already exists in the cyber field, defined as “an array of partially overlapping and nonhierarchical institutions that includes more than

---


7 Arguably, this is what happened to the “responsibility to protect” norm.
one international agreement or authority.” Conceivably, the cyber regime complex will strengthen and become more coherent as key stakeholders converge on a set of norms and institutions that serve their mutual interests. If that convergence occurs, it will likely be through the practice of living and interacting within the regime complex, as well as through negotiation.

The chapter proceeds as follows. I begin in the next section by briefly reviewing theories of compliance with international law. While these theoretical perspectives are not mutually exclusive, they suggest alternative implementing mechanisms that may be used to mete out rewards and penalties. In the third section, I outline three broad considerations that underpin any attempt to build a cybersecurity regime: the distribution of power and ideological differences among states; diverging capacity and interests among all stakeholders; and the multiplicity of possible institutional forms. The fourth section identifies five categories of implementation devices that could be used within those institutional forms: information-sharing and dialogue; monitoring and attribution; financial and capacity-building assistance; dispute settlement; and collective sanctions. Within each category, I describe the devices and identify those that hold the most promise in moving forward on cybersecurity.

THEORIES OF COMPLIANCE: PENALTIES AND REWARDS

Theories of compliance with international law help us to understand and assess the range of possible mechanisms that could be constructed to implement cybersecurity norms. In this section, I briefly review the theoretical literature through the lens of “penalties” and “rewards.” Most legal writing on compli-
ance focuses on the former, either because scholars do not think of rewarding as a compliance mechanism or because they treat it as the mirror opposite of penalizing and therefore of little distinct analytical significance. Yet as Anne van Aaken and Betül Simsek wrote recently, not only are rewards used to induce compliance in many areas of law, in some contexts they are more effective than penalties. Below, I survey the penalties and rewards associated with each theory of compliance. I allude to those that may apply to cybersecurity norms, and then develop the analysis more fully in the third and fourth sections of this chapter.

**Enforcement Model**

The enforcement model posits that “true” compliance is rare and occurs only when sanctions are threatened. According to this model, while states often behave in a manner that accords with the law, it is not because they are “complying” but because they would have behaved that way even if there were no law. What looks like compliance is either coincidental or what Downs, Rocke and Barsom call “shallow cooperation.” True compliance is measured by the extent to which a treaty requires a state to depart from what it would have done in its absence. Their argument is that “deep cooperation” only occurs with strong enforcement mechanisms.

In this model, compliance, therefore, is largely explained in terms of penalties rather than rewards. These penalties may come in various forms: military action (either kinetic or cyber), economic sanctions, or international criminal prosecution. As a penalty, military action is legal in three circumstances: in self-defense based on Article 51 of the UN Charter; when authorized by the UN Security Council under Chapter VII; or against a non-state actor with the consent of a host state. Economic sanctions may be imposed by the UN Security Council, by a regional organization, by a group of states or unilaterally. The penalty ranges from a full-scale embargo or commodity sanctions against a country to targeted sanctions on individuals, such as asset freezes. There is no international legal prohibition against the imposition of sanctions, so when applied unilaterally in response to a cyber operation, they could be considered retorsion (an “unfriendly” act taken in response to another unfriendly act). Criminal prosecution applies to individuals, not states. It must be applied in domestic courts unless the attack rises to the level of one of the

---

11 Van Aaken and Simsek, “Rewarding in International Law,” 198.
four international crimes specified in the Statute of the International Criminal Court: genocide, grave war crimes, crimes against humanity and – for parties that ratify the Kampala amendments – aggression. It is unlikely, although conceivable, that a cyberattack would rise to the level of one of those crimes.

Rational Choice Theory

Rational choice theory, in contrast, argues that coercive enforcement is not always necessary. States often comply with the law because, weighing the costs and benefits, they conclude that compliance is in their interest. The most straightforward reason for compliance is reciprocity: a state complies with a trade agreement, for example, because it hopes for and expects reciprocal compliance by other states. Additional rewards (beyond reciprocal compliance) can be offered as an incentive. This may be in the form of financial assistance to meet the obligations of a treaty, or compensation for losses suffered as a result of fulfilling the terms of a treaty. It could simply be a side-payment to get a state or non-state actor to behave in a certain way. In the cyber realm, several of the norm processes have urged states to promise economic assistance in rebuilding after an attack on infrastructure.

Rational choice theory also highlights the importance of reputation. States comply with international law because they have an interest in preserving a reputation for playing by the rules. The “shadow of the future” creates a powerful incentive to comply with the law, even at the expense of short-term gains, in order to preserve a reputation for being a reliable counterpart in future cooperative arrangements. Reputational effects can operate as either a penalty or reward. Reputational damage from non-compliance can be inflicted through “naming and shaming,” either by other states, intergovernmental organizations, or non-state actors. In the cyber realm, the public attribution of respon-
Implementing cybersecurity norms

sibility for a cyber incident to a state or non-state actor is a form of penalty, even if no sanctions follow immediately. 16 Conversely, states and non-state actors can enhance their reputation through pro-norm behavior, which translates into opportunities for future cooperation. Beyond overt “naming and praising,” reputational gains can be accrued in multiple ways: winning a court case, getting a clean bill of health from a certification agency or human rights non-governmental organization (NGO), or moving up the scale on a global index (more on indicators and rankings below).

Managerial Model

The managerial model of compliance, first developed by Abram and Antonia Chayes, starts from the rational choice proposition that states have a general propensity to comply because it is in their interest to do so. 17 But they add several elements to that explanation. States do not constantly calculate and recalculate whether compliance is in their interest; rather, they typically comply as a matter of bureaucratic and political routine. Compliance is the default position, almost a matter of habit, deviation from which takes a special effort. Along similar lines, Harold Koh and the transnational legal process school claim that international law acquires a certain “stickiness” through a process of interaction, interpretation, and internalization in domestic legal, political, and bureaucratic systems. 18 In this way, the law becomes “sticky” – states can pull out of a treaty or institution, but they tend not to do so lightly or without considerable disruption to their normal international relations. This “stickiness” will not stop powerful states from engaging in cyberwarfare if they decide it is in their national security interest to do so, but as cyber norms become entrenched in international and domestic systems, they may inhibit the casual launching of cyberattacks by even the most powerful states. If a low-level government official feels such an attack is necessary, the burden of persuasion would be on him or her to make the case for violation of a widely-accepted norm.

The Chayeses also argue that non-compliance with a treaty is often not willful but rather due to lack of state capacity or insufficient information about

16 Finnemore and Hollis, “Beyond Naming and Shaming,” 969–1003.
the treaty requirements. Beyond financial assistance, technical, legislative, and institutional capacity-building may be offered as a reward. This is common in many areas of international life – peacebuilding, global health, nuclear non-proliferation, human rights. In the cyber realm, a cottage industry is developing around the idea of building cyber capacity in “cyber have-not” states, both as a matter of equitable development and as a way of building secure and resilient cyber systems.\textsuperscript{19} Information provided by a state or non-state actor can also serve as a reward. This could be information about cyber threats and system vulnerabilities. It can come in the form of classified intelligence or public but not widely known facts. Relieving a state of the burden of gathering information itself can be proffered as a reward, perhaps through granting access to data and expertise that resides in a credible international organization, such as the International Atomic Energy Agency (in the nuclear realm) or World Health Organization (in the health field).

The Chayeses also suggest that compliance can be improved through creation of mechanisms for clarification and authoritative interpretation of the norm, whether by a court, committee or even the secretariat of an international organization. This is highly relevant to cybersecurity, where there is considerable confusion about the applicability of general international law and about which norms are binding and which are not. Moreover, many non-state actors, including those in the cyber industry, have little knowledge of the norms being discussed at the UN and in other international organizations. Industry understands the language of standards, security baselines, security controls, and good practices, but not necessarily how these correlate with international law.\textsuperscript{20}

**Legal and Diplomatic Discourse**

Legal discourse is not a separate model or theory of compliance, but rather a mechanism through which some of the penalties and rewards are meted out. Following the Chayeses, Thomas Franck, Harold Koh, Jutta Brunnée and others, I have argued elsewhere that the law operates in part through

\textsuperscript{19} The Global Forum on Cyber Expertise was established primarily to coordinate cyber capacity-building efforts. Capacity-building is among the OSCE’s Confidence-Building Measures. It is also among the “preventive measures” in the EU’s Cyber Diplomacy Toolbox. Reports coming out of the UN GGE, Open-Ended Working Group (OEWG), the GCSC, and the French-led proposal for a new “Program for Advancing Responsible State Behavior” all call for capacity-building. The Final Report of the UN GGE lists areas in which more capacity-building is needed.

\textsuperscript{20} I am grateful to Anastasiya Kazakova for this observation.
Implementing cybersecurity norms is a process of justificatory discourse. States feel compelled to give reasons and justifications for their conduct; these justifications are reviewed and critiqued in various settings, including international institutions. The felt need to have these justifications accepted pushes them in the direction of compliance because, being bound up in an interdependent international system, they want to remain members in good standing in that system – or at least in some of the legal regimes within it.

If the justificatory discourse leads to material sanctions and rewards, or produces reputational effects, its impact can be explained in rational choice terms. But the idea of “good standing” has another connotation, which relates to status. Social constructivist scholars posit that “back-patting” can reinforce a state’s identity and sense of self-worth, pushing the state in the direction of pro-norm behavior, unrelated to the material benefits that may accrue. (Reputational effects, by way of contrast, are tied to long-term material costs and benefits.) Importantly, the benefits of status depend on public affirmations of it, tied to the degree of identification a state feels (or wants to feel) with some reference group. The reference group need not be members of a formal intergovernmental organization (it could simply be “great powers,” for example), but institutionalization helps. International institutions are the social environment states inhabit, without which it would be harder to register social approval. They make acting in a particular way more public by creating a focused arena for observing behavior and for “naming and praising.” Conversely, “shaming” that diminishes one’s status in the eyes of a reference group may be felt as penalty in itself. The term “responsible state behavior” in cyberspace is indicative: governments do not like to be branded as irresponsible.

This theoretical perspective illuminates how penalties and rewards are dispensed through diplomatic relations. An official protest or démarche through diplomatic channels can serve as a penalty. Withdrawal of an

---

25 In its Cyber Diplomacy Toolbox, the EU lists statements of concern by the High Representative, démarches by EU delegations, and “EU Council Conclusions” among the “stability measures” it envisages in response to malicious cyber incidents. Council of the European Union General Secretariat, Draft Implementing Guidelines for the
ambassador is a common way of signaling displeasure, as is the expulsion of diplomats. Expulsion or suspension from an international organization is also possible if the rules of the organization permit it. Described in the literature as “outcasting,” 26 this can be a powerful diplomatic sanction. Conversely, diplomatic recognition or an upgrade in diplomatic relations is a reward. Even something as simple as an invitation to the White House in Washington D.C. (or Zhongnanhai in Beijing), or a bilateral meeting on the sidelines of the UN General Assembly, can be offered as a reward. Joining or re-joining an international organization, either formal (like the EU or UN) or informal (such as the G20) usually provides some tangible benefits, but simply being counted as a member of the club may serve as a reward in itself.

BUILDING A CYBERSECURITY REGIME: UNDERLYING CONSIDERATIONS

The multiple normative processes described elsewhere in this volume have produced a variety of norms, some at a high level of abstraction, others more technical. 27 Some count as hard binding law, some are widely accepted softer law, some are highly contested and clearly non-binding. Although they do not add up to a single, coherent cybersecurity regime, there is enough normative raw material to begin designing collective mechanisms for implementation (rather than relying entirely on unilateral, self-help measures). Indeed, doing so can lead to further development of the norms. In many legal fields, once norms have been established, state and non-state actors adopt and act on them in different ways, at different paces, to different degrees. They may even disagree on whether the norms are binding. An intersubjective process of interpretation kicks in, a collective – although often contested – search for meaning. The interpretation occurs not only in courts but also in the political organs of intergovernmental organizations, quasi-judicial committees, legislatures, bilateral diplomatic exchanges, industry and academic conferences, mainstream and social media, and other forms of public discourse. 28 This diffuse process may eventually lead to the adoption of a comprehensive, precisely worded, enforceable treaty with aspirations of universal adherence. But that need not be the starting point. Nor, for that matter, should it necessarily


27 Carnegie Endowment of International Peace, “Cyber Norms Index and Timeline.”

be the end point. In the cyber realm, the Global Commission for Stability in Cyberspace argues for a flexible approach, allowing states to embrace some norms and not others. A more flexible, adaptable approach could mix hard law, softer commitments, confidence-building measures, voluntary restraints among like-minded states, codes of conduct, industry standards, and an inventory of best practices. Indeed, that is essentially what the constellation of cybersecurity norms looks like today.

In this section, I set out three factors that complicate any attempt to move beyond the articulation of norms to the design of implementation mechanisms in the cybersecurity realm. While these factors look like obstacles, identifying them helps point the way to a politically realistic if not entirely “rational” institutional design. The practical challenge is not to envision an ideal cybersecurity regime and hope it can be built when the political conditions are right, but to determine what is achievable in light of prevailing political conditions and build from there.

First, the distribution of power and ideological differences matter. The US and Russia may share a broad interest in ensuring that low-level cyberattacks do not escalate into full-scale war, but that does not translate into shared views on how to limit the use of cyber technology. The US and China have been able to reach an agreement on cyber espionage for commercial purposes, but they disagree on many other aspects of cyber relations. Great powers respond to different incentives than lesser powers: what induces Estonia to comply with cybersecurity norms may not induce Russia, China or the United States. Moreover, there is wide disparity in the ability of states to impose penalties and bestow rewards unilaterally. Estonia could not launch countermeasures against

---

31 In that spirit, the OSCE has been in the forefront of cyber confidence-building measures. Organization for Security and Co-operation in Europe – OSCE Permanent Council, Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, March 10, 2016, https://www.osce.org/pc/227281?download=true.
Russia in response to the denial-of-service attack in 2007. Some countries are much better placed to provide cyber capacity-building assistance than others.

More generally, states start from different ideological assumptions about what cybersecurity really means. For the US and like-minded states, the starting point is the free flow of information and the ability to protect technology which enables that. For Russia and China, the starting point is information security and cyber sovereignty, which appears to include the ability to control online activity and content. In authoritarian states, the economic benefits of cyber technology may be outweighed by threats to the security of the governing regime. In democratic states, the appropriate trade-off between security and privacy is contested. These ideological differences, moreover, go beyond great power rivalry. Southeast Asian states, for example, have struggled to agree on cyber norms because of the diversity of their membership – some are democratic, some authoritarian; some are economically advanced, others much less so. Moreover, the populist backlash in many states (including democratic ones) translates into suspicion of “legalist” solutions to global problems, of what are seen as self-serving elites and self-designated experts, and of multilateralism generally. In an environment where populist and nationalist impulses are on the rise, international regime-building on any issue is a challenge.

Second, capacity and interests matter. The level of “cyber maturity” of countries – measured by the sophistication of cyber infrastructure, digital economic dependence, and information security – falls on a wide spectrum. Borrowing language from the nuclear context, the world is full of “cyber haves” and “cyber have-nots”; where one falls on the spectrum has an impact on one’s attitude towards the development of cybersecurity norms. Cyber haves (and the digitally connected) will be motivated by a different set of incentives from the cyber have-nots. They may also bring different attitudes towards the relative merits of precise, hard law versus ambiguous soft law. Arguably, states with the most cyber capacity benefit from a lack of precision and bindingness of the

---

34 International law does not permit collective countermeasures, but Estonia, among others, has argued that should be allowed by law.
35 Grigsby, “The End of Cyber Norms.”
norms. On the other hand, they may also be the most vulnerable to attacks, suggesting they would benefit from greater transparency.

When one adds non-state actors to the equation, the situation gets even more complicated. Some have an interest in greater international governance of the cyber realm; others benefit from a lack of regulation. ICT companies have an important role to play in developing and implementing norms, but it is not easy to integrate them into existing legal structures. Nor is it necessarily desirable for non-states actors with profit motives to lead in building a cybersecurity regime. Even not-for-profit actors (philanthropies, NGOs) have particular agendas and are not well-equipped to weighing the sort of trade-offs that governments must make. Because non-state actors, both for-profit or not-for-profit, have different interests in cyber regulation from each other and from governments, it may not be possible to build a one-size fits all cybersecurity regime. The implementation mechanisms will have to vary depending on the interests of the different actors involved. Some rewards, such as offers of financial and capacity-building assistance, will have little impact on the US, Russia, China or Iran (they already have great cyber capacity). But they may respond to collective economic sanctions (applying the enforcement model) or even naming and shaming. Less coercive implementation mechanisms may be both more effective and normatively preferable when applied to lesser powers and “cyber have-nots” if the goal is to build an inclusive regime.

Third, multiple institutional forms are possible. The traditional model of global governance is intergovernmental (i.e. state-based), universal, and formal. The archetype is a treaty negotiated in an international organization or ad hoc conference, the goal of which is universal participation, whose implementation is overseen by a monitoring agency and/or has built into it a formal dispute settlement mechanism. The Nuclear Non-Proliferation Treaty and WTO law are examples. Some regional organizations have already been successful in developing binding cyber norms (the Council of Europe and the European Union).

Another form of intergovernmental cooperation is so-called “plurilateral arrangements,” informal groupings of either like-minded or not-so-like-minded states. The G7 and Five Eyes are examples of the first. The G20 and Nuclear Suppliers Group are examples of the second. The BRICS countries (Brazil, India, China, South Africa, Brazil, India, China, South Africa)
Russia, India, China, and South Africa) fall somewhere in between. Typically, these groupings do not have any institutional machinery, but they may have a formal association with an existing organization. While forming clubs of like-minded states may seem like a more promising route than universality, it runs the risk of framing the enterprise as “good-guys” versus “bad-guys,” forcing states and non-state actors to pick sides, which can be counter-productive. And it is not at all clear which side the fence-sitters would choose. The US is not the only “norm entrepreneur” in this field. Russia has received broad support in its push for a binding treaty and other instruments for codifying ICT norms. China has been using the Shanghai Cooperation Organization and other fora to build support for tighter control of the dissemination of information online.

A third institutional form is transgovernmental networks. These are networks of sub-state public authorities that interact with their counterparts in other countries. The network can be quite institutionalized, for example, the Basel Committee on Banking Supervision, composed of central banks and banking supervisors. Or it can be a looser association, such as cooperative arrangements among law enforcement agencies.

When non-governmental actors are brought into the mix, we see true multistakeholder institutions. This form brings together some combination of international organizations, national governments, sub-state governmental actors, businesses, civil society, technical experts, think-tanks, academics, and philanthropies. The Vaccine Alliance (GAVI) is an oft-cited example of a success story at the global level. The Internet Corporation for Assigned Names and Numbers is an example from the cyber domain. Smaller multistakeholder groupings of like-minded states and other actors can also be

---

42 A defining feature of informal intergovernmental organizations is that they lack a permanent Secretariat. See Felicity Vabulas and Duncan Snidal, “Organization Without Delegation: Informal Intergovernmental Organizations (IIGOs) and the Spectrum of Intergovernmental Arrangements,” The Review of International Organizations 8, no. 2 (2013): 193–220.


formed. The Global Commission on the Stability of Cyberspace (GCSC) calls these “communities of interest.”

These institutional forms are not mutually exclusive. We already seem to be moving in the direction of a regime complex, defined above as “an array of partially overlapping and nonhierarchical institutions that includes more than one international agreement or authority.” Collective mechanisms for cybersecurity norm implementation include the instruments associated with the EU Cyber Diplomacy Toolbox and the Organization for Security and Cooperation in Europe’s confidence-building measures, the International Telecommunications Union, UNIDIR’s Cyber Policy Portal, the Global Forum on Cyber Expertise, the CyberPeace Institute, the Cyber Threat Alliance, and the various plurilateral arrangements mentioned above. It would be easier politically to build on the complex of institutions that already exist than to start again from scratch.

BUILDING A CYBERSECURITY REGIME: IMPLEMENTATION MECHANISMS

Within the various institutional forms listed above, many devices have been used for rewarding and penalizing in different international regimes. Below I cluster the mechanisms or devices into five categories that are most pertinent to cybersecurity: information-sharing and dialogue; monitoring and attribution; financial and capacity-building assistance; dispute settlement; and collective sanctions. The mechanisms are presented in ascending order of intrusiveness into sovereign prerogatives, with the first being the least intrusive and entailing the lowest level of sovereignty costs. For each category, I begin with a generic description of the mechanisms, illustrated with examples that currently exist in the cyber realm and from other regimes. I then make concrete – albeit speculative – recommendations as to which devices hold the most promise as short and longer-term steps in constructing a cybersecurity regime.

47 Global Commission on the Stability of Cyberspace, “Advancing Cyberability.”

Information-sharing and Dialogue

*Information sharing* is a non-intrusive mechanism for norm implementation. In the cybersecurity realm, it can enable better cooperation on prevention and response, and reduce suspicions about behavior.\(^{49}\) The most valuable information is about cyber threats. The most contested is the disclosure of vulnerabilities.\(^{50}\) Other types of information that can usefully be shared are security standards and information about the consequences of a cyberattack.\(^{51}\) The EU has begun to institutionalize this through its EU Cybersecurity Strategy of 2020, which calls on private companies, public institutions and national authorities to systematically and comprehensively share information on cyber incidents.\(^{52}\)

Another valuable kind of information sharing is best practices in building cyber resilience and security. The publication of best practices can encourage compliance not only by demonstrating what is possible and cost-efficient but also by providing models that other states can “mimic.”\(^{53}\) The intended effect is to ratchet up compliance with norms, while also giving content to and thereby “hardening” them through emulation rather than coercion. Institutionalized information-sharing is a way of meting out rewards: states (or non-state actors) that join the regime – the “club,” so to speak – are given access to the information. Conversely, it can serve as a penalty by denying access to information to those who do not join the regime or who join but then violate its norms.\(^{54}\)

---


\(^{50}\) The final report of the UN GGE prioritized “the responsible reporting of vulnerabilities.”

\(^{51}\) Joseph Nye argues that fear of unintended consequences can lead states to restrain non-states actors that they might otherwise let loose. Nye, “Normative Restraints,” 14.


\(^{54}\) In their proposal for a cyber treaty, Hathaway et al would include an agreement to share cyber-related information with other member states and deny it to non-members or those who fail to comply (out-casting). Oona Hathaway et al, “The Law of Cyber Attack,” *California Law Review* 100, no. 4 (2012): 817–886, at 883. See also William...
State self-reporting to an international organization is a more intrusive information-sharing mechanism if it entails a legal obligation to do so. Because states are more likely to pat themselves on the back and exaggerate their accomplishments than to engage in self-flagellation, this may seem like an ineffective compliance mechanism. Indeed, self-reporting does not work well when the parties have an incentive to lie because others tend to be suspicious about the accuracy of the reports. Yet there is substantial evidence that it is effective in the human rights realm, and it is a common feature of environmental agreements, including the Paris Agreement on climate change. It is wrong to assume the principal motive of all states is to avoid complying with the norms they commit to. The opposite may be truer: many states want to live up to the commitments they make and want to be seen to do so. Self-reporting – to the extent that it is public and therefore subject to scrutiny – enables them to put their “good” behavior on display. In the cyber realm, states may well have an interest in self-reporting on the due diligence steps they have taken to ensure non-state actors do not engage in cyberattacks. The reward is the reputational and status benefits they accrue, as well as perhaps capacity-building assistance (see below).

Closely related to self-reporting and information-sharing are mechanisms for constructive dialogue. The UN human rights treaty bodies are an example. They rely first on persuasion, and only secondarily on naming and shaming. When reports are submitted, Committee members can ask questions, seek clarifications, and request additional information. Sometimes the questioning is tough, but the idea is to foster a spirit of constructive dialogue, not to embarrass states at that stage of the proceedings. The EU Cyber Diplomacy Toolbox includes political and thematic dialogues in its toolbox of “cooperative measures.” These dialogues can signal the seriousness of a situation, facilitate peaceful resolution of an ongoing incident, or generate assistance to mitigate a situation.


What more can be done to institutionalize information-sharing and dialogue in the cyber realm?

• Establish a multistakeholder mechanism, initially among like-minded states and non-state actors among whom a modicum of trust exists. The principal function of the mechanism would be to share information about cyber threats and technological breakthroughs in how to address those threats. Over time, a culture of self-reporting should be cultivated, encouraging states and non-state actors to report on steps they have taken to address vulnerabilities. An inventory of best practices could be compiled, with the multistakeholder mechanism serving as a clearinghouse for information and expertise, as well as a venue for constructive dialogue.

• As this mechanism establishes its credibility and demonstrates value, it could be expanded to include other states and non-state actors, offering access to the information as a reward for committing to a specified set of cybersecurity norms. This would hold little appeal for states who see the mechanism as a “club” of adversaries, but it could draw in those who are sitting on the fence – especially the “cyber have-nots” who are starting to build capacity. It would bring them into the regime, providing the opportunity to engage in the further development of norms and implementation mechanisms.

Monitoring and Attribution

Monitoring mechanisms can foster compliance, even if not followed by enforcement. They are a common feature of treaty regimes, although far from universal. They tend to be more intrusive than self-reporting because a third party is empowered to assess the quality of the reports and to gather informa-

---


60 In her authoritative study of 146 treaties, Barbara Koremenos found that 60 per cent included monitoring provisions. They are common in disarmament and human rights treaties, and uncommon in financial and investment treaties. Koremenos, The Continent of International Law 262.
tion on its own. They provide transparency and impact compliance through the latent potential to “shame.”

Formal, intergovernmental monitoring mechanisms come in many forms. Some are ad hoc, such as human rights fact-finding commissions and expert panels that monitor sanctions regimes. Others are permanent, such as the Special Rapporteurs for human rights, and inspection agencies like the International Atomic Energy Agency (IAEA) and Organization for the Prohibition of Chemical Weapons. Occasionally non-governmental organizations are assigned a formal monitoring role in a treaty regime – the International Committee of the Red Cross for the Geneva Conventions being the best example. More common is when NGOs play an informal monitoring role. In the human rights realm, NGOs are not given a formal mandate by the intergovernmental organizations, but their reports are considered by the UN Human Rights Council, UN treaty committees, the Inter-American Commission on Human Rights and other bodies. The parties to human rights treaties know well that NGOs play this role, even if they do not always approve of it, and so may adjust their behavior in anticipation of a negative judgment – or perhaps hoping for the reward of a positive judgment. Moreover, even without any direct association with an intergovernmental organization (IGO), NGO monitoring can be a powerful tool for mobilizing shame. Interestingly, in the disarmament realm, clusters of NGOs have reached explicit agreements to monitor some treaties together.61

A mechanism that has proven to have an impact on the implementation of norms in domains other than cyber is indices and rankings. There is a growing body of literature on “governance by indicators,” both supportive and critical.62 These rankings are a form of social influence that can operate as both a penalty and a reward: in terms of status, a low ranking is a penalty, a high ranking is a reward. From the point of view of institutional design, much turns on the credibility of the entity doing the ranking. That credibility, in turn, depends on a variety of factors, including expertise, impartiality, and access to data. Examples are the World Bank’s Good Governance and Rule of Law indicators and the UNDP’s Human Development Index. Non-governmental actors also produce these rankings, for example, Transparency International’s corruption

indicators and the Fund for Peace’s Fragile States index. The International Telecommunications Union produces the Global Cybersecurity Index, which assesses countries along five pillars: (i) legal measures, (ii) technical measures, (iii) organizational measures, (iv) capacity development, and (v) cooperation.

In the cyber realm, the *attribution* challenge is both the most important reason for effective monitoring and the biggest obstacle to it. Public attribution is a form of naming and shaming – a way to punish the perpetrator (by extracting reputational costs) and to deter others. Individual attribution (i.e. by a single state or non-state actor that has been the victim of an attack) is always possible but has several limitations as a compliance mechanism. First, the injured party may have an incentive to lie – especially a state that is in a hostile relationship with the alleged perpetrator. Second, the injured party may be reluctant to reveal the intelligence on which the attribution is based. Third, the injured party may not have the capacity to make a credible attribution. All three factors are further complicated by the fact that the law of attribution is uncertain, especially in the cyber realm. As a matter of law, it is accepted that one need not prove a state is directly responsible for an attack that emanated from its territory – it is enough to show that the state failed to exercise due diligence.63 But precisely what due diligence requires is unclear, as is the burden of proof.64 Also, if countermeasures are contemplated in response, timing of the attribution is an issue: if one acts too soon, before solid evidence of state complicity is uncovered, the countermeasure could be illegal; if one acts too late, the countermeasure may be regarded as “punitive” and illegal for that reason.65

The limitations of unilateral attribution suggest there is value in devising institutional arrangements for either coordinated or third-party public attribution. Coordinated attribution is when a group of states collectively calls out a wrongdoer. The Five Eyes, plus Japan and Denmark, collectively attributed the WannaCry attack to North Korea. Essentially the same group (plus Ukraine, minus Japan) coordinated their attribution of NotPetya to the Russian military. Brad Smith, CEO of Microsoft, called for more of this in his blog following the SolarWinds attack.66 An advantage of coordinated public attribu-

---

Implementing cybersecurity norms

Implementing cybersecurity norms is that it adds credibility to the pronouncement. A second advantage is that it enhances the reputational or status impact, on the assumption that states care more about being called out by a large group than by one state. A third advantage, according to Florian Egloff, is that coordinated public attributions “shape the operational and normative environment.” He explains that the motivation for the UK’s systematic effort to orchestrate the response to WannaCry was to demarcate clear lines of unacceptable or “irresponsible” behavior. The more states involved in that demarcation, the more it contributes the norm shaping and hardening process.

A more ambitious approach to collective attribution would be to establish an attribution organization. The CyberPeace Institute, founded by Microsoft, the Hewlett Foundation, and Mastercard, is a non-governmental example. Its mandate includes the analysis of attacks, their impacts, and how they violate international law. While it seemed to refrain from public attribution in its early years, after Russia’s invasion of Ukraine in 2022, it launched a platform that identifies the source of attacks there on a sliding scale of certainty. A Rand Study proposes a “consortium” of 30–40 independent cybersecurity experts (not associated with their governments) from around the world that would investigate and publicly communicate who was responsible for a cyber incident and how confident they are in that assessment. How to respond to the findings (whether through enforcement or in some other way) would be left to governments and other actors.

Establishing an intergovernmental attribution organization is a more daunting prospect. While states tend to view “political” (as opposed to technical) attribution as the prerogative of governments, the political will to institutionalize this in a permanent organization at the global level does not exist. A regional attribution organization is a more realistic possibility. The EU leaves cyber-attribution to member states, but there have been proposals to

---


68 On its website, the CyberPeace Institute describes one of its functions as aggregating and analyzing “data about cyberattacks from a wide range of public and restricted sources in order to assess the type of threats, the threat actors and their tactics (modus operandi), and to assess whether victims can be identified.” “Analyzing Cyberattacks,” CyberPeace Institute, accessed September 26, 2022, https://cyberpeaceinstitute.org/analyzing-cyberattacks/


empower the EU to do so by qualified majority vote. Another option would be for an IGO, such as the UN Security Council, to establish an ad hoc institution to address a particular incident or the cyber behavior of a particular state or non-state actor. The UN Security Council did this for Iraq’s chemical, biological and ballistic missile weapons (UNSCOM, then UNMOVIC) after the Gulf War. Such an international entity would help to resolve one of the problems with attribution noted above: intelligence. States provided intelligence to UNSCOM on a confidential basis.

From the point of view of legitimacy and effectiveness, a multistakeholder attribution organization comprised of governmental, intergovernmental and non-governmental (for-profit and non-profit) actors makes sense. It would combine the authority of governments, with the expertise of the ICT community and the legitimacy of civil society participation. On the other hand, the diverging interests among the stakeholders both about the political impact of “naming” and the consequences that might follow would make it difficult to reach consensus on a particular attribution. In any case, the current geopolitical climate is even less conducive to establishing a multistakeholder organization than a purely intergovernmental one.

What ideas hold the most promise for the short and long term?

• An international collection of non-governmental organizations could form a monitoring organization that includes independent technical experts, ICT industry representatives and civil society representatives. The organization should monitor state and non-state actors, primarily to assess their performance against agreed cybersecurity norms. It should also develop indicators and ranking for cyber due diligence, to complement the ITU’s index. All findings should be public so that states and intergovernmental organizations can use them as the basis for constructive dialogue as well as naming and praising or shaming.

• Separately, a non-governmental attribution organization should be established, staffed by independent technical experts and highly respected former government and intergovernmental officials from around the world. Its sole purpose would be to analyze and identify sources of cyberattacks, making clear the degree of certainty it has in the attribution. This would build on the informal exchange of intelligence and information that already takes place within the cybersecurity research and technical community.

• Meanwhile, a core of like-minded states should establish mechanisms for coordinated attribution. As the norms solidify and the politics of attribution become less fraught, this core should expand to other states, including the

71 Bendiek and Shulze, “Challenge for EU Cyber Sanctions.”
Implementing cybersecurity norms

“non-like-minded” who nevertheless have an interest in minimizing the dangers of cyberattacks.

- Eventually, if coordinated attribution becomes standard, it may be possible to convert this informal grouping of states into a formal intergovernmental organization, similar to the IAEA. Governed by member states, expertise would reside within the Secretariat, but it would draw on information/intelligence provided by other stakeholders, both governmental and non-governmental.

Financial and Capacity-building Assistance

Mechanisms for channeling financial assistance are another feature of global governance in many realms: development, the environment, humanitarian action, health, and peacebuilding. In addition to bilateral state-to-state assistance, intergovernmental organizations often serve as mechanisms for pooling resources and distributing them equitably (if not always efficiently). Short of pooling resources, “clearinghouse” mechanisms can be established whereby an intergovernmental organization or some other third party seeks to match donor funding with recipient needs. Private sector investment is less susceptible to collective action, but there are examples of philanthropies and corporations cooperating to meet global public policy goals – for example, COVAX, the mechanism set up to fund equitable access to the COVID-19 vaccines.

Institutionalized mechanisms for technical, legislative, and other capacity-building assistance can also be valuable. The main purpose of such assistance in the cyber realm is to build resilience against cyber threats and the ability to respond effectively. An equally important purpose, which relates directly to regime building, is to bridge the digital divide. The Global Commission on Stability in Cyberspace observes that states with capacity are more likely to be effective in supporting and promoting norms. The final report of the latest UN Group of Governmental Experts lists areas where capacity-building is needed, to enhance the capacity of computer emergency response teams, to improve the security of critical infrastructure, and to build capacities to detect, investigate and resolve ICT incidents. Andrea Calderaro and Anthony Craig add another dimension of capacity-building: training in cyber diplomacy to enable countries of the Global South to become active

---

72 For example, the Counter-Terrorism Committee established by UN Security Council resolution 1373, on the suppression of financing of terrorism.

73 Global Commission on the Stability of Cyberspace, “Advancing Cyberstability.”
Building an international cybersecurity regime

players in the development of a “coherent and coordinated transnational governance approach to cybersecurity.”

There are models for this in the weapons of mass destruction (WMD) regimes. The Nuclear Non-Proliferation Treaty (NPT), the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC) all offer technical assistance as a reward for compliance. In the case of the NPT, the reward is assistance in developing peaceful nuclear energy, facilitated by the IAEA. The BWC lacks a verification agency, but assistance in the development of biological agents for peaceful purposes is provided on an ad hoc basis by parties to the Treaty. For the CWC, the assistance takes the form of protective measures against chemical weapons, including equipment, decontaminants, and advice. This is overseen by the Organization for the Prohibition of Chemical Weapons.

While the UN, ITU and other intergovernmental organizations have programs aimed at “bridging the digital divide,” there is no dedicated cybersecurity IGO. However, a multistakeholder approach to cyber capacity-building has begun to emerge. The Global Forum on Cyber Expertise is an NGO whose mission is “building cyber capacity to strengthen cyber resilience through developing skills and capacities that address threats and vulnerabilities.” It does this by coordinating regional and global capacity projects, involving governments, civil society, and private sector – functioning as a clearinghouse to match needs with offers of support. Some 60 countries, eight IGOs, and many private companies, NGOs and think-tanks are members or partners.

How can these efforts be built on?

- To expand multistakeholder efforts to match capacity-building resources with needs, a government or group of like-minded governments could convene a “cybersecurity summit.” Analogous to the series of nuclear security summits from 2010 to 2016 convened to address the danger of fissile material being stolen, the purpose would be to share expertise on

---


75 Implementation of the Article X of the BWC is a matter of discussion at the periodic review conferences, and proposals have been made to introduce a peer review mechanism, whereby parties report on what they have done, and other parties examine and comment on those reports. James Revill et al, “Options for International Cooperation Under Article X of the BWC,” Trust and Verify 154 (2016): 1–6.

Implementing cybersecurity norms

detection and domestic enforcement of cybersecurity laws, as well as the development of new technologies, in consultation with the ICT industry.\(^77\)

- In the longer term and with the goal of moving beyond the club model, the UN Security Council could adopt a resolution similar to the “quasi-legislative” resolutions designed to suppress the financing of and other forms of support for terrorism,\(^78\) and to prevent weapons of mass destruction from falling into the hands of non-state actors.\(^79\) The regimes produced by those resolutions continue to this day, an important function of which is to serve as a clearinghouse for resources and expert assistance.

- Capacity-building is usually discussed in terms of state-to-state assistance, but states can and should also assist non-state actors. The Swiss Federal Department of Foreign Affairs does this through the Geneva Dialogue, which gathers industry partners to discuss aspects of digital security, who are also invited to take a cyber diplomacy course aimed at helping them to become more adept in diplomatic negotiations.\(^80\) Other states should consider similar initiatives.

- Any cybersecurity capacity-building initiatives should be connected to broader development-oriented initiatives to bridge the digital divide. In this way, digital assistance of all sorts (not just for cybersecurity) can be used as a reward to incentivize “good” cyber behavior and to build a globally inclusive cybersecurity regime.

Dispute Settlement

_Peaceful dispute settlement_ mechanisms range from dialogue and consultation, to third party good offices and mediation, to arbitration and adjudication. Consistent with the managerial model of compliance, disputes can sometimes be resolved through dialogue in which the meaning of the norm is clarified and reasons for non-compliance are explored. “Good offices” is a loosely defined term (typically associated with the UN Secretary-General), which refers to informal diplomatic action to help prevent, manage, or resolve a conflict. Slightly more formal is “mediation,” in which a neutral third party helps

---

\(^77\) These were elements of the First Nuclear Summit (2010) outcome document.


\(^80\) “The Geneva Dialogue on Responsible Behavior in Cyberspace,” accessed September 29, 2022, www.genevadialogue.ch. I would like to thank Anastasiya Kazakova for drawing this to my attention in her comments on a draft of this chapter.
the parties to a dispute to resolve their differences without rendering a decision. Arbitration is a quasi-judicial dispute settlement mechanism, in which a neutral individual or panel chosen by the parties makes a decision about the dispute after receiving evidence and hearing arguments. In adjudication, a court renders a decision based on the prevailing law.

Today, cybersecurity disputes tend to be settled through diplomacy or not at all. There is no dedicated mechanism for formal dispute settlement, other than for those that arise under the Budapest Convention. However, the UN Charter (and the constitutive acts of many regional organizations) provide for generic dispute settlement procedures. Article 33(1) calls on parties to a dispute to seek a solution first by “negotiation, enquiry, mediation, conciliation, arbitration, [or] judicial dispute settlement.” Article 33(2) empowers the Security Council to call on parties to use such means. Articles 98 and 99 have been interpreted to give the Secretary-General substantial independent authority to engage in fact-finding and mediate disputes.81

In principle, a cyberattack dispute could be submitted to the International Court of Justice or some other court of general jurisdiction, but that is unlikely. There have been proposals for the creation of a specialized cyber court to deal with government-level cyber conflicts,82 or an “attribution and adjudication council” for cyber operations alleged to constitute an “armed attack.”83 One advantage of such formalized dispute resolution is that it can impose reputational costs (as well as monetary damages) in ways that less formal dispute settlement mechanisms, by design, cannot. It does not appear, however, that the political will for this exists among states and non-state actors that are likely to be involved in cyber disputes.

What more can be done to institutionalize peaceful cyber dispute settlement?

- Adopt a UN General Assembly resolution that calls for member states to invoke the peaceful settlement mechanisms set out in the UN Charter to resolve cyber disputes, including disputes about attribution. Similar appeals could be made by the plenary organs of regional organizations.
- Establish dedicated cyber offices in intergovernmental organizations, whose principal task is to offer informal dispute settlement services, such as good offices, or facilitated dialogue. As necessary, the head of the

organization could appoint a Special Representative to lead the effort, with support from the dedicated offices.

Collective Sanctioning Mechanisms

As noted in the second section, states can and often do act unilaterally in response to violations of international law, but collective sanctioning mechanisms are rare. The UN Security Council can impose sanctions on a state, individual leaders, or a non-state actor. Its authority to do so is based partly on treaties (for example, the NPT, CWC and BWC) but mainly on its inherent authority to maintain international peace and security. The EU often imposes economic sanctions on states, and it recently started sanctioning individuals for cyberattacks. The African Union also has the capacity to impose sanctions. A feature of these mechanisms is that they require consensus among the five permanent members of the Security Council in the case of the UN and among all members in the case of the EU. The African Union can impose sanctions by a majority vote, but it normally operates by consensus.

Countermeasures are seen by some as a more promising tool for imposing penalties than IGO sanctions. The law of countermeasures, as it stands, restricts that right to the victim of a cyberattack. Estonia has proposed that collective countermeasures ought to be legal, to make up for the fact that the capacity of some states to inflict a proportionate (and impactful) response is limited. Given the reluctance of the states to endorse collective countermeasures generally, it is unlikely that this will crystallize as customary law in the cyber domain any time soon. More politically feasible is a collective mechanism for assessing whether individual countermeasures meet the requirements of international law. The EU Cyber Diplomacy Toolbox includes “support to member states that individually or collectively resort to responses in accord-

---

84 In the case of the NPT, Article III requires parties to adopt IAEA safeguards. The IAEA Statute stipulates it shall report violations of the safeguards to the Security Council.


86 That assessment would include whether the measures are proportionate (taking into account the gravity of the act and rights in question), whether they amount to the use of force, whether they violate human rights or any peremptory norms, and whether they are taken in a way that permits the perpetrator state to end the wrongful conduct. International Law Commission, Articles on State Responsibility, Chapter II, “Countermeasures” Articles 49–54.
ance with international law.” If the response is a countermeasure, then EU support for it would be tantamount to a judgment that the measure is legal.

“Shaming,” as has been discussed, is a sanction, which affects both reputation and status. The research on naming and shaming is inconclusive, but there is reason to believe it does have an impact in some situations. Circumstantial evidence in the human rights realm is the length to which states go to be elected to bodies like the UN Human Rights Council in order to avoid being “shamed” there. Similarly, major NGOs such as Human Rights Watch and Amnesty International must believe it has an impact, given the resources they invest in shaming states. They do so not only in the hope or expectation that the shaming will be followed by tangible consequences (such as the cutoff of aid, boycotts, or the threat of international criminal prosecution, etc.) but also because they believe the reputational and status costs themselves are a penalty.

What more can be done in the way of collective sanctioning for violation of cybersecurity norms?

• The measures suggested above about non-governmental and coordinated attribution can serve as a sanction. The sense of shame may be felt less acutely for non-binding norms than hard law but may nevertheless extract reputational costs. A more long-term objective would be to establish a dedicated IGO committee that would, in addition to monitoring and constructive dialogue, blacklist states for violating cyber law and norms (analogous to the UN human rights committees).

• Collective economic and diplomatic sanctions should be imposed by (i) groups of like-minded states and (ii) regional organizations. The first is already occurring and may be all that is possible in the short term, given geopolitical polarization. The problem is that it sets up an “us” versus “them” framework, which is as likely to exacerbate tension as it is to deter wrongdoers. Doing so through regional organizations may be seen as more legitimate because most are not composed entirely of like-minded states.

• The same is true for collective assessment of the legality of countermeasures. This could be institutionalized among groups of like-minded states and/or in regional organizations. For the reasons given above on collective sanctions, doing this through the latter is better for regime-building than the former, though more politically difficult.

• Finally, the UN Security Council can impose sanctions for cyberattacks, but, again, current geopolitical tensions make that unlikely and, in any case, would never be imposed against the P5. However, if and when tensions precipitated by the Ukraine war subside, the SC may be able to adopt

87 Schmitt, “International Law and Cyberspace.”
a thematic resolution on what sort of cyber incidents constitute a threat to international peace and security, along with an indication that the Council will take appropriate steps should violations occur.88

CONCLUSION

This chapter has argued for moving forward on building collective mechanisms for implementing cybersecurity norms, even as negotiating processes on the norms themselves continue. The case for collective mechanisms is rooted in legitimacy. A cybersecurity regime that depends entirely on unilateral or bilateral responses will suffer from legitimacy deficits because a “self-help” approach necessarily favors actors with the most power. Of course, even in the most multilateral and institutionalized regimes, power matters – and it should. The effective bestowal of rewards and penalties depends on the participation of the powerful. But other stakeholders – smaller states and non-state actors – have an interest in cybersecurity. If their interests are not accounted for in designing a regime, it will be perceived as illegitimate, and the powerful will have to rely more heavily on coercion. This is not only costly but also unstable, as military, economic and technological power balances shift. Already, the number of states with offensive cyber capabilities has grown to the point when no state can feel confident in its ability to manage the threat alone.89 This is not to say that unilateral measures, responses, and activities do not have a place. But the time is right to also work on expanding the range of collective mechanisms to promote cyber norm implementation.

In designing these mechanisms, both rewards and penalties should be considered. Penalties may be necessary, but when it comes to regime-building – seeking not only broad adherence but also progressive development of cybersecurity norms – rewards may be more effective. One obstacle to developing customary law in the cyber realm is that much state practice is secretive, mainly to protect intelligence sources.90 What implementation mechanisms can do is to shed as much light on practice as possible, and generate as much legal discourse as possible, so that opinio juris can emerge. Rewards are

88 The Security Council (SC) has adopted such resolutions on the “responsibility to protect” (SC resolution 1674, 28 April 2006, para. 26) against the proliferation of WMD (SC resolution 1887, 24 September 2009, para. 28) and foreign terrorist fighters (SC resolution 2178, 24 September 2014, paras 7 and 23(b).

89 At least 30 states now have the ability to use cyber tools as weapons. Banks, “International Law of Cyber Attribution,” 191.

more likely to do that than penalties because fear of penalties adds one more reason for states to hide their behavior and obfuscate norms that fall in a legal grey zone. Moreover, multistakeholder institutions may be more capable of dispensing rewards than penalties. While non-governmental actors can impose reputational sanctions in the form of shaming, they do not have the legal authority to impose material sanctions. Instead, they can provide information, financial assistance, expertise for capacity building and other material rewards.

What might those mechanisms look like? Geopolitical tensions suggest that seeking to construct a single, universal, coherent cybersecurity regime would be a fool’s errand. Instead, effort should be invested in building on the nascent steps that have already been taken in five areas: information sharing and dialogue; third party monitoring and attribution; financial and technical assistance; dispute settlement; and collective sanctions. This would not only make compliance with existing norms more likely, but also contribute to the consolidation and progressive development of those norms. Information sharing can help to identify best practices, which may themselves become legal obligations (for example, on due diligence). Collective attribution can help to demarcate clear lines of what constitutes “irresponsible” behavior in cyberspace. Clearinghouses for financial and technical assistance may become focal points for multistakeholder engagement in the development of norms – not through negotiation but through operational activities (a role the GFCE is currently playing). A habit of collective countermeasures could generate a pattern of international practice that crystallizes as customary law, as proposed by Estonia.

This incremental, practice-oriented approach is likely to create tensions and possibly even the fragmentation of the nascent cybersecurity regime. But a fragmented regime complex is not necessarily a bad thing. Multiple channels of influence are better than no channels, or than a single narrow channel that does not account for the complexity of the issue and multiplicity of stakeholders. Fragmentation that produces outright conflict, however, is problematic. The goal should be to design institutional arrangements that minimize those contradictions and conflicts, while seeking convergence (if not consolidation) over time, through practical experience and multistakeholder interaction.

---

ACKNOWLEDGMENT

The author would like to thank Anirudh Nanda and Lyndon Sam for their research assistance. He would also like to thank Anastasiya Kazakova, as well as his co-editors Arun Sukumar and Joel Trachtman, for comments on a draft of this chapter.
PART III

Country perspectives
6. U.S. multistakeholder engagement in cyber stability issues

Christopher Painter

INTRODUCTION

The U.S. government has a long history of championing multistakeholder involvement in a range of cyber and Internet policy issues. The clearest example of this has been in the area of Internet governance where the U.S. has been a forceful proponent of the private sector, civil society, academia, and the technical community working alongside governments – not subservient to them – in determining the technical aspects of how the Internet is run and governed. In the field of cybersecurity writ large, the U.S. has also recognized that other stakeholders, particularly the private sector, are essential and that the U.S. government cannot ensure cybersecurity on its own. This approach is grounded in the realization that the private sector owns and operates the large majority of the Internet and computer network infrastructure and that the private sector often has insight and capabilities that the government lacks – although, of course, the government brings its own set of capabilities and insights not available to the private sector. Although the U.S. government has been a leader in advancing an international stability framework globally, consultation with, and participation by, other stakeholders in that process has been less formal and more episodic than in larger cybersecurity or Internet governance debates.

This paper will first lay out some of the doctrinal statements made by the U.S. government on multistakeholder participation and cyber diplomacy over the last 20 years. It will then discuss the various U.S. stakeholders who have an interest in cyber norm and stability developments. A somewhat unique characteristic of U.S.-based stakeholders is that they are often global entities that seek to influence not just U.S. positions but the global debate. The paper will then discuss the nature of stakeholder interactions to date and some of the actual and perceived challenges to greater inclusion. Finally, the paper will propose a number of actions the U.S. can take to enhance interaction with other stakeholders both domestically and internationally, including creating
Building an international cybersecurity regime

a more formal model of stakeholder engagement to supplement existing informal engagement, closer collaboration on norm implementation and capacity building, and working together to increase accountability for bad actors. The increased priority that the Biden Administration is placing on cybersecurity issues coupled with recently announced structural changes with respect to cyber issues at the U.S. State Department create an opportunity for greater and more substantive multistakeholder interaction.

THE U.S. DOCTRINAL COMMITMENT TO MULTISTAKEHOLDER PARTICIPATION

For over 20 years, the U.S. government has extolled the virtues of multistakeholder participation in both operational issues and policymaking. In the 2003 U.S. Strategy for Securing Cyberspace, President Bush wrote: “[s]ecuring cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people.”¹ The strategy itself was focused on multistakeholder engagement.² The chapter on the international aspect of the strategy, conceived before norms and stability were a focus of international attention, focuses on industry as a stakeholder for more operational ends and to persuade other governments to prioritize cybersecurity.³

The Obama Administration’s 60-Day Cyberspace Policy Review (2009) took a broader view of multistakeholder engagement.⁴ The White House

¹ U.S. Strategy for Securing Cyberspace (2003), https://www.hsdl.org/?view&did=1040, Letter from the President (Foreword). He further noted that the strategy itself was based on multistakeholder participation: “ten town hall meetings were held around the Nation to gather input on the development of a national strategy. Thousands of people and numerous organizations participated in these town hall meetings and responded with comments.”

² “Public–private engagement is a key component of our Strategy to secure cyberspace. This is true for several reasons. Public–private partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public–private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.” Ibid at ix.

³ Ibid at 51.

⁴ Federal Communications Commission, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (CreateSpace Independent Publishing Platform, 2013), https://books.google.com/books?id=W8oCn-AEACAAJ. Like the Bush-era Strategy, the review team recognized “that there are opportunities for everyone – academia, industry, and government – to work together to build a trusted and resilient communications and information infrastructure,” and hun-
U.S. multistakeholder engagement in cyber stability issues

stated that “[e]nsuring that cyberspace is sufficiently resilient and trustworthy to support U.S. goals of economic growth, civil liberties and privacy protections, national security, and the continued advancement of global democratic institutions requires working with individuals, academia, industry, and governments.”

In 2011, the U.S. issued the International Strategy for Cyberspace, the first international cyber strategy created by any country. In discussing norms, the strategy focused on state-to-state interactions and building consensus among states rather than multistakeholder input. However, later in the document, in a section entitled “Strengthening Partnerships,” the Strategy gives a general endorsement of multistakeholder involvement: “[t]hrough our international relationships and affiliations, we will seek to ensure that as many stakeholders as possible are included in this vision of cyberspace precisely because of its economic, social, political, and security benefits. These efforts will be supported by meaningful collaboration with the private sector at home and abroad.”

The 2011 International Strategy also commits to work with multistakeholder organizations and states, stating that “we will work closely with infrastructure owners and operators – who are responsible for the majority of network functionality – to expand initiatives to secure the network ecosystem, preserve the benefits and character of cyberspace, avoid unnecessary impediments to technological evolution, and extend principles of peace and security.” In contrast to the largely state-centric language in the International Strategy when discussing international security issues, there is abundant language encouraging multistakeholder participation in Internet governance.

dreds of stakeholders and groups were consulted and provided input into the review.


7 Ibid at 12.

8 Ibid.

9 Ibid at 22. (“[t]he United States stands firm in our conviction that when the international community meets to discuss the range of Internet governance issues, these conversations must take place in a multistakeholder manner”).
In the 2016 International Cyberspace Policy Strategy report mandated by Congress,\(^\text{10}\) the State Department was more clear that other stakeholders would be engaged on norms issues, stating:

> [o]ur future work on voluntary norms will consist of political-level affirmation of defined norms in a range of regional and international venues; further expert-level identification and articulation of additional stability measures that can also contribute to stability in peacetime, including via the next UN Group of Governmental Experts (UN GGE) process; and more expansive awareness-raising and engagement with a large and diverse group of actors: states with emerging and established cyber capabilities; other potential like-minded states; the CSIRT community; academia; critical infrastructure owners and operators; and other industry partners.\(^\text{11}\)

During the Trump Administration, the State Department set out a number of goals, including advancing a framework of cyber stability (including voluntary norms) and deterrence. In a catch-all section dealing with all the State Department’s lines of effort, the report states: “U.S. government engagement to achieve these objectives takes a range of forms from direct diplomatic action, to include diplomacy and foreign assistance, and joint military exercises to participation in policy and technical standard-setting bodies alongside non-governmental stakeholders.”\(^\text{12}\) In the subsequent White House-issued National Cyber Strategy of the United States of America, non-government stakeholders, particularly the private sector, are mentioned in several areas, including with respect to countering disinformation, but are not named in the discussion of advancing norms or deterrence.\(^\text{13}\)

Overall, although the U.S. is a strong proponent of multistakeholder engagement more generally, most of the U.S. government doctrinal statements focus on technical Internet governance, operational collaboration (particularly with the private sector) and domestic policymaking with only a few references to such interactions with respect to norms and international security. The relative lack of focus on multistakeholder input or involvement in norms and stability

---


\(^{11}\) Ibid at 15.


negotiations is likely attributable, in part, to cyber stability being a relatively new priority issue of U.S. government focus. Moreover, stability issues grew out of a Russian resolution promoting a “cyber arms control” regime – traditionally a state-centric issue – and were largely being negotiated in the UN First Committee – a venue that was traditionally the province of states and not of other stakeholders. While those factors did not preclude multistakeholder input into norms negotiations, there was not as much of a history or stated imperative for those interactions as in other areas of cyber policymaking. More recently, however, the U.S. explicitly made strong statements in favor of non-state stakeholder participation in the latest UN First Committee negotiations of international security in cyberspace. The U.S. stated that “Multistakeholder participation is not simply a matter of principle; it’s also essential to our shared purpose. The vast majority of ICT infrastructure is owned and operated by the private sector, and it is non-governmental organizations that ensure the functioning of cyberspace. They play an integral role in implementing our decisions. And they bring valuable insight and expertise to bear on our discussions.”

GOVERNMENT, NGO AND PRIVATE SECTOR ACTORS RELEVANT TO CYBERSECURITY NORMS INITIATIVES

The U.S. is home to a wide range of actors relevant to the international cyber stability debate and related issues. Many of these entities, including think tanks and large companies, operate on an international level and participate in and seek to influence these discussions at both a domestic and international level. On the government side, the U.S. State Department’s former Office of the Coordinator for Cyber Issues (“S/CCI”) has led negotiations in the UN, regional forums such as the Organization for Security and Co-operation in Europe (“OSCE”) and the Organization of American States (“OAS”) and has provided thought leadership on norms and cyber stability issues. The U.S. government positions have been determined by interagency processes led by the National Security Council and State Department. Moreover, the S/CCI-led

---


delegations to the UN and various other forums often include representatives from these other agencies.

For over a decade, the U.S. has been a leader in advancing an international cyber stability framework that includes the application of international law, the acceptance of certain voluntary norms of responsible state behavior and the adoption and use of cyber confidence-building measures. The voluntary “peacetime” norms that the U.S. government primarily advocated were proscriptions from attacking the critical infrastructure of another country or attacking its cyber incident response and recovery teams (“CSIRTs”), and a norm of cooperation that urges countries to heed calls for assistance when malicious cyber activity is originating from the requested country. These “political–military norms” are voluntary rather than mandatory for a number of reasons, including the relative lack of maturity in the discussion of cyber capabilities and restraint, the need to assess unanticipated second-order effects, and the need to gain commitment and agreement both domestically and internationally on still novel issues. There is also the concern that binding norms are the gateway to a cyber treaty – long advocated by Russia and China – that would seek to control content including political dissent. Nevertheless, states agreeing to even voluntary norms evince a political commitment to follow them and a rallying point for other countries to seek accountability. The U.S. also took the lead in negotiating and advancing an economic stability norm – that no country should use cyber means to steal business intellectual property and trade secrets to benefit its commercial sector. More recently, the U.S. has taken the lead in advancing a “deterrence” initiative that seeks to work with other nations to build collective responses to cyber threats. With respect to both norms and to deterrence, a cornerstone of the U.S. efforts has been building like-minded partnerships with other countries.

Civil society participants include a plethora of U.S. think tanks and academic institutions that have been involved in the discussion of norms and international stability. These include, among many others, the Center for Strategic and International Studies (“CSIS”), The Council on Foreign Relations, The Carnegie Endowment for International Peace (“Carnegie”), New America Foundation, R Street Institute, Harvard’s Belfer Center, Tufts’ Fletcher School.

---

16 Ibid at 3-4, 12-16.
17 Ibid at 14-15.
and Temple University. The activities of these groups range from commentary to convening discussions on these topics to launching initiatives. Other U.S. non-governmental organizations are more specialized, including: Access Now, both a U.S. and a global organization, that focuses on promoting human rights; the Global Cyber Alliance, which specializes in promoting cybersecurity; the Forum of Incident Response and Security Teams (“FIRST”) (also a global organization) that focuses on strengthening computer incident response; and the Center for Democracy and Technology that focuses on privacy issues. The William and Flora Hewlett Foundation has also played an instrumental role in funding a number of academic and civil society organizations on various cyber policy issues and convening discussions on these issues.

The private sector is represented by both industry associations – such as the U.S. Council for International Business, the U.S. Chamber of Commerce, the Information Industry Technology Council, the Business Software Alliance, and the Cyber Threat Alliance – and by individual companies. By far, the one company that has been most active in cyber norm discussions for many years, both domestically and globally, has been Microsoft Corporation.

Microsoft broached the subject of norms as early as 2012 but devoted significant attention to this issue, including publishing several papers, following the 2013 Snowden disclosures concerning U.S. surveillance practices. Microsoft argued for the inclusion of the private sector in cyber stability discussions in 2013, stating: “Unlike the historical evolution of international norms, the development of “cybersecurity norms” should engage the private sector, which creates and operates most of the infrastructure that underpins the Internet.”

The company further articulated the need for a larger multistakeholder approach in 2014 stating:

The development of cybersecurity norms cannot be a niche foreign policy issue reserved for diplomats. Cybersecurity norms are an imperative for all users, governments, the private sector, non-governmental organizations (NGOs), and individuals, in an Internet-dependent world – each contributes to the peace, security, and sustained innovation of a globally interconnected society.

The company proposed a number of norms and was also instrumental in setting up other stakeholder platforms – including being a founding member and organizer of the Cybersecurity Tech Accord (“Tech Accord”), now comprising

---


Building an international cybersecurity regime

over 150 global tech companies, helping to launch the Paris Call for Trust and Security in Cyberspace (“Paris Call”), helping create the Cyber Peace Institute (“CPI”) and helping fund the Global Commission on the Stability of Cyberspace (“GCSC”).

In addition to individual actors, multistakeholder international initiatives contributing to the norms and stability discussion include the Paris Call and the GCSC. The Paris Call began as a statement and set of principles that was launched at the inaugural Paris Peace Forum in November 2018. The Principles included support of those agreed to by states in the UN as well as norms developed in other processes, such as the GCSC, and by the private sector. Currently, 81 states, 706 companies and 391 civil society representatives have signed on to and endorsed the call. The U.S. just recently joined the Paris Call.

Although the GCSC was an international body comprising former government, private sector and civil society representatives from over 16 countries around the globe, nine of its 28 commissioners, including this author, were from the U.S. Unlike the UN negotiations, the GCSC sought to examine the conduct of, and propose norms and recommendations for, both state and non-state actors. The Commission met for three years and produced a report that, among other things, recommended “establishing a standing multistakeholder engagement mechanism to address stability issues, one where states, the private sector (including the technical community) and civil society are adequately involved and consulted.”

INTERACTION OF STAKEHOLDERS

There are various kinds of interaction among stakeholder groups and individuals both among groups and between those groups and the U.S. government. In addition, several stakeholders interacted directly at the international level, including participating in UN and regional meetings or through other efforts such as the Paris Call.

---

24 Ibid.
Non-government Stakeholders

As noted earlier, think tanks and academic institutions have sponsored a number of events and published commentaries on a range of norm and cyber stability issues over the last decade. These events and commentary have ranged from norm negotiation and how to apply international law to accountability and deterrence. For example, New America published an entry-level explainer on norms. CSIS’s Jim Lewis has been a frequent commentator on norms processes and was involved in helping to draft the 2013 and 2015 UN GGE Reports. Carnegie launched an initiative on international cyber norms and their application to the financial sector and have conducted research and created a Cyber Norms Timeline and Index. Professor Joseph Nye and others at the Belfer Center have authored a number of commentaries on norms and cyber conflict. Although too numerous to fully list here, many organizations posted blogs, commentary or even longer articles discussing the various UN cyber processes and aspects of norms and accountability. And there was a plethora of meetings, seminars, speeches and other gatherings held by various non-government stakeholders that promoted interaction among stakeholders and often with the U.S. government.

Among private sector entities, Microsoft led in both quantity and variety of interactions both domestically and globally. First, Microsoft helped fund and support many of the think tank and conference efforts discussed above. The company has also been very active in its own right, posting a number of blogs and position papers, participating in a wide variety of academic and think tank forums around the world and making significant speeches and launching initiatives from the leadership level. Indeed, Microsoft’s President, Brad Smith, has been personally very active in this area. Moreover, the company has built a significant international team of policy experts to support the company’s cyber policy efforts. Recently, Microsoft took the novel step of establishing

---

a “representation office to the United Nations headquarters in New York” headed by a senior executive to deal with cybersecurity policy issues, UN Development goals and other issues.  

Although not a formal U.S. entity, the Tech Accord industry group includes many U.S. companies. Its mission is to promote “a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.” Among other things, it has put forth a number of “industry norms” for cyberspace – that is, rules of the road for certain private sector company signatories. It has also taken the lead in the Paris Call working group devoted to multistakeholder involvement in UN norms processes.

U.S. Entity Participation in United Nations Stakeholder Activity

Although still limited, the first UN Open-Ended Working Group afforded the greatest multistakeholder participation of any of the UN processes devoted to international cybersecurity and norms. Although only a few ECOSOC accredited organizations were permitted to be formal observers, the Chair of the Open-Ended Working Group (OEWG) convened an informal multi-stakeholder meeting in December 2020 that was much more inclusive. While numerous civil society groups attended, many with U.S. membership, only

---


34 The UN Cyber GGEs, in contrast, offered little in the way of multistakeholder involvement, though there were presentations and lunches sponsored by non-state stakeholders for the GGE delegates and one country, Estonia, included an academic on its delegation.

35 The Economic and Social Council of the UN handles the accreditation of non-government entities for UN processes. “Welcome to Csonet.Org | Website of the UN DESA NGO Branch. At Your Service.” Accessed September 27, 2022. https://csonet.org/?menu=100. The process of accreditation, however, is not speedy, simple or assured and many non-government organizations who deal with cyber policy are not officially accredited so their participation is restricted.
a comparatively few U.S.-based organizations participated, including Access Now, the EastWest Institute, Human Rights Watch, FIRST, the World Wide Web Foundation, R Street Institute, Temple University, Freedom House, Stimson Center, and the German Marshall Fund. Private sector U.S.-based company participation was even more sparse. Although a few multinational companies were represented by their U.S. personnel or U.S. subsidiaries, only a very small number of U.S.-headquartered entities participated. However, both the U.S. Chamber of Commerce and the U.S. Council for International Business – trade groups representing a number of U.S. businesses – participated in the OEWG informal multistakeholder discussion.

The OEWG also welcomed written submissions by non-state stakeholders following the circulation of the “pre-,” “zero,” and “first” drafts of its report, but only a few U.S.-based organizations submitted comments. Again, there were written submissions from a variety of groups with U.S. members or participation, including the International Chamber of Commerce, the CPI, the Tech Accord, The Global Forum on Cyber Expertise and the GCSC. Given the seeming non-state stakeholder interest in having a greater impact on UN cyber processes and the fact that opportunities were given in the OEWG for input, it is somewhat surprising that there wasn’t greater U.S. non-state stakeholder involvement in that process.

Multistakeholder participation has been a major point of discussion and conflict in the second Open-Ended Working Group that convened with a five-year term in 2021. There were extended debates among countries on “modalities,” where the U.S. and many like-minded countries sought to expand non-state stakeholder participation beyond what was permitted in the former OEWG. The group agreed on a compromise that would allow more stakeholder involvement by a consensus of member states and this time a good number of U.S.-based organizations formally applied. Unfortunately, the Russian Federation blocked virtually all U.S.-based organizations and most

---

36 Observations of the author who attended the meeting.
37 Ibid.
39 Limited participation from businesses may reflect a lack of more widespread understanding of how these proceedings could affect their bottom line or a reliance on trade associations to espouse their views.
41 Ibid.
all applicants for accreditation from “like-minded” countries. Significantly, the U.S. offered several organizations, including businesses, the opportunity to join the U.S. delegation for the meeting. Like the first OEWG, the Chair has held an informal consultation session with all stakeholders, including those who were blocked.

**U.S. Government Stakeholder Interaction**

There has been a blend of both formal and informal interactions between the U.S. government and other stakeholders. First, the government communicated its positions to all stakeholders on norm and international security matters through formal documents including the U.S. International Strategy for Cyberspace, the State Department’s International Strategy in 2011, Report to Congress in 2016, and the Trump White House Cybersecurity Strategy in 2018 detailed above. This was supplemented by Congressional testimony regarding stability issues on several occasions by the State Department Coordinator for Cyber Issues and other officials and high-level speeches made by both Secretaries Clinton and Kerry. The U.S. also released its country position papers submitted in the course of GGE processes. Although these statements and documents were primarily transparency measures rather than interactive ones, they allowed other stakeholders to assess the development of formal U.S. positions.


S/CCI, together with the CSIS, sponsored a multistakeholder seminar in Geneva in 2016 hosted by the United Nations Institute for Disarmament Research (UNIDIR). This seminar capped off a series of several U.S.-sponsored multistakeholder workshops organized by CSIS that focused on international law, norms and confidence-building measures. The U.S. also participated in UNIDIR multistakeholder seminars both before and after that series. In addition, the U.S. participated in and later helped sponsor a series of multistakeholder meetings organized by MIT, Harvard, and the University of Toronto on cyber norms. These conferences included academics, think tanks, private sector and other civil society actors with the aim of informing government positions in the 2013, 2015 and 2017 cyber GGEs. Moreover, the U.S. worked with the UK and subsequent hosts of the so-called London Process series of conferences, Hungary, South Korea, the Netherlands and India, to hold multistakeholder discussions about cyber stability and UN developments. It also is a founding member of the Global Forum on Cyber Expertise (“GFCE”), a global multistakeholder capacity-building organization. One GFCE Task Force is focused on norms, Confidence-Building Measures and stability – not as a negotiating platform but as a way to garner greater acceptance and implementation of these measures.

In addition, the U.S. held a number of formal bilateral and regional “all of government dialogues” with other countries, including Japan, Brazil, India, Germany, and the European Union. These dialogues often featured a day or half-day multistakeholder component where a range of issues were discussed, including stability issues. Moreover, norms and stability were discussed in “track two” dialogues with India and Australia. State Department lawyers participated, albeit informally, in discussions that led to the production of the Tallinn Manual and Tallinn Manual 2.0 regarding the application of international law to cyberspace. The State Department’s Democracy, Human Rights and Labor Bureau and S/CCI engaged with a number of civil society groups on human rights aspects of cyberspace and how they applied to security, including in the context of the Coalition for Freedom Online.


47 Interview of Michele Markoff, Acting Coordinator for Cyber Issues, U.S. State Department, lead U.S. negotiator for the OEWG and GGE.

48 The author, while serving as Coordinator for Cyber Issues at the U.S. State Department, participated and helped in the organization of these meetings.
These formal and semi-formal interactions were supplemented by a bevy of other interactions both domestically and globally. The U.S. government participated in discussions and as presenters at the yearly multistakeholder Internet governance Forum that included discussion of cyber stability issues. Senior S/CCI representatives frequently participated in multistakeholder discussions and panels organized by a host of domestic and international non-governmental groups. The U.S. also participated in multistakeholder events organized by individual countries and regional organizations including ones held by OSCE, Singapore’s Cyber Week, the OAS, and the ASEAN Regional Forum. Finally, the U.S. engaged in some direct domestic outreach, meeting periodically with trade organizations and their member companies, though these engagements were somewhat sporadic.

U.S. government interactions with other stakeholders around the globe allowed the U.S. to announce, test, and refine its positions based on these interactions. The plethora of interactions detailed above provided an opportunity for the U.S. to espouse its positions and hear the comments and feedback on those positions from a range of stakeholders. The U.S. also benefited from more in-depth discussions that helped inform developing policies, including policy positions relating to accountability, collective action and deterrence in cyberspace. Nevertheless, while there were many opportunities for interaction – particularly informally – between the U.S. government and other stakeholders, formal or structured interactions were limited. The lack of any sustained formal process of interaction and the lack of a clear connection to UN and other policy development and negotiation processes left some stakeholders frustrated. While the U.S. government benefited from informal interactions, it too was deprived of potentially more structured and varied input that a more formal process could provide as a supplement to informal interactions.

PERCEIVED CHALLENGES TO GREATER U.S. GOVERNMENT–MULTISTAKEHOLDER INTERACTION

The absence of a more formal U.S. government engagement regarding ongoing negotiations is due to a number of factors. First, as noted earlier, the UN First Committee on Disarmament and International Security has long been the province of states alone. In traditional arms control, states are the primary, if not sole, actors. Many of the lead negotiators in the First Committee, including the long-time former U.S. chief negotiator, Michele Markoff, come from a nuclear or other strategic arms control background and state-centric perspective. While Ms. Markoff acknowledges the value of non-state stakeholder input – and recently forcefully argued for such input in the new OEWG – she notes that, at the end of the day, only states can negotiate in the UN and that the norms...
are expressly focused on “voluntary norms of appropriate state behavior.”

That is particularly true with respect to “norms of restraint” as only states can actually refrain from taking those actions that they agree to limit.

Moreover, neither the private sector nor civil society is a monolithic group and individual members of each have widely diverging, and sometimes conflicting, priorities, views and reasons for engagement. In some cases, entities engage with the government, at least in part, to avoid greater government scrutiny, and potential regulation, of their practices or products. Some companies prioritize particular policies to give them a perceived advantage over their competitors. Some civil society entities prioritize their advocacy of a single issue or perspective. Of course, every stakeholder – state or non-state – will have their own perspectives guided by their experience, and, to some extent, every stakeholder operates from their own enlightened self-interest. Businesses have to think about profits, competitiveness, and access to international markets, and civil society’s interests and motivations are incredibly broad. Yet integrating these various perspectives through the lens of their varying vantage points is what the government does routinely, both with respect to physical and cyber policy issues. While the U.S. government will not agree with all stakeholders’ input, and vice-versa, accounting for, synthesizing, and, where appropriate, challenging those views can lead to a better end result.

Accordingly, a challenge for the government is having sufficient diversity of stakeholder and stakeholder groups so that they represent a broader cross-section of views. Generally, the U.S. government favors engaging with industry groups over individual companies so as to avoid the appearance that it is favoring one company’s views over another potential competitor. As noted, Microsoft has long been the dominant industry player in the stability area and, for a period, other companies either appeared uninterested or had other priorities. The Tech Accord helps mitigate that concern as it is a collection of companies with a norms and stability focus, but greater involvement by individual tech and non-tech companies is still lacking. When garnering formal input, government agencies also have to make sure they comply with the Federal Advisory Committee Act in not taking group advice unless a formal FACA committee is established. Setting up a formal FACA-compliant committee takes a significant commitment of resources. Both formal and informal stakeholder engagement was also hampered during the Trump Administration by the downgrading of the Office of the Coordinator for Cyber Issues, the resulting departure of personnel and more stringent budgetary constraints.

---

49 Interview with Michele Markoff. (emphasis added).
Regardless of past perceived challenges, greater stakeholder engagement can not only be valuable in informing U.S. positions and negotiations, but it is critical to the implementation of already agreed stability measures. Private sector entities argue that they are essential players because they own and operate the great majority of the infrastructure in cyberspace, and that makes cyberspace different from other domains because the potential “field of battle” is their infrastructure. Although some might argue that cyberspace is not so unique, since privately owned infrastructure – such as train lines, communication systems and shipping routes – are affected in a potential physical conflict, it is true that cyberspace operates on a much greater scale where civilian and military activities coexist and can conflict. Moreover, constructing “rules of the road” for state activities in cyberspace benefits from a technical understanding of that platform and non-government stakeholders can bring a unique and informed perspective both to what is possible and the likely second- and third-order effects of various measures. Think tank and academic stakeholders can often examine issues in far more detail and over a longer period than government negotiators, and human rights groups can bring a much-needed perspective to even traditional security discussions. Moreover, the interaction of these stakeholder groups could reveal gaps or produce solutions that would evade any one group acting alone.

The State Department’s recent creation of the Bureau for Cyberspace and Digital Policy (“Cyber Bureau”)\(^50\) affords an ideal opportunity for the State Department to overhaul its methods for engaging with other stakeholders and creating new formal and informal structures. In the speech announcing the new Bureau, Secretary of State Anthony Blinken made clear that multistakeholder engagement, at least domestically, was vital to the State Department’s work more generally, stating:

\[\text{we have got to do more listening. That’s not just the right thing to do; it’s the necessary thing to do. If key stakeholders aren’t with us on the take-off, they are less likely to stick with us on the landing. We need their ideas, and we need their buy-in … We are going to reach out much more regularly to civil society, to private companies, state and local government, community organizations, universities} \]

and we’ll make sure that we’re connecting with people from different parts of the country – urban and rural – because our mission isn’t to serve some Americans, but all Americans.\textsuperscript{51}

While the bureau is still in its early development, its broad mandate (including cyber stability, digital economy and human rights issues) is an ideal structure for broad multistakeholder engagement both within these individual issues and across them as they are often interdependent. Moreover, the promise of substantially increased resources and personnel for the bureau allows for greater structured and informal interaction with other stakeholders both domestically and internationally. The new bureau is currently working on a new international cyberspace strategy mandated by the U.S. Congress that offers opportunities to both engage stakeholders in its creation and establish more formal interactions. Nathaniel Fick, the Ambassador at Large appointed to head the new bureau, comes from a private sector background and is engaging frequently with a range of non-state stakeholders. Among other things, the State Department and the new Cyber Bureau should consider the following.

**Create More Formal Stakeholder Interaction Mechanisms to Supplement Informal Ones**

Several other democratic countries have created formal mechanisms to garner stakeholder input into UN and other stability discussions. Estonia and the Netherlands have had an academic representative on their formal delegation to the OEWG and/or GGE. Canada co-sponsored with Australia an initiative entitled “Let’s Talk Cyber” that convened a number of multistakeholder events on the sidelines of the OEWG. Canada also expressly solicited non-state stakeholder comments on a paper that it planned to submit to the OEWG and incorporated many of those comments on successive drafts of that paper.\textsuperscript{52} The Netherlands helped fund and launch the GCSC and advocated in the UN for some of the recommendations that group made in its report.

Australia conducted perhaps the most ambitious formal stakeholder engagement. In December 2019, the Australian Department of Foreign Affairs and Trade (“DFAT”) published a formal call for submissions to a Public


\textsuperscript{52} Interview with Sirine Hijal, lead Canadian Cyber Negotiator in the OEWG.
Consultation: Responsible State Behaviour in Cyberspace in the Context of International Security at the United Nations. In June 2020, the Australian government compiled a “Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report, as endorsed by the UN General Assembly” and submitted it to the OEWG for consideration by all member states. According to Australia’s former chief negotiator on UN cyber matters, Johanna Weaver, “[i]t’s truth, not lip service, to say that this engagement shaped Australian positions.”

The U.S. should adopt a formal consultation process based on that used by Australia. This would supplement the many informal engagements detailed above, which should continue, but bring more structure and predictability for non-state stakeholders seeking to have meaningful input into U.S. positions. Like the one conducted by Australia, the formal consultation process should be broad-based and open to all stakeholders, conducted periodically (but particularly linked to ongoing negotiations), and be a mix of both written submissions and live interactions to allow optimal interaction. This approach has the advantage of being open to a wide range of stakeholders and should not be overly burdensome for the State Department to conduct. The State could also consider creating a cyber policy advisory committee that complies with FACA, as discussed above. For example, this approach has been used to help inform the International Telecommunications Union and other negotiations through an International Digital Economy and Telecommunications Advisory Committee.

---


54 Ibid. Interview with Johanna Weaver, former Australian chief negotiator in the OEWG and GGE.


56 Interview with Johanna Weaver.
Committee. Of course, such a formal committee would necessarily have limited membership.

The U.S. should also co-sponsor innovative platforms for stakeholder engagement, like Let’s Talk Cyber, that have a broad base of international stakeholders, and take a more active role in the Paris Call and other multi-stakeholder platforms. Within weeks of announcing the new Cyber Bureau, the Biden Administration took a significant step in reversing the Trump Administration’s decision and joining the Paris Call. The White House Fact Sheet issued when Vice President Harris announced the U.S. was joining the Call expressly references working with other stakeholders, stating the “United States looks forward to continued partnership with France and other governments, private sector, and civil society around the world to advance and promote norms of responsible behavior in cyberspace.” Now that the U.S. is a formal member of the Paris Call community it could, and should, avail itself of the opportunities for stakeholder engagement it provides – both at the working and senior levels – and, as appropriate, help lead and shape conversations in that platform.

**Step-up Multistakeholder Engagement on Norm Implementation and Capacity Building**

An additional aspect for enhanced U.S. government/multistakeholder interaction is norms and stability measure implementation. Implementation involves gaining greater understanding of the agreed-on norms and other stability measures and putting them into practice. Translating sometimes high-level norms into concrete practice helps give them more meaning and force. Implementation also includes cyber capacity building as a foundational pillar to getting more countries to embrace norms and stability measures and to build the capabilities to put them into practice.

Other stakeholders, including the private sector, can be instrumental in working with states on norm implementation, particularly as an aspect of cyber capacity building. Although some countries objected to greater non-state stakeholder involvement in the UN First Committee negotiating processes, the consensus UN GGE report makes clear that “[i]ncreased cooperation alongside

---

more effective assistance and capacity-building in the area of ICT security involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behavior of States in their use of ICTs.59

The U.S. has prioritized implementation and cyber capacity building for several years and there are many opportunities for further partnerships with other stakeholders, especially now that the U.S. State Department’s cyber efforts are set to receive greater stature, resources and funding under the Biden Administration. As noted earlier, the U.S. government is already an active participant with private sector and civil society actors in the multistakeholder GFCE, and those and other capacity-building efforts can be strengthened.

Increase Work with Other Stakeholders on Accountability

There is also an opportunity for increased U.S. government-stakeholder collaboration in bolstering accountability for norm violations. Norms, international law and other rules in cyberspace, or in the physical world, are little more than words on paper if there is no accountability when they are violated. One aspect of accountability is public attribution of an event. Several private sector cybersecurity companies already share threat and other information with the U.S. government, and some have independently and publicly attributed malicious cyber activity to nation-states in the past. The U.S. government has also increasingly publicly attributed malicious conduct to nation-states both by itself and collectively with several country partners. Increased private sector attribution, even when not in concert with U.S. government statements, nevertheless can help with calling out bad behavior. In addition, norm implementation can be aided by both the U.S. and non-state actors tying instances of attribution to particular norm or law violations. Yet, for some actors, public attribution and so-called “naming and shaming” are unlikely to lead to a change in behavior or norm compliance. In these cases, additional, non-escalatory consequences for malicious actions are required. The U.S. government has a range of tools at its disposal to “impose costs,” including diplomatic, law enforcement, economic (including sanctions) and military action (including targeted “cyber operations”). Although that tool set could be used much more strategically and effectively than it has been in the past, it still has limitations, and some, including the author, have called for creatively expanding the tool set by working with the private sector and others.60 Of course, this can only

59 OEWG Final Report, para. 87.
go so far – private sector entities are unlikely to want to be on the front lines of state-to-state responsive actions both for fear of retaliation and for market/economic reasons. However, how the government and private sector can creatively discuss new tools of deterrence, including both tools to impose costs and tools to reward positive behavior, is worth further study.

**Continue to Advocate for Greater Multistakeholder Participation in UN Processes**

At the time of writing, the UN First Committee is already two years into a new five-year cyber OEWG. In addition, France and over 40 other countries proposed a follow-on “Program of Action”61 (“POA”) for advancing responsible state behavior in cyberspace. The POA originally contemplated organizing “consultations with other stakeholders (private companies, NGOs, civil society …), regional organizations, representatives of other UN processes, and relevant multi-stakeholder initiatives dealing with cyber-related issues in the context of international security.”62 The proposal for a POA has been formally adopted by the UNGA First Committee but the details — including the scope and modalities of non-state stakeholder engagement are still being negotiated.63

The U.S., of course, has supported multistakeholder participation in prior UN meetings, but because they are consensus-based and some countries oppose that formulation, other stakeholder involvement has been limited. Of course, those same dynamics remain and, indeed, have become even more complex given the war in Ukraine. However, as noted above, the U.S. has been a strong and vocal advocate of including other stakeholders in this process – going so far as to offer to include stakeholders in its formal delegation. The U.S. can continue to look for creative ways – including active participation in informal side processes – to involve other stakeholders to the maximum extent possible in the OEWG, potential POA and other processes.

---


63 https://dig.watch/updates/resolution-on-the-programme-of-action-poa-on- -cybersecurity-adopted)
CONCLUSION

The U.S. government has long espoused the need for multistakeholder input and participation in a range of policy and operational aspects of cyberspace. While there has been good interaction between stakeholders on issues of cyber stability policy, the ever-rising policy and technical threats in cyberspace, coupled with an active, growing and varied non-state community who can bring needed perspectives and value to state-centric discussions, argues for that interaction to be substantially increased and formalized. This need is especially acute since many relevant stakeholders have been blocked from formal participation in the new OEWG. The creation of a new Cyber Bureau at the State Department provides a perfect opportunity to leverage and involve the multistakeholder community to aid in norm and other stability measure development, implementation, global cyber capacity building and ensuring accountability for bad actors. No stakeholder, including the U.S. government, has all the answers or capabilities in this complex area. If the U.S. wants to achieve at least a measure of increased global cyber stability, it can’t afford to not fully engage the capabilities and perspectives of the private sector, civil society, and academia.
INTRODUCTION

Russia has always adhered to traditional approaches to diplomacy on international political matters. Moreover, Russia traditionally relies more on bilateral relations with specific countries to resolve disputes than on international multilateral institutions. On matters that require international cooperation, Russia emphasizes the central role of UN system organizations, particularly the Security Council, in which Russia is a permanent member with the right to veto decisions.

Internet governance is therefore a challenge for some aspects of Russia’s foreign policy and diplomacy because the Internet inherently is a global supra-national environment, free from individual state control. At various times, beginning in the late 1990s, attempts were made to create multiple informal instruments concerning rights and freedoms on the Internet. Among the first was the “Declaration of Independence for Cyberspace” by John Perry Barlow, founder of the Electronic Frontier Foundation. The document states:

We are creating a world into which everyone can enter without privileges and discrimination, regardless of skin color, economic or military power, and place of birth. We create a world where anyone can express their opinions, no matter how extravagant they may be, without fear that they will be forced to silence or agree with the opinion of the majority […]. In China, Germany, France, Russia, Singapore, Italy, and the United States, you are trying to establish an information quarantine to prevent the spread of the free-thinking virus by setting up outposts at the borders of cyberspace. These measures can contain the epidemic for a while, but in a world that will soon be engulfed in a communication medium carrying bits, they will not work.¹

This document, which is more literary than political or legal, nevertheless anticipated the emergence of measures seeking to regulate the rights and freedoms of Internet users.

The very idea of the participation of non-state actors in international diplomatic decision-making is not new. As early as 1919, the International Labour Organization (ILO) included non-state actors among its representatives. The tripartite system implemented in the ILO can rightfully be called the predecessor of the multistakeholder approach. The ILO’s report noted that “tripartite or multi-stakeholder frameworks to oversee institutions and processes depend on stakeholders’ capacity, independence, and legitimacy, but [their] quality may be impaired if dispute resolution practitioners, including the social partners, have limited capacity, knowledge or skills.”

RUSSIAN PERSPECTIVES ON GLOBAL INTERNET GOVERNANCE

The Russian Federation carefully monitors and resists encroachments on its sovereignty, including in cyberspace. Even before the adoption of amendments to the Constitution of the Russian Federation, Russia withdrew from the Convention on Cybercrime to protect its sovereignty. With the adoption of the Constitutional amendments, Russia consolidated this position. Article 79 of the Constitution now reads as follows:

The Russian Federation may participate in interstate associations and transfer to them part of its powers by international treaties of the Russian Federation if this does not entail restrictions on the rights and freedoms of man and citizen and does not contradict the principles of the constitutional system of the Russian Federation. Decisions of interstate bodies adopted based on the provisions of international treaties of the Russian Federation in their interpretation, contrary to the Constitution of the Russian Federation, are not subject to execution in the Russian Federation.

The protection of sovereignty as a principle of the Russian Federation’s activities in the field of information and communication technologies can be judged by an assessment of Russia’s participation in international agree-

---

ments on cybercrime. The Russian Federation is a party to the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in the fight against crimes in the field of Information Technologies, which it ratified with the following reservation: “The Russian Federation reserves the right to refuse the execution of the request in whole or in part, if the execution of the request may damage its sovereignty or security.” The reservation is related to a provision on trans-border access to stored computer data with consent or where publicly available.

The Russian Federation initially signed the Budapest Convention on Cybercrime but withdrew its signature and completely refused to join the Convention. Russia explained its action by claiming that provisions of paragraph “b” of Article 32 of the Convention are formulated in a way that includes the possibility of their being interpreted in a manner that does not correspond to the purposes and principles set out in paragraphs 9 and 10 of the preamble to the Convention and may harm the sovereignty and national security of the participating States, the rights and legitimate interests of their citizens and legal entities. According to the contested clause 32 (b), a Party may, without the authorization of another Party, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the legal authority to disclose the data to the Party through that computer system.

Different states use different models to regulate the Internet, and Russia adheres to the concept of cyber sovereignty, following the model implemented in China. With more Internet users than any other country, China is an essential player in Internet governance. In digital politics, China balances the “economics” of freedom of communication and the “politics” of filtering Internet access for Chinese users. Protecting sovereignty, a cornerstone of Chinese foreign policy is also reflected in its approach to cyberspace. Lu Wei, former head of the Cyberspace Administration of China, said at the second China-South Korea Internet Roundtable, “[Just] as the seventeenth century showed the expansion of national sovereignty over parts of the maritime space

---

and the twentieth over airspace, currently national sovereignty extends to cyberspace [...] cyberspace cannot exist without sovereignty.”

In Russia’s legislation, the desire to establish sovereignty in cyberspace has emerged as a dominant theme. Russian cyber power has become widespread in the relevant regulatory legal acts. On May 1, 2019, the President of the Russian Federation signed the law “On Amendments to Certain Legislative Acts of the Russian Federation,” known as the “Law on the Sovereign Internet.” This law prescribes the creation of an alternative system, the purpose of which is to ensure the functioning of the Internet in Russia in the event of its disconnection from the global network. This Act partially entered into force on November 1, 2019, and into full force in 2021.

According to the drafters of the law, protective measures are necessary to ensure the long-term and stable operation of the Internet in Russia and to increase the reliability of Russian Internet resources. The law determines the rules required for traffic routing and includes measures to ensure compliance. It aims to minimize the transfer abroad of data exchanged between Russian users.

The law also defines cross-border communication lines and traffic exchange points. Telecom operators are obliged to ensure the possibility of centralized traffic management in case of a threat. In other words, the law creates the infrastructure to enable the continued operation of Russian Internet resources in the event that connecting to root servers located abroad becomes impossible. Control over the implementation of the law is entrusted to the Federal service for supervision in the sphere of communications, information technologies, and mass media (hereinafter “Roskomnadzor”).

According to experts from the Agora human rights group, the so-called “Law on the Sovereign Internet” provides for strictly centralized control over the points of exchange of cross-border Internet traffic, which allows the authorities, at their discretion, to disable certain services, traffic types, and restrict Internet access for individuals and territories. According to the specified parameters. The bill also provides for an emergency regime for managing the Russian segment of the Internet, when in the event of “threats to the integrity, stability, and security of operation,” Roskomnadzor can take over the centralized management of all communication networks.

8 Jovan Kurbalija, An Introduction to Internet governance, 7th ed. (Msida, Malta: DiploFoundation, 2016).
The adoption and implementation of the law on the Sovereign Internet creates risks for the very existence and functionality of the Russian segment of the Internet, including its commercial or non-profit usage, excessively expands the powers of Roskomnadzor, and requires significant budget expenditures. These critiques were first articulated in the expert council’s response to the draft law of the Russian Federation’s Government. The experts pointed to the technical impossibility of telecom operators “transferring to Roskomnadzor the complete scheme of their network and traffic routing in it.” They explained that this is impossible because the network is constantly expanding and updating.

The experts also pointed to the non-transparent purpose of the bill. The amendments refer to the potential threat to the Russian segment of the Internet, but their authors did not specify the threat. In addition, the Russian Government experts felt that the amendment extends the powers of Roskomnadzor, and concentrates regulatory functions in one entity that is not independent of the government. They stated that the transfer of the tasks of legal regulation, supervision, and direct management of the communications industry to Roskomnadzor “carries unacceptable risks of corruption.”11

In November 2017, Russian President Vladimir Putin demanded that Russia undertake the development of autonomous control systems for the Internet, which would counter US “dominance” of the web. The Ministry of Telecom and Mass Communications, together with the Ministry of Foreign Affairs, was instructed to reach an agreement with the BRICS countries on the creation of a system of root domain name servers (DNS), which would “duplicate” the existing one, would be independent of the control of international organizations (such as the Internet Corporation for Assigned Names and Numbers, ICANN) and would protect, among other things, Russian users from “targeted impacts” (e.g. sanctions imposed by the United States). The “sovereignization” of the Internet could be considered a part of the Russian domestic and international cybersecurity strategy. The concerns posed by the deterioration in United States–Russia relations and the potential imposition of US sanctions on Russia against the use of critical Internet resources is a key factor animating this strategy. The explanatory note to the “Sovereign Internet” law states that it was “prepared to take into account the aggressive nature of the US National

---

Cybersecurity Strategy adopted in September 2018.” The US strategy mentions Russia twice. The document notes that

Russia, Iran, and North Korea conducted reckless cyberattacks that harmed American and international business, as well as our allies and partners, without paying expenses that could prevent future cyber aggression. […] Russia, China, Iran, and North Korea use cyberspace to fight the United States, their allies, and partners, often with recklessness never used in other areas. These opponents use cyber tools to undermine our economy and democracy, steal our intellectual property and sow discord in our democratic processes.12

According to supporters of the Russian strategy, state sovereignty necessarily extends to the national information spaces, which are connected to the Internet.13 The law makes it possible to create an alternative system of DNS addresses, as well as technical tools for disconnecting the local Internet from the outside world. This law drew criticism not only from outside but also from the Internet community within Russia since the fragmentation or “balkanization” of the Internet would inevitably lead to its disintegration, which, in the opinion of the critics, was unacceptable. It would limit technological development, and violate the rights of Internet users, both in Russia and abroad. In addition, shutting down the Internet with the transition to the internal network within the same country is hardly technically feasible without serious negative consequences for the economy, citizens’ rights, and global governance in general.

In our opinion, meaningful multistakeholder cybersecurity governance of “sovereign Internets” as contemplated by Russian law is not possible because of the lack of participation of global stakeholders. The example of China, on which the Russian strategy is modeled, is illustrative: only national stakeholders participate in cybersecurity policymaking, and global international platforms are absent.

PARTICIPATION OF RUSSIAN NON-GOVERNMENTAL STAKEHOLDERS IN GLOBAL CYBERSECURITY AND INTERNET GOVERNANCE

Several Russian stakeholders participate in global processes of Internet and cybersecurity governance. Stakeholders involved in some of these processes

Russia’s participation in multistakeholder diplomacy

are outlined in the annexed table. Only some Russian stakeholders are under direct government control, but executive authorities exert a guiding and regulatory influence over them. At the same time, the business community (private sector) is also interested in implementing government projects. According to V.M. Aliyev, in a geopolitical environment reminiscent of the Cold War, including intensified political and tough economic sanctions against Russia, it will be impossible to build the foundation of the future digital economy on “borrowed technologies.” Therefore, the digitalization of the economy requires import substitution in the field of information technology. Most of the state information infrastructure required by this strategy should be converted to Russian software. It is no coincidence that one of the declared goals of the government is the indigenization of the Russian part of the Internet and the transfer of control over it to the government. Therefore, the private sector has to be mindful of competing for domestic and global imperatives while engaging with global processes of Internet governance and cybersecurity.

Private Sector

Software companies are interested in the existence of a register of Russian software. The need to localize personal data on servers within Russia also has a certain economic effect, generating profit from renting server capacities. Amendments to the Law on Information introduced a unified register of Russian programs for electronic computers and databases to expand the use of those programs, confirming their origin from the Russian Federation, as well as to provide copyright holders with programs for electronic computers or databases of government support measures. However, there are no Russian companies that offer major, internationally adopted software (like Windows from Microsoft, Android from Google, or iOS from Apple). Manufacturers of software that have successfully established themselves on the global market (for example, Kaspersky Lab products) have an interest in the global reduction of legislative and administrative barriers to doing business. Kaspersky Lab products, however, appear to have been caught in the crosshairs of geopolitics and are now prohibited in the United States. The Independent reported that the U.S. government has banned federal agencies

14 V.M. Aliyev, “Political And Legal Aspects of the Transition to a Digital Economy in Russia.” Russian Investigator (2018).

from using Kaspersky Lab security software, a Russian company, over concerns that it may be tied to state-sponsored espionage.\textsuperscript{16}

**Civil Society**

Another group of stakeholders – civil society institutions – have other interests, the fulfillment of which requires direct and sustained cooperation with foreign partners. Foreign agent legislation in Russia makes it very difficult for such organizations to carry out any foreign-funded political activity. Thus, under the law on public associations, a non-profit organization performing the functions of a foreign agent is defined as

one that receives money and other property from foreign states, their state bodies, international and foreign organizations, foreign citizens, stateless persons or persons authorized by them and (or) from Russian legal entities that receive funds and other property from these sources (except for open joint-stock companies with state participation and their subsidiaries), and which participates, including in the interests of foreign sources, in political activities, carried out on the territory of the Russian Federation.\textsuperscript{17}

Foreign agent legislation doesn’t restrict any political movement but makes it complicated and ethically challenging for fundraising and mobilization by civil society.

Actions to influence Internet governance, or to join in multistakeholder cyber diplomacy, can be considered “political activity.” A non-profit organization is deemed to be engaging in political activities carried out on the territory of the Russian Federation if it participates (including by financing) in the organization and conduct of political actions to influence the adoption of decisions by state bodies aimed at changing their state policy, as well as in shaping public opinion for these purposes.

**Academic Community**

The academic community may have difficulties implementing a new law restricting educational activities. According to the law, which entered into force on June 1, 2021, the conclusion of contracts by non-governmental


educational organizations, except for agreements on the provision of educational services to foreign citizens, must be carried out “under the supervision of the federal executive body performing the functions of development and the implementation of state policy and legal regulation in the field of higher education, or the national administrative body responsible for the development and implementation of state policy and legal regulation in the field of general education.” Schools and universities have the right to participate in international cooperation only if there is an opinion from the Ministry of Education or the Ministry of Education and Science of Russia, respectively. An exception is made only for schools and universities under federal control. Consequently, it would be difficult for educational institutions and the academic community to freely and meaningfully participate in cybersecurity policymaking and discussions.

THE PAST AND PRESENT OF RUSSIA’S CYBERSECURITY DIPLOMACY

At the 2012 World Conference on International Telecommunications in Dubai, Russia sought to strengthen the role of states through an affirmation of their sovereign right to formulate and implement public policy, including international policy, on the governance and regulation of the national segment of the Internet, territorial organizations that provide access to the Internet and carry Internet traffic, as well as equitable, international distribution of critical Internet resources. In other words, the Russian proposal aligned the internationalization of Internet governance with the simultaneous expansion of the capacity of governments to influence the governance of national network segments. Moscow has repeatedly expressed its unhappiness with the governance of the Domain Name System being in the hands of the US-based non-governmental organization (NGO) ICANN. President Vladimir Putin proposed making the International Telecommunications Union (ITU) the main supervisory authority in Internet governance. Several member states (including the CIS countries and the BRICS – Brazil, Russia, India, China, and South Africa) have expressed support for Russia’s position.

---


It is important to jointly develop and implement universal and fair rules of responsible behavior of states in the information space and to agree on legally binding criteria for acceptable and unacceptable actions. At the same time, Russia calls for the inviolability of the digital sovereignty of states. This means that each country can independently determine the parameters for regulating its own information space and corresponding infrastructure.

President Putin declared at a 2022 meeting of the Security Council of the Russian Federation that it is largely thanks to the efforts of Russia that the topic of information security firmly entered the agenda of the UN General Assembly. In 2018, the UN First Committee on Disarmament and International Security approved, by a vote of 109 in favor to 45 against, with 16 abstentions, the draft resolution “Developments in the field of information and telecommunications in the context of international security,” tabled by the Russian Federation. The proposal sought for the UN General Assembly to convene an Open-ended Working Group (OEWG) acting on a consensus basis to develop rules, norms, and principles of responsible behavior of States in cyberspace. The OEWG has been positioned as a Russian counterweight to the UN Group of Governmental Experts on ICT security – itself a Russian creation, but in which the US and its allies have increasingly played an influential role – and submitted its report in March 2021.

According to Andrey Krutskikh, Director of the Russian Department of International Information Security between 2020 and 2022, lead Russia negotiator for the UN Group of Governmental Experts (UNGGE) and OEWG, and one of the most prominent governmental speakers in the sphere of cybersecurity, the foreign policy strategy of Russia concerning Internet governance is based on its national interests. He notes that Russian policymakers have repeatedly affirmed their country’s support for the principle that no single government should have power over the international governance of the Internet. Russia actively defended its position in the World Summit on the Information Society, advocating the transfer of ICANN functions to international control. The Russian Federation supports the active involvement of the ITU and the

---

Russia’s participation in multistakeholder diplomacy

Desire of the institution to play a key role in the field of management of the Internet. In Krutskikh’s view, Russia’s goal was to transfer the functions of ICANN to the ITU, which has already expanded its sphere of responsibility and assumed new functions in the area of telecommunications regulation. Krutskikh also notes that Russia has expressed its support for the preservation of the principles of multistakeholder partnerships and participation in Internet governance. Not only states but also representatives of civil society, businesses and the academic community, engineers and developers of the Internet – technologies that will in the long term serve to maintain the innovative nature of the Internet, its openness and availability.\(^\text{24}\)

According to Konstantin Noskov, the Minister of Digital Development, Communications and Mass Media of the Russian Federation, in the context of the rapid development of information technologies, the ITU should remain the leading UN platform for agreeing on collective approaches to solving urgent problems in the field of ICT development, including the Internet. The key task of the ITU should be to enhance international cooperation for the safe and rational use of all types of telecommunications.\(^\text{25}\)

The official website of the Ministry of Telecommunications and Mass Communications of the Russian Federation notes that the ITU is looking for ways to expand its role in the management of the critical infrastructure of the Internet and make this management more international. The Ministry of Telecommunications and Mass Communications of the Russian Federation and the Regional Commonwealth in the Field of Communications supports the ITU in this.\(^\text{26}\)

A representative of the Ministry of Communications, Igor Milashevsky, said at the Forum 2013 in Bali, that the Russian government supports the general principles of Internet governance developed by the Organisation for Economic Co-operation and Development, the Council of Europe, and other forums.\(^\text{27}\) Robert Schlegel, who was the deputy of the State Duma, noted the need for internationally recognized principles of content management. These


principles should resist the control or blocking of content and emphasize the need to ensure open access for adults while protecting children from malicious content.  

The 2025 United Nations Forum on Internet governance is to be held in Russia. UN representatives sent official confirmation of the status of the host country to the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. Deputy Head of the Ministry of Telecom and Mass Communications of the Russian Federation Maxim Parshin said: “The choice of Russia as the venue for the anniversary forum is a great honor for us and evidence of the recognition of our country in the development of the information society and digital technologies. We aim to ensure that the forum results in practical solutions to ensure the openness and security of the Internet, taking into account the interests of all participants in cyberspace.”

As for the global Internet governance Forum (IGF), Russia has been a constant participant, but its participation could be double-edged in terms of multi-stakeholder governance. Early in the history of the Internet governance Forum, government officials stressed that the IGF’s mandate was clearly outlined in the Principles for the World Summit on the Information Society and the Tunis Agenda. The Russian Federation indicated in its communication that it would like the IGF to consider the principles and future mechanisms of international Internet governance and to discuss issues related to the administration of the DNS and IP addresses.

Thus, in theory, Russia seeks for and engages the IGF to develop and implement international principles of Internet and cybersecurity governance based on a multistakeholder approach. However, the representatives of Russia insist on giving the leading role to government stakeholders, which has historically made Russian participation at the IGF processes quite formal. It can be assumed that one of the goals of organizing and holding the Internet governance Forum in Russia may be international legitimization of its recently adopted laws on a sovereign Internet, as well as legislation restricting the rights and freedoms of Internet users in Russia, sometimes for political reasons. Otherwise, the holding of the Forum in 2024 in Canada could come to be seen as proof of the consolidation of the international principles of a free, open and accessible Internet around the world.


Within the framework of the Russian Internet governance Forum,\(^{30}\) which has been held annually since 2010 and is one of the national initiatives of the international Internet governance Forum, the problems of developing clear and agreed “rules of the game” in the international information space is being discussed. Within the framework of the Russian Internet governance Forum, particular attention is paid to Russia’s participation in global Internet governance and cybersecurity. It is argued that Russia could become “a bridge” to different ideas and models of global Internet governance. In other words, the Russian Internet governance Forum reflects the agenda promoted by Russian representatives at the global level.

RUSSIA AND MULTISTAKEHOLDER CYBER DIPLOMACY: A DIFFICULT ROAD AHEAD

In July 2018, UN Secretary-General António Guterres announced the creation of a High-Level Panel on Digital Cooperation that would, inter alia, develop proposals for reinforcing cooperation in the digital world among governments, the private sector, civil society, international organizations, academic institutions, the technical community, and other relevant stakeholders. The group, co-chaired by Melinda Gates and Jack Ma, comprised 20 members who served in their personal capacities, representing a wide array of professions and constituencies as well as geographic, gender, and age diversity. Russia was “represented” in this group by Marina Kolesnik, senior executive director, entrepreneur, and participant of the Forum of Young Global Leaders. Among the deliverables of the High-Level Panel was to improve the IGF mechanism following a likely revision of its mandate in 2025 and to propose effective multistakeholder models of Internet and cybersecurity governance. The Panel proposed the following three conceptual models:\(^{31}\)

- **Digital Commons Architecture (DCA).** This model seeks to develop management decisions based on a commitment to protecting the Internet for the common interest through multistakeholder approaches.
- **Distributed Collaborative Governance Architecture (CoGov).** The distributed collaborative governance architecture is based on horizontal networks of experts who develop voluntary norms quickly and so convincingly that

---


governments and other actors see them as “regulatory decisions” that must be made and enforced.

- **Internet governance Forum Plus (IGF+).** Building on existing structures, this model entails adding functionality to the Internet governance Forum, the world’s largest multistakeholder Internet-related forum at the highest level, with a UN mandate to enhance its legitimacy and effectiveness and address institutional weaknesses.\(^3\)

Russia may be represented in the HLP, but its official position on these particular models has not been widely articulated. Russia tends to see a divide in the global Internet governance and cybersecurity agenda – some nations focus on the positive potential of the Internet and build their national policies around minimum restrictions and regulations towards technological innovation, development, and cooperation across sectors and countries, while other nations such as Russia choose a more conservative path, focusing on the implications of digital technologies for national security and consider states as the primary and often exclusive stakeholder responsible for it. For the latter group, states are the guardians, or “gatekeepers” – a term widely used in the Russian political lexicon. The recent report of the High-level Panel on Digital Cooperation calls for strengthening and complementing effective multilateral digital cooperation through multistakeholderism. The IGF Plus proposal is especially interesting against the backdrop of Russia hosting the IGF in 2025. For instance, IGF high-level sessions seem to be cut off from the rest of the Forum. Reinforcing IGF through a reconceptualization of stakeholder roles – as IGF Plus does – to ensure the interdependence of cybersecurity, digital economy, and human rights and enhance the global policy process may not be met with enthusiasm among “gatekeepers.”

Despite these considerations, Russia can still emerge as a constructive player in global processes by facilitating the convergence of traditional and multistakeholder cyber diplomacy. Russia should use its hosting of the 2025 IGF to demonstrate that it supports inclusive multistakeholder processes and is ready to confer greater autonomy and decision-making power to the IGF. However, given Russia’s previous attempts to enhance the role of the ITU in multilateral cybersecurity and Internet governance, Moscow is unlikely to adopt such a position. Russia could also balance its diplomatic goals by continuing to press for an international legal instrument in the field of cybersecurity while making certain concessions in such an instrument. While a “cybersecurity treaty” could define the rules for determining the jurisdiction of

states on the Internet, as Russia seeks, it may have to accept as a trade-off the “indivisibility” of the Internet, certain user rights, as well as the participation of non-governmental actors in multistakeholder processes to implement and review those rights.
### Table 7A.1 Stakeholders involved in Internet governance in Russia

<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Stakeholders</th>
<th>Examples of stakeholders</th>
<th>Activities</th>
<th>Interests</th>
<th>Fears</th>
</tr>
</thead>
<tbody>
<tr>
<td>International organizations</td>
<td>International intergovernmental organizations</td>
<td>United Nations, International Telecommunications Union, UNESCO</td>
<td>Building an international regulatory environment for Internet governance</td>
<td>Sustainability of the Internet around the world, implementation of the rights and freedoms of users</td>
<td>Deepening digital divide, Internet fragmentation</td>
</tr>
<tr>
<td>Government</td>
<td>Legislative authorities of the Russian Federation</td>
<td>State Duma of the Russian Federation, Federation Council of the Russian Federation</td>
<td>Legislative regulation in the field of Internet functioning, implementation of international norms</td>
<td>Protection of the sovereignty of the Russian Federation in the information sphere</td>
<td>Disconnecting the Internet in Russia “from the outside,” sanctions against Russia</td>
</tr>
<tr>
<td>Executive authorities of the Russian Federation</td>
<td>Government of the Russian Federation, Ministry of Digital Development, Communications and Mass Media, Roskomnadzor</td>
<td></td>
<td>Public administration and legal regulation in the field of information technology and the Internet</td>
<td>Protection of the sovereignty of the Russian Federation in the information sphere</td>
<td>Disconnecting the Internet in Russia “from the outside,” sanctions against Russia</td>
</tr>
<tr>
<td>Stakeholder group</td>
<td>Stakeholders</td>
<td>Examples of stakeholders</td>
<td>Activities</td>
<td>Interests</td>
<td>Fears</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>Private sector</td>
<td>Russian IT companies</td>
<td>Kaspersky Lab, ABBYY, 1C</td>
<td>Creation of software products and services in the field of information technology included in the register of Russian software</td>
<td>Making a profit through import substitution in the field of information technology</td>
<td>Competition with foreign manufacturers, threats to economic stability, sanctions against Russia</td>
</tr>
<tr>
<td></td>
<td>Russian Internet platforms</td>
<td>Mail.ru, Yandex, “Vkontakte”</td>
<td>Building user communities on the platforms they create</td>
<td>Making a profit on the foreign market</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Attracting users, making profit from advertising</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Stakeholders</th>
<th>Examples of stakeholders</th>
<th>Activities</th>
<th>Interests</th>
<th>Fears</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private sector</td>
<td>Foreign IT companies</td>
<td>Microsoft, Google</td>
<td>Creation of software products and services in the field of information technology</td>
<td>Attracting users, making profit from advertising</td>
<td>Competition from Russian companies, prohibition of activities on the territory of Russia</td>
</tr>
<tr>
<td></td>
<td>Foreign Internet Platforms</td>
<td>Facebook, Twitter, Telegram</td>
<td>Building user communities on the platforms they create</td>
<td>Expansion of platforms by attracting Russian users, making profit from advertising</td>
<td>Competition from Russian platforms, banning activities on the territory of Russia</td>
</tr>
<tr>
<td>Stakeholder group</td>
<td>Examples of stakeholders</td>
<td>Activities</td>
<td>Interests</td>
<td>Fears</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Academic community</td>
<td>Universities, research organizations</td>
<td>Conducting research on the Internet</td>
<td>Access to information and knowledge, cooperation with the international academic community</td>
<td>Restrictions on freedom of speech, right of access to information, academic rights and freedoms</td>
<td></td>
</tr>
</tbody>
</table>

Stakeholder group examples:
- National Research University Higher School of Economics, Moscow
- State Institute of International Relations, Free University
<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Stakeholders</th>
<th>Examples of stakeholders</th>
<th>Activities</th>
<th>Interests</th>
<th>Fears</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil society</td>
<td>International non-governmental organizations</td>
<td>ICANN, Internet Society</td>
<td>Representation of interests, as well as protection of the rights and freedoms of Internet users around the world</td>
<td>Sustainability of the Internet around the world, rights and freedoms of users, compliance with international norms</td>
<td>Disconnection of the Internet in certain countries, fragmentation of the Internet, prohibition of activities on the territory of Russia</td>
</tr>
<tr>
<td>Russian</td>
<td>Regional Public Center of Internet Technologies, Russian Association for Electronic Communications, Agora, Internet Protection Society, Roskomsvoboda</td>
<td></td>
<td>Representing the interests of the Russian Internet business, as well as individual users, conducting research</td>
<td>Compliance with Russian legislation, protection of the rights of Internet business and the rights of Internet users</td>
<td>Threat of being recognized as a “foreign agent” and prohibition of activities, threat to Internet stability, Internet fragmentation</td>
</tr>
<tr>
<td>End users</td>
<td>85% of the population of Russia</td>
<td>Personal and professional use of the Internet</td>
<td>Realization of rights and freedoms on the Internet</td>
<td></td>
<td>Fragmentation of the Internet, disconnection of the Internet in Russia, violation of rights and freedoms</td>
</tr>
</tbody>
</table>
8. Rethinking Chinese multistakeholder governance of cybersecurity

Jinhe Liu

THE QUESTION OF A “CHINESE MODEL”

The Chinese cybersecurity governance model is always described as state-led in the cyber sovereignty rhetoric. When Chinese society uses the term “governance,” it often has the connotation of “management.” China has its specific understanding of multistakeholder governance and has even developed the concept of “multi-participation” (多方参与), which is stated in the White Paper1 issued by the central government. The Internet used to be an exception to the state-dominated character of Chinese politics, but is now reintegrated within the political system and deeply merged with political traditions. In the sphere of Internet policy, despite its criticism of the ICANN model of multistakeholderism, China still acquiesces to a multistakeholder model in the form of “state–industry” cooperation.2 There is a general pattern or dominant policy approach that the Chinese government adopts towards the issue of multistakeholder engagement in technical global Internet governance.3 However, this paper carefully distinguishes between the attitudes toward multistakeholder governance of the Chinese government and the attitudes of Chinese society as a whole. It attempts to identify the actual operating mechanism and distribution of power in multistakeholder Chinese cybersecurity governance.

---

Already one of the biggest actors in cyberspace, China enjoys a complex and seemingly paradoxical relationship with the Internet. There exist two important questions concerning multistakeholder governance of cybersecurity in China. Firstly, does the multistakeholder model that is typical in the Western world actually exist in China? If not, what does a Chinese-style multistakeholder model look like and how much does it resemble those that exist in most Western countries? Drawing on interviews with key people in the development of the Internet in China, as well as important historical events and documents, this paper analyzes the governance processes responsible for the articulation of Chinese cybersecurity norms. It also seeks to analyze the application of multistakeholder cyber governance and diplomacy in China and their influence on international rules.

The chapter is in four parts. The first part classifies Chinese stakeholders in cyberspace into three categories and introduces the main actors. The second divides the Chinese approach to cybersecurity governance into two periods, based primarily on a review and clarification of the Chinese government’s role in cybersecurity policymaking. The third outlines four representative models of multistakeholder operations. Finally, returning to the question asked at the beginning, I argue that it is necessary to revisit and rediscover the earlier Chinese model of multistakeholder governance in cybersecurity.

STAKEHOLDERS AND THEIR POSITIONS IN CHINESE GOVERNANCE

This chapter categorizes stakeholders into three groups: government actor, private sector, and technical and academic community. It treats international organizations and industry organizations as falling within the first and second categories.

---


5 The interview materials used by this paper are derived from the “Oral History of the Internet” project, launched by Dr Fang Xingdong, containing the oral history materials of 8 key personages affecting the development of China’s Internet, including Hu Qinheng, Lu Shouqun, Qian Hualin, Tian Suning, Liu Yunjie, Xu Rongsheng, Zhang Chaoyang and Zhang Shuxin.
Governmental Actors

Cyberspace Administration of China
The Chinese government has long been concerned with information security. After the Snowden revelations, China took swift action to re-design its cyberspace governance regime. The Chinese Communist Party, the governing political force in China, set up a Central Cybersecurity and Informatics Leading Group, led by Xi Jinping, the General Secretary of the CPC Central Committee, as Group leader on February 27, 2014.

The first move of the Leading Group was to combine the National Informatics Office, the Informatics Development Bureau, and the Network Security Bureau of the Ministry of Industry and Information Technology, along with other functions relating to cyber affairs from other ministries, into the Cyberspace Administration of China (CAC). Acquiring two important Internet technical entities of China Internet Network Information Center (CNNIC)\(^6\) and National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) under its umbrella, the CAC is the administrative department for the Leading Group to be the nodal governmental authority in cybersecurity regulation, which includes national cybersecurity legislation.

Ministry of Foreign Affairs
The Chinese Ministry of Foreign Affairs (MFA) is the most important stakeholder in cybersecurity diplomacy. More precisely, cybersecurity affairs have been managed by the Bureau of Arms Control and Disarmament within the MFA.\(^7\) Since the 2000s, the MFA has nominated Experts to the UN Group of Governmental Experts (UN GGE), submitted a code of conduct proposal in 2011, and lately represented the country in the 2019–2021 UN Open-Ended Working Group (OEWG) on cybersecurity. The MFA is also an active participant in the UN Intergovernmental Expert Group meeting on Cybercrime.

Ministry of Industry and Information Technology
The Ministry of Industry and Information Technology (MIIT), created in 2008, oversees the national ICT infrastructure, telecommunications, and Internet-based services. In carrying out this oversight, MIIT not only encourages and enforces network security standards but also participates in the rule-making processes in the International Telecommunication Union (ITU).

---

\(^6\) CNNIC was incorporated into MIIT in 2021.

\(^7\) See the official introduction of the Bureau of Arms Control and Disarmament of MFA, http://switzerlandemb.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/.
and the Internet Corporation for Assigned Names and Numbers (ICANN). It is worth noting that MIIT, the first Chinese government ministry that has engaged in multistakeholder diplomacy, has manoeuvred skillfully overall.8

Private Sector

Technology companies
Chinese Internet companies are mostly privately owned and have a major stake in cybersecurity governance. Traditional leaders like Baidu, Alibaba and Tencent and new ones such as ByteDance, Meituan and DiDi not only dominate their competitors in China, and, like WeChat, are part of the social infrastructure,9 but also serve as the international digital infrastructure.10 The top companies offering cybersecurity services, like 360, Sangfor, DAS-Security and Huawei are becoming strong stakeholders with more robust engagement in cybersecurity governance.11

Industry associations
In China, it is relatively rare to witness one company promote its public policy initiatives. Instead, Chinese companies rely on industry associations to do their cybersecurity governance and diplomacy bidding. Two such industry associations – the Internet Society of China (ISC) and the Cyber Security Association of China (CSAC) – present viable vehicles for multistakeholder cybersecurity governance and diplomacy, through activities such as lobbying for industry-friendly rules, settling disputes among member companies, and promoting shared cyber diplomacy goals.

Internet Society of China
The ISC was founded in 2001 and is the leading industry association, boasting over 1000 members from ISPs, network operation service providers, and

---

10 Chunmeizi Su and Terry Flew, “The rise of Baidu, Alibaba and Tencent (BAT) and their role in China’s Belt and Road Initiative (BRI),” *Global Media and Communication* 17, no. 1 (2021): 67–86.
11 360 launched the influential Internet Security Conference in China, while Huawei actively participated in international cybersecurity standards and rules-making in Internet Engineering Task Force and UN Open-Ended Working Group.
Internet companies. The ISC serves as the bridge that links government, Internet companies, and Internet users.

A big multistakeholder cybersecurity achievement that can be credited to the ISC was its anti-spam initiative, which began in 2006. The association motivated relevant organizations to analyze the origin of spam, and to urge email service providers to fortify their service loopholes as well as set up an anti-spam platform to implement mechanisms to fight against spam. According to Sophos, a leading UK cybersecurity firm, spam originating from China has dropped from 22.3% worldwide in 2006 to 4.1% in 2014.12

**Cyber Security Association of China**

The CSAC was founded in March 2016, with a mission to organize and motivate forces from all walks of life to participate in the building of cybersecurity, to serve its members, the industry, and above all, the national cybersecurity strategy. As of December 2020, it has 388 corporate members and 262 individual members. Since its inception, CSAC has been actively engaged in promoting cybersecurity industry self-discipline, education, and competitions to raise cybersecurity awareness in China. Internationally, CSAC has assisted Sino-US Track 2 cybersecurity Dialogues, helping to organize bilateral cybersecurity roundtable talks with counterparts in the UK, France, Germany, India etc.13

**Technical and Academic Community**

**China Internet Network Information Center**

The CNNIC operates the country-code Top-Level Domain (ccTLD) of “.cn” and performs the duties of the national Internet Network Information Center, subordinated to the Chinese Academy of Sciences initially, and later transferred to the CAC and finally to MIIT. As an important infrastructure builder, operator, and manager of China’s information society, CNNIC is responsible for the operation, management, and service of national network basic resources; undertakes security assurance and technology research and development of national network basic resources; carries out Internet development research and provides advice; and promotes global Internet openness, cooperation, and technology exchange. CNNIC, serving as an important technical community

---


in China, has made many technical contributions in the field of Domain Name System (DNS) and plays an important role as a participant in global Internet technical communities such as ICANN, Internet Architecture Board, Internet Engineering Task Force, Asia-Pacific Network Information Center, etc.

**National Computer Network Emergency Response Technical Team/Coordination Center of China**

The CNCERT/CC, China’s computer emergency response team, was founded in 2001 as a non-governmental, non-profit technical institution. CNCERT/CC has branches in 31 provincial administrations and also hosts the “Anti Network-Virus Alliance of China,” an industry-wide anti-virus self-regulation initiative organization, as well as the “China Cyber Threat Governance Alliance,” yet another industry self-regulation endeavour to share cyber threats intelligence, against cybercriminals. CNCERT/CC has long been an active participant in cybersecurity diplomacy at ITU, Shanghai Cooperation Organization, Association of Southeast Asian Nations, BRICS, etc.

**Tsinghua University**

Tsinghua University is one of the most prestigious universities in China, with high calibre Internet researchers and students. It hosts the backbone network of the China Education and Research Network (CERNET). Given its rich technical and human resources, Tsinghua University has been leading the research in networking theories and has produced significant contributions to the technical community, such as contributing Internet standards of the IETF’s Request for Comments (RFCs).14 Tsinghua University has collaborated with cybersecurity companies such as 360, to launch joint labs and projects.

**Scientists**15

Scientists have played a key role in the evolution of cybersecurity technology and governance in China. *Hu Qiheng*, an academician of the Chinese Academy of Engineering, viewed as the Chinese mother of the Internet, has led and organized several essential projects and organizations including the direct connection of the CNNIC and ISC. In 2004, she was appointed by the United Nations as a member of the Working Group on Internet governance. *Wu Jianping*, Dean of National Engineering Lab of Next Generation Internet,

---


serves as professor in Tsinghua University and used to serve as Chairman of the Asia Pacific Advanced Network. He led the development of Chinese IETF RFCs and hosting of the IETF 79th Meeting in Beijing in 2010. Qian Hualin, as one of the important pioneers of China’s Internet, is among the “Forerunners of China’s Internet” and put multistakeholder governance into practice in China. In April 1994, he took part in China’s full functional connection to the Internet and served as the technical and administrative liaison between China and the Internet.

TWO STAGES OF CHINESE CYBERSECURITY GOVERNANCE

Although the Central Cyberspace Affairs Commission of China (中共中央网络安全和信息化委员会) places equal emphasis on development ( informatization) and cybersecurity, or so-called “development and governance” (发展治理), cybersecurity governance and Internet development are separate phenomena. Most public policies are aimed at guaranteeing cyberspace safety, while the development of the Internet has been left to the market economy rather than regulatory policies. From this perspective, the history of Internet “governance” in China is to some extent the history of cybersecurity governance.

The core issue as regards the multistakeholder model is the position and the role of the government. Thus, the historical evolution of the Chinese government’s position in cybersecurity governance provides a clear picture of how multistakeholder governance in China works.

Reviewing the history of cybersecurity governance in China from when the Chinese first accessed the Internet in 1994, we can see that its logic is different in the early days compared to the later period. The establishment of the Central Leading Group for Cyberspace Affairs directed by President Xi Jinping in 2014 (upgraded in 2018 as the Central Cyberspace Affairs Commission) was the turning point. China’s cybersecurity governance system began a transformation from the so-called “Nine Dragons Governing the Flood” (九龙治水) model, where the Internet is governed by multiple agencies reporting to single and centralized governmental management. (see Figure 8.1) The periods can be labelled the “pre-centralization period” and the “post-centralization period.” In the pre-centralization period, China’s model was to some extent

---

a typical Western-style multistakeholder model, while in the post-centralization period, a multistakeholder model with Chinese characteristics began to take shape, in which the key factor was the changing role of government. In the earlier period, China’s cybersecurity governance was characterized by a decentralized approach within the government while the post-centralization period marks a “re-centralization” of the government. The regime of cross-border data flows, like other cybersecurity governance fields, is a typical product of “re-centralization,” under the leadership of the CAC.17

Pre-centralization Period

In the pre-centralization period, the Internet was regarded as a technological “system” with a focus on the deployment and diffusion of digital technology. Cybersecurity governance in China was undertaken by a large number of scientists. From the very beginning of its access to the Internet, China seriously discussed how the Internet should be managed or governed, and eventually, a decentralized, scientist-driven model prevailed.

Lu Shouqun, who presided over the planning of several important Internet projects and was the head of China’s first Internet regulation preparation group, said in an interview, “the opening of China’s Internet was also the process of emancipation, opposing the obsolescent management system,

attaching importance to security and striking a good balance between openness and security.” 18 As Lu recalled, the State Information Technology Joint Office organized a cross-sectoral symposium on August 19, 1995, in which most experts and leaders from various ministries clearly expressed disapproval of governing the Internet through a “monopoly” model of single-agency governance. The symposium participants were in favour of the proposed model of establishing multiple Internet centres chaired by the Joint Conference on economic informatization of the State Council. It is worth noting that most of the early Internet and cybersecurity policy-making in China was completed by CNNIC, using a consensus-based approach led by scientists. 19

Subsequently, on January 15, 1996, the Interim Provisions on the Management of Computer Information Networks and International Networking in the People’s Republic of China (the so-called Internet Management Provisions, the first Internet regulatory document in China) was approved to establish four Chinese backbone networks. 20 This event was not only of epochal importance in breaking the sectoral monopoly and boosting the development of the Internet but also established the “Nine Dragons Governing the Flood” model of decentralization inside government. This marked the beginning of the pre-centralization period. 21 This design of institutions aligns with the inherent properties of the Internet and also contributed to the rapid development of the Internet in China in the early days.

From 1994 to 2014, legislation was limited to two instruments: the Decision of the Standing Committee of the National People’s Congress on Safeguarding Internet Security, composed of only seven articles adopted in 2000 and amended in 2009; and the Electronic Signature Law, which has been criticized for being incompatible with Internet governance and having no top-level institutional design, but precisely reflects the fact that the early approach to Internet governance in China was not top-down or centralized. The ISC was founded in 2001 by more than 70 organizations, including network operators, service providers, equipment manufacturers, system integrators, and scientific and educational institutions. The ISC was the first Internet industry organization in China and has shouldered the important responsibility of industry autonomy by issuing a large number of industry self-regulatory conventions.

---

It was founded and chaired by Ms Hu Qiheng, a highly respected scientist and academician of the Chinese Academy of Sciences, reflecting the distinctive self-governance characteristic of the industry and technical community.

On June 8, 2010, the Information Office of the State Council published its first white paper setting out China’s Internet policy, which covered active utilization, scientific development, legitimate management and security assurance. The document also put forward the concept of Internet sovereignty and began to articulate general ideas on the institutional construction of cybersecurity governance.

**Post-centralization Period**

With rapid digitalization in China, the Internet is no longer simply a technology, but a social force with empowering capabilities. The logic of China’s cybersecurity governance mechanism has accordingly begun to transform and has entered a post-centralization governance period. China’s societal structure is one of a “powerful government and weak society,” as reflected in the corresponding architecture of Internet governance. An important ideological change in this period is the rise of “cyber sovereignty” theory, where cybersecurity governance is considered a fundamental element of national sovereignty, emphasizing the need for the government to actively govern the sovereignty of its digital spaces, and thus to shift from a passive regulator to an active one. The reasons for this transformation are complex. On the one hand, the political and ideological attributes of the Internet became more apparent, especially after the Arab Spring in 2010 and the Snowden incidents in 2013, and the political influence of the Internet aroused important global concerns. On the other hand, the Internet-based information and communications technology industry has become an important arena for competition among countries, and digital technology has become a global force affecting national strategies, in which cybersecurity has become a core governmental concern.

The milestone marking the beginning of the post-centralization period was the establishment of the Central Leading Group for Cyberspace Affairs on February 28, 2014. According to the official announcement, Xi Jinping,

---


General Secretary of the CPC Central Committee, President of the State and Chairman of the Central Military Commission, personally served as the head of the Group. Li Keqiang and Liu Yunshan served as deputy heads, reflecting the will of the Chinese leadership to comprehensively deepen reform, strengthen the top-level design of cyberspace policy, safeguard national interests and promote the development of information technology. The CAC, as the executing agency of the Central Leading Group for Cyberspace Affairs, became the leader and promoter of cybersecurity and informatization development.

The first task for the CAC was to enhance the top-level design of cyberspace policy. The notion of “Internet Empower the Nation” (网络强国) became a national strategy, and “Internet+,”\(^\text{26}\) which actively promotes the development of the Internet industry, became a state-led development policy. The CAC also led the most important Internet legislation – the Cybersecurity Law (passed in November 2016) – which was a manifestation of the top-level design of China’s Cybersecurity regulation system. Then, the CAC led the organization of the World Internet Conference (WIC), the largest and highest-level Internet conference held in China, bringing unprecedented attention to cybersecurity governance into Chinese society while also drawing high-level attention from the international community. In the second year of the WIC in 2015, the CAC planned President Xi Jinping’s attendance and keynote speech and issued China’s famous “Four Principles and Five Proposals” for Internet governance, which were later transformed into the “Four Beams and Eight Pillars” of China’s cybersecurity governance regime. The CAC also planned President Xi Jinping’s speech at the National Conference on Cybersecurity and Informatization on April 19, 2016 (often referred to as the “419 Speech”), which proposed six core questions about different aspects of Internet development and the balance between cybersecurity and informatization.

The CAC also made great contributions to launching important instruments that pertained to China’s cybersecurity governance. The National Strategy for Cyberspace Security, released on December 27, 2016, and the Strategy for International Cooperation in Cyberspace, published on March 1, 2017, are two official documents that illustrate the Chinese policy on cybersecurity from domestic and international perspectives. Three more key instruments were released between 2019 and 2021: Jointly Building a community with a shared future in cyberspace, Action initiative for Jointly building a community with a shared future in cyberspace and Best Practice for Jointly building a commu-

\(^{26}\) The milestone event was the publication of Guiding Opinions of the State Council on Vigorously Advancing the “Internet+” Action by the State Council on July 1, 2015.
nity with a shared future in cyberspace. These reflect China’s understanding, initiative, and best practices of global Internet governance.

Although this series of actions were led by the CAC, non-governmental actors participated and influenced the formation of relevant policies and rules in an indirect way. For example, the Cybersecurity Law, the first piece of legislation, received a large number of comments from stakeholders during the drafting and two consultation processes, and the comments ultimately influenced the content of the law. The subsequent Data Security Law and Personal Information Protection Law similarly involved a large amount of social cooperation. The demands of enterprises especially were absorbed into the legal rules by way of consultation. Meanwhile, from the central CAC to provincial CACs and the WIC, professional advice on important topics of cybersecurity governance has been provided by expert advisory committees.

Additionally, the China Internet governance Forum (China IGF), which is organized as a multistakeholder model, also set up an expert advisory committee to solicit views from society as a whole to initiate discussions in an open manner. At this stage, China’s multistakeholder governance model allowed for the participation of enterprises, academic institutions, technical communities, and civil society, as well as government entities, in the government-led process according to their respective roles. All groups acted according to the established rules and became an important force in cybersecurity governance, gradually forming a new governance ecology.

MULTISTAKEHOLDER CYBER GOVERNANCE PRACTICES IN CHINA

Officials, experts, and scholars from different fields and professional backgrounds have made positive efforts to help Chinese communities integrate into the global Internet governance system to varying degrees. By identifying the dominant forces, several patterns are discernible. In addition to the noticeable government-led cybersecurity legislation described above, this part will introduce three other practices led by different groups of stakeholders.

28 For example, the Expert Advisory Committee of CAC for Zhejiang Province and the first Expert Advisory Committee of WIC.
Government-led Model: World Internet Conference

In October 2014, the first WIC was held in an idyllic small water-side town – Wuzhen in Zhejiang Province – which is near the headquarters of Chinese Internet tech company Alibaba. Even though it was hosted by CAC, the WIC adopted a multistakeholder model, open to all stakeholders to participate and even inviting different stakeholder groups to host the sub-forums, but under the leadership and stewardship of CAC. The first WIC invited participants from nearly 100 countries, among which were prominent Internet luminaries, ICANN, big Internet companies like Microsoft, Google, Facebook, Apple, Cisco, Qualcomm and Chinese Internet champions such as Alibaba, Tencent, Baidu and others.30

At the WIC 2015, President Xi Jinping called for building a community with a shared future in cyberspace in his opening remarks. This notion encapsulates China’s overall attitude towards cyberspace and its vision of a fair international cybersecurity regime. In the following WICs, this notion was developed further. In October 2019, at the 6th World Internet Summit, a formal concept document, named “Building a Community with a Shared Future in Cyberspace,” was published. In 2022, the WIC evolved into an international organization led by CAC.31

In short, WIC is now the official multistakeholder platform for the Chinese government to promote its principles and norms in cyberspace and cybersecurity, in a multistakeholder fashion.

Private Sector-led Model: Internet Security Conference32

The Internet Security Conference is a series of annual events hosted and organized by Qihoo 360, a privately owned security vendor in China. The founder of Qihoo 360, Mr Zhou Hongyi, and his company, employed a free service model to disrupt the anti-virus market. In just a couple of years, 360 APP, the flagship product of Qihoo 360, has been installed by millions of users and the 360 Antivirus suite has become a must-have tool for Chinese Internet users.

To put a positive spin on its business, starting in 2013, 360 began to hold a yearly Internet Security Conference, inviting government agencies, cyberse-

security vendors, researchers, and hackers to discuss a wide array of cybersecurity issues, and of course, to showcase 360 services.

The Internet Security Conference 2014 invited Tom Ridge, former Secretary of the Department of Homeland Security of the US, and Fred Cohen, computer virus guru, to attend. Guo Qiquan, the CTO of the network security bureau of the Ministry of Public Security, Professor Wu Hequan, a member of the Chinese Academy of Engineering, and leading experts on cybersecurity were also invited to the conference.

Ensuing Internet Security Conferences have had high visibility among different stakeholders. John A. Davis, CSO of Palo Alto Networks and former US Army Major General, and Denis Davydov, Director-General of Russian Secure Internet Alliance, both attended Internet Security Conference 2016. Former US Navy Admiral Bill Owens attended in 2017, and former head of cyber operations at US Cyber Command, retired Major General Brett Williams, was a participant in 2018. However, high-profile figures from the US stopped attending Internet Security Conference in 2019 and 2020. More Israeli cybersecurity professionals have been participating in the ISC of late.

**Technical Community-led Model: IETF/ICANN Conference in China**

As the operating organization of ccTLDs and an important member of the technical community, CNNIC hosted the 14th and 46th conferences of ICANN. The 14th ICANN conference in 2002, held in Shanghai and co-hosted by CNNIC and ISC, was the first large-scale international Internet conference held in China and had a profound impact on the Chinese Internet technical community. The 46th conference was held in Beijing, co-hosted by CNNIC, the China Organizational Name Administration Center and ISC. The number of participants reached 2,500, which was the highest recorded at that time. CNNIC has also hosted large-scale international conferences such as the Asia Pacific Network Information Centre Conference in 2009 and helped to open channels of communication between Chinese Internet communities and international organizations.

The 79th IETF meeting, initiated and hosted by Tsinghua University and co-organized by ISC and CNNIC, was held at the Shangri-La Hotel in Beijing from November 7–10, 2010, which was also the first time that IETF held a meeting in China. Before the IETF China meeting, the Chinese technical community had already been deeply involved in the IETF and made many contributions. Research institutions and enterprises such as Tsinghua University, Huawei, China Mobile and CNNIC have been widely involved in the development of international Internet standards. The leader of this conference was the computer department of Tsinghua University, led by Professor Wu Jianping. He and his team worked actively to make the IETF convene smoothly in China.
CNNIC and Tsinghua University have not only participated in Internet global governance work technically and contributed technical standards such as RFC of IETF, but more importantly, they streamlined the transformation of such technical influence into governance engagement and directly promoted better connections between China and international organizations and the further integration of China into the global cybersecurity governance system. This path reflects the multistakeholder path led by the technical community.

**Hybrid Model: Sino-US Cybersecurity Dialogue**

Track 1.5 and Track 2 Dialogues between countries can serve as another mode of multistakeholder cyber diplomacy from a national and diplomatic perspective. Sino-US cybersecurity diplomacy epitomizes multistakeholder diplomacy practice, which involves not only official channel diplomacy but also unofficial Track 2 diplomacy led by think-tanks, private sector actors, and even individuals.

The first cybersecurity dialogue was proposed by then US President Barack Obama, and echoed by Chinese President Xi Jinping, leading to the Sino-US Strategic Security Dialogue framework in 2013. At this dialogue, both sides agreed to set up a cybersecurity working group to discuss matters of mutual interest. At the first cybersecurity dialogue, the Chinese delegation, led by a state councillor, was composed of officials from the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Public Security, Ministry of Industry and Information Technology, Ministry of Commerce and News Office of State Council. Likewise, the United States was represented by the Department of State, Department of Defense, Department of Homeland Security, Department of Justice, Department of Treasury, Department of Commerce, Federal Bureau of Investigation, and National Security Council.

Accompanying formal Track 1 diplomacy, there was also a Track 2 Dialogue between the American and Chinese non-governmental think-tanks, cybersecurity experts and private sector actors to supplement the Track 1 Dialogue. Compared with Track 1 diplomacy, Track 2 arguably allows more room for both sides to discuss thorny cybersecurity topics before it is presented for official discussions.

Through Track 2 diplomacy, popularized in the 1980s, China leveraged “Ping-Pong Diplomacy” (乒乓外交) to break the ice in the Sino-US relationship.33 In the field of cybersecurity during the Trump administration, there

---

33 Ping-pong diplomacy refers to the exchange of table tennis (ping-pong) players between the US and China in the early 1970s, which paved the way for President Richard Nixon’s visit to Beijing in 1972 and has been seen as a key turning point in
was Track 1 Dialogue in Washington DC, and Track 2 Dialogue in Beijing in 2017. After that, because of the US sanctions on China’s technology champion Huawei and the ensuing tech cold war between two nations, the Dialogue was all but suspended.

CONCLUSION

Ms Hu Qiheng recalled the history of China’s Internet development in 2013 with emotion: “One thing I am proud of is that the development of China’s Internet is basically consistent with the global spread of the Internet. The main driving force is the initiative spontaneously formed by the bottom-up scientific and technological community, and a multistakeholder governance structure has been formed.” However, in its official wording, the Chinese government supports a multilateralist approach based on cyber sovereignty, which is often interpreted to mean China pursues only top-down and centralized Internet governance, leaving no room for multistakeholder governance or diplomacy. However, this understanding, as this chapter has sought to show, is neither objective nor fully accurate.

Multistakeholder cybersecurity governance in China requires an insider’s perspective as well as a historical perspective. After examining the history of cybersecurity governance in China, this chapter finds that there are two historical periods, the “pre-centralization period” and the “post-centralization period.” The multistakeholder approach in the first stage was Western-style and in line with international standards. After further integration with China’s local governance experience, a Chinese-style multistakeholder governance model gradually materialized, which is still evolving.

China has a defensive mentality towards global governance, so it chooses to use the government as a spokesperson. With respect to domestic governance, China’s Internet governance has cybersecurity as its policy concentration. A traditional unified central government habit of thinking becomes a cultural behaviour and translates into the structure of modern politics. However, under the wave of globalization, China has accepted foreign ideas, and after the continuous promotion of reform and opening-up, an external impetus has emerged that continues to make Chinese governance more modern, rationalized, and with a Westernized tinge, to form its own model.


INTRODUCTION

Indian diplomacy has always accorded a central role to the state in its approach to global negotiations. Yet while formal mechanisms to contribute have not always existed, various stakeholder groups have impacted the negotiating stances and approaches adopted by the Indian government at several global negotiations. This approach continues as India engages with a range of technology regimes, including that of cybersecurity regime formation.

Convergence of interests with that of the state and mediums through which interests can be asserted by each non-state actor has impacted the extent to which these interests were represented in global negotiations. India has been non-specific when it comes to controversial fissures in global cybersecurity negotiations. Further, there has been no “conscious structuring of mechanisms” from India to facilitate multistakeholder cyber diplomacy.

Additionally, none of the actors in the Indian cybersecurity ecosystem (hereinafter “stakeholder groups”), including the government, private sector, media, and civil society (which includes experts and advocacy groups) have articulated or even recognised a clearly defined interest or “stake” that they want India to bring to global negotiating tables. Instead, much of the focus has been on shoring up domestic cybersecurity resilience and building capacity, which has also been the emphasis of India’s diplomatic contributions abroad. All stakeholders are thus relatively satisfied with the outcome, and there is a negligible clash of competing interests between stakeholders because they do not perceive yet a clearly defined cost or opportunity in shaping the global cybersecurity regime.

1 Karthik Nachiappan, Does India Negotiate (Oxford University Press, 2019) 194.
2 Nachiappan, Does India Negotiate, 194.
Studying India’s approach to cyber norms formulation offers an opportunity to unpack this unique case characterised by a relative lack of participation and “passive” engagement by all stakeholder groups, and offer recommendations.

This chapter is in three parts. First, it evaluates the interests and actions of each stakeholder group in India with respect to cybersecurity regime formation, and how these actions (or lack thereof) are interdependent. In the second section, it highlights India’s contributions to global cyber norms processes and evaluates how this has been shaped by the stakeholder ecosystem. In the final section, the chapter offers recommendations for more optimal multistakeholder engagement going forward.

Methodology

To supplement and clarify publicly available information on this multistakeholder ecosystem on cybersecurity norms formulation, I conducted a number of interviews with key stakeholders to gain insights into the processes, actors and interests involved. Some interviewees preferred to remain anonymous. To the extent possible, I have attempted to corroborate information obtained in interviews through publicly available primary and secondary sources.

ACTIONS AND ENGAGEMENT BY STAKEHOLDER GROUPS

Each stakeholder group in the Indian ecosystem impacts and is impacted by the actions of all other stakeholder groups. With cybersecurity regime formation, the non-committal actions of each stakeholder group have reinforced each other, leading to limited engagement or contestation between groups. In this section, I delve into a detailed evaluation of the contributions of each stakeholder group on India’s approach to cyber norms formulation processes.

Government

The Indian delegations at the United Nations General Assembly Committee on Disarmament and International Security (“First Committee”) cyber norms processes have been led by the Ministry of External Affairs, sometimes accompanied by the National Cybersecurity Coordinator as well as representatives from other concerned ministries,3 including the Ministry of Electronics.

---

3 Raman Chima, email message to author, August 12, 2022.
India’s “passive” multistakeholder cyber diplomacy

and Information Technology. With respect to Internet governance regimes, representative delegations from the Ministry of External Affairs (MEA) have endorsed a nuanced or limited view of multistakeholderism. At the second Meeting of the Working Group on Enhanced Cooperation in Geneva (2014), the MEA representative stated that multistakeholder inputs were useful in policy formulation but not in implementation and enforcement, which should remain the domain of states. This was echoed in India’s contribution at the NETmundial Global MultiStakeholder Meeting on the Future of Internet governance in 2014 which stated that Internet governance should be “multilateral, transparent, democratic, and representative, with the participation of governments, private sector, civil society, and international organizations, in their respective roles.”

In cyber norms conversations, including at the Open-Ended Working Group (OEWG), the Indian delegation has largely remained non-specific on the nature and extent of multistakeholder participation in cybersecurity regime formation processes. However, India has never opposed multistakeholder cooperation. In fact, a statement by the Foreign Secretary at the United Nations Security Council Open Debate on Cybersecurity explicitly mentioned that “multi-stakeholder involvement would help in achieving” commonly agreed rules and norms in cyberspace. Further, Indian delegates observed but did not speak at the OEWG intersessional multistakeholder meeting in December 2019. There was also a verbal nod to the importance of

---

4 India’s lead interlocutor at the recently concluded OEWG and GGE discussions was Dr S. Janakiraman, Joint Secretary of the Cyber Diplomacy Division and E-governance and Information Technology. At the 2016/17 GGE, India was represented by Santosh Jha, who was then head of the MEA’s Policy Planning Division.


7 The NETmundial Initiative that followed the conference was discontinued and key partners such as the World Economic Forum withdrew.


industry stakeholders in implementing Confidence-Building Measures at the Eighth meeting of the first substantive session of the OEWG.\textsuperscript{10}

Despite endorsements of multistakeholder contribution to regime formation, India has not formally engaged in multistakeholder diplomacy in cyber norms processes – that is, the delegations have generally not formally included participation from the private sector or expert groups.\textsuperscript{11} The only exception was a multistakeholder delegation sent to consultations conducted by the Netherlands government on Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.\textsuperscript{12}

The MEA has not opened a public call for comments for stakeholders to give inputs on India’s negotiating stances or represent India at cyber norms negotiations. Instead, the Ministry has engaged with other actors in two important ways. First, it has requested \textit{ad hoc} legal or policy inputs from experts on global cyber norms processes on at least five occasions.\textsuperscript{13} However, on all such occasions, there was no substantial engagement with the experts to concretely demonstrate how these inputs were used by decision-makers. Second, the MEA has funded or participated in conferences organised by think-tanks on questions of technology and global governance, which usually include at least one session or panel on cybersecurity norms formulation.\textsuperscript{14} These conferences are well attended by all stakeholder groups, and panels on cybersecurity norms formulation involve multistakeholder participation. While the impact of these conversations is difficult to assess, they are an important means of fostering public discussion on the topic.

Notably, India also hosted the fifth and latest edition of the Global Conference on Cyberspace, as an evolution of the London Process, which started in 2011.\textsuperscript{15} It was a grand multistakeholder event where international leaders, policymakers, industry, experts, academics, and security research-


\textsuperscript{11} Confirmed in an interview with Arun Sukumar.

\textsuperscript{12} Interview with anonymous sources.

\textsuperscript{13} Confirmed from interviews.

\textsuperscript{14} This includes CyFy, Observer Research Foundation’s conference on technology, security and society since 2016, Carnegie India’s Global Technology Summit since 2016, and the Raisina Dialogue since 2016, which is India’s flagship conference on global issues with cross-sectoral multistakeholder participation and inevitably includes several key panels on technology governance and the future of conflict.

\textsuperscript{15} Conference website at https://digitalindia.gov.in/content/5th-global-conference-cyberspace-2017.
India’s “passive” multistakeholder cyber diplomacy 205

ers met to discuss issues and challenges in the optimal use of cyberspace.16 A journal following the Conference titled “Our Common Digital Future” was published by the Observer Research Foundation, featuring contributions from several prominent voices across stakeholder groups.17 However, several civil society organisations criticised the exclusion of prominent voices within the Indian community owing to their disagreements with government policy on digital identity, leading to a “shallow conversation.”18

Apart from the short-lived reputational advantage of being the first country not from the Organisation for Economic Cooperation and Development group19 to host the conference, there is again no evidence of sustained engagement with the process. Consequently, it has played a negligible role in either fostering multistakeholder engagement or driving India’s negotiating stances on cybersecurity regime formation.

The office of the National Security Council Secretariat (NSCS), which falls under the aegis of the Prime Minister’s Office, has conducted two important formal multistakeholder exercises. First, after the collapse of the UN Group of Governmental Experts (UN GGE) talks in 2017, it set up a multistakeholder committee to “suggest policy and strategy for India for development and negotiating of cyber norms.”20 The committee was chaired by Asoke Kumar Mukerji, India’s former Permanent Representative to the United Nations, former Deputy National Security Advisor Arvind Gupta (presently Director of think-tank Vivekananda International Foundation), representatives from the Ministry of Defence, Ministry of Electronics and Information Technology, academia and industry.21 While an unidentified member of the committee wanted to steer the community to push India to become “a leader for the

---

21 Srivas, “After UN Talks on Cyber Norms Collapse, India Starts Chalking out own Strategy.” Interview with Arun Sukumar.
development of global cyber norm policy," others were more circumspect in commenting on the norms that India might want to formulate. The substantive report submitted by the committee to the Prime Minister’s Office (PMO) has not been made public, and there has been no public reference made to its processes, conclusions or impact by the government. Apart from one article covering the origins of the committee by online news portal The Wire, this committee saw no media coverage either. This structured exercise led by key domain experts was an important mechanism for soliciting multistakeholder feedback and crafting a robust approach to cyber norms. Yet the absence of a statement from the government on the work of this distinguished committee combined with the lack of public information on how this committee may have contributed to shaping India’s stances at global cyber norms formulation settings impedes a thorough evaluation of its precise contribution to Indian multistakeholder diplomacy.

The NSCS also organised an open consultation on India’s National Cybersecurity Strategy (NCSS) that invited written submissions from all interested stakeholders. The NCSS was to be based on three pillars: cyber secure; secure (national cyberspace) and strengthen (structures, people, processes, capabilities); and synergise (resources including cooperation and collaboration). In the public call, there was no request for inputs on India’s negotiating positions. As per the National Cybersecurity Coordinator, Lt Gen. Rajesh Pant, this call received robust multistakeholder engagement with over three hundred submissions from companies, business coalitions, and all civil society sub-groups. The NCSC also invited key entities from all stakeholder groups to make presentations building on their submissions. A public draft of the strategy is yet to be released. While consultations around the NCSS were undoubtedly a multistakeholder process, the extent to which multistakeholderism impacted the strategy – both in terms of its domestic posture, and its framework for India’s global normative stances – can not yet be determined.24

---

22 Srivas, “After UN Talks on Cyber Norms Collapse, India Starts Chalking out own Strategy.”
24 Multistakeholder actors interviewed (Trisha Ray and Udbhav Tiwari) and other anonymous individuals agreed.
Private Sector

The corporate sector – individual entities and business coalitions – has not made any direct public comments on India’s negotiating stances at cyber norms processes. Foreign technology companies that have India-based public policy teams, including Google, Facebook, Microsoft, and Twitter, do not have dedicated individuals in India engaging in cyber norms diplomacy. Domestic organisations have also not commented on the global cybersecurity regime or India’s role in it at all. However, global multistakeholder agreements, most notably the Paris Call for Trust and Security in Cyberspace, have seen participation from Indian industry stakeholders. At the time of writing, this includes 20 entities, including law firms and public enterprises, and important Indian business coalitions such as the Federation of Indian Chambers of Commerce and Industry and Confederation of Indian Industry. The scale of uptake is a result of sustained outreach by the French government, with efforts from individuals based both in Paris and New Delhi. Microsoft’s efforts to get both the Indian government and others to sign on were driven by their Digital Diplomacy Team based in Europe and the United States with limited intervention from individuals or teams based in India. Microsoft has also been involved with, and supported, private gatherings on the sidelines of summits and conferences.

Technology companies are driven primarily by business interests. The public policy and government relations teams are designed to shape domestic policy in a manner that benefits these interests. Therefore, they are preoccupied with regulatory issues such as intermediary liability, data protection, and cross-border data flows that would lead to immediate financial compliance costs, and reputational costs in cases of non-compliance. India’s positioning on cyber norms at the First Committee impacts them only indirectly – when it translates into domestic policy or law that either undermines or bolsters their business interests. For example, telecom companies have vociferously weighed in on decisions such as whether Huawei should be allowed to participate in 5G trials.

---

26 Interview with anonymous source.
27 Interview with anonymous source.
28 This paragraph was aided by my interview with Udbhav Tiwari.
29 Speaking at the World Economic Forum in 2019, Bharti Enterprise (Airtel) Chairman Sunil Mittal was quick to dismiss the notion that 5G should be politicised, and further stated that “[Huawei’s] products in 3G and 4G are significantly superior to Ericsson and Nokia. I use all three of them.” In December 2018, after the Telecom
Unsurprisingly, the private sector has been far more active when it comes to devising domestic frameworks for cybersecurity. Cyber hygiene, resilience, and trusted supply chains are critical to preventing financial and reputational costs brought about by data breaches or falling prey to cyber criminals. For example, the Data Security Council of India has made detailed publicly available submissions in response to stakeholder consultations on the NCSS.\(^3\) Both these submissions and other publicly available statements by business entities focus on issues directly connected with domestic resilience. These include supply chain security, protection of critical information infrastructure, security in payment services, budgetary allocation to cybersecurity, standards development, and public–private partnerships. While passing references were made to the significance of norms formulation processes and cyber diplomacy in these submissions, no concrete positions on international law or cyber norms were posited.

Historically, there has been a noted lack of private–public congruence and coordination when it comes to implementing cybersecurity frameworks within the country. In 2012, a Joint Working Group (JWG) on Engagement with the Private Sector on Cybersecurity was established by the PMO, which was supposed to serve as a platform for fostering continued and sustained collaboration.\(^3\) However, the JWG failed to produce any concrete outcomes due to mutual mistrust on the part of the private sector and the government of the other’s commitment to and capability to guarantee cybersecurity.\(^3\) The Equipment and Services Export Promotion Council argued for a ban on the grounds of national security, COAI sent a letter to the Department of Telecommunication arguing that Huawei was “suitably equipped” to build 5G capabilities in the ecosystem and comply with government requirements. Mukesh Ambani of Reliance, on the other hand, who stands to benefit from Huawei’s exclusion owing to the costs it would impose on competitors, has proudly claimed to former President Donald Trump that Reliance uses no Chinese parts. Arindrajit Basu and Justin Sherman, “The Huawei Factor in US–India Relations,” The Diplomat, March 22, 2021, https://thediplomat.com/2021/03/the-huawei-factor-in-us-india-relations/.

\(^3\) Data Security Council of India, National Cybersecurity Strategy 2020: DSCI Submission (DSCI, 2020), https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20Submission.pdf. The Data Security Council of India (DSCI) is a premier industry body on data protection and cybersecurity set up by NASSCOM, which is the premier trade body and chamber of commerce of the technology industry in India, comprising over 3,000 members that span both Indian and foreign organisations.


\(^3\) Hannes Ebert, “Hacked IT Superpower: How India Secures its Cyberspace as a Rising Digital Democracy.” India Review, 19, no. 4 (October 2020), 376,394 (“the
key point of departure appeared to be the industry’s desire to self-regulate in order to prevent needless compliance costs – a notion championed by leading coalitions like NASSCOM. However, the multistakeholder approach to the NCSS in 2020 indicates that these tensions have been ironed out, and both the government and private sector have recognised the need for greater cooperation to tackle the growing array of shared threats to both public and private information infrastructure. It remains to be seen whether this synergy will extend as India engages with cyber norms.

Civil Society and Media

There has been limited interest and engagement with India’s approach to cyber norms formulation from all civil society sub-groups. The most pronounced engagement has come from experts. This includes research produced by think-tanks and research institutes specialising in technology policy issues such as data protection or intermediary liability, and from older think-tanks that are working on questions of security and governance.

In addition to publicly available research, these institutions have organised closed-door multistakeholder roundtables, and larger conferences like CyFy hosted by the Observer Research Foundation (ORF) with the aim of fostering more public discourse on cyber norms.

Experts from India have also directly engaged with global multistakeholder and multilateral processes (detailed in Table 9.1). Representatives from the Centre for Communication Governance at the National Law University, New Delhi (CCG) and MediaNama (a leading media house covering technology issues) attended the OEWG multistakeholder inter-sessional meeting in December 2019. The Centre for Internet & Society (CIS) and CCG also made submissions in response to the Pre-Draft of the OEWG report commenting on all five issues covered in the Pre-Draft report. Representatives from CCG and CIS also aired their views on ‘Existing and Emerging Threats’ at Let’s Talk Cyber, an informal multistakeholder virtual dialogue organised in December.
2020 to support the OEWG discussions then ongoing. ORF President Samir Saran was a Commissioner in the multistakeholder Global Commission on the Stability of Cyberspace, contributing to their efforts in articulating norms for stable cyber governance.

Table 9.1 Direct engagement of stakeholder groups in India with global norms formulation processes

<table>
<thead>
<tr>
<th>Forum/initiative</th>
<th>Direct international participation by Indian stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Commission on Stability of Cyberspace (2017–2019)</td>
<td>Latha Reddy served as Co-Chair, Samir Saran was a Commissioner. Experts from CIS, Vivekananda International Foundation and ORF responded to public consultations and provided expert advice</td>
</tr>
<tr>
<td>Paris Call for Trust and Security in Cyberspace (2018)</td>
<td>Participation from over 20 business and civil society entities in the call</td>
</tr>
<tr>
<td>Global Forum on Cyber Expertise</td>
<td>Indian business coalition NASSCOM is a partner</td>
</tr>
</tbody>
</table>

Former diplomats, including former Deputy National Security Adviser Latha Reddy and former Permanent Representative to the United Nations Asoke Kumar Mukerji, have attempted to influence public discourse policymaking on cyber norms through formal engagements, writing and public speaking. In addition to chairing the multistakeholder study group set up by the NSC after the breakdown of the 2017 GGE, Mukerji has written and spoken extensively on the need to conceptualise an international convention for cyberspace. Reddy served as a Commissioner with the Global Commission on Internet governance 2014–2016, and as a Co-Chair of the Global Commission on the

---

35 As of November 20, 2021, the session can be accessed at: https://letstalkcyber.livecasts.eu/existing-and-emerging-threats.

36 As of November 20, 2021, Samir Saran’s Commissioner profile: https://cyberstability.org/commissioners/samir-saran/.

India’s “passive” multistakeholder cyber diplomacy

Stability of Cyberspace from 2017. Amandeep Gill, a career diplomat from India, was appointed by UN Secretary-General António Guterres in 2018 as the executive director of the UNSG’s High-Level Panel on Digital Cooperation. Gill was more recently appointed as the UNSG’s Envoy on Technology.

Advocacy groups are also yet to either apply external pressure on or engage directly with the government on cyber norms. India-based NGOs have focussed on digital rights issues such as the implementation of facial recognition technology and domestic cybersecurity issues such as the penalising of cybersecurity researchers for vulnerability disclosures. Global advocacy groups like Access Now which have a presence in India, have directed their cyber norms advocacy efforts to direct engagement with the UN processes or with other countries where the foreign policy establishment has been more receptive to their inputs.

Significantly, unlike other negotiations at other global governance regimes such as the World Trade Organization or nuclear security, the Indian media has been strikingly quiet when it comes to covering cyber norms negotiations. Leading media houses, both print and television, have not covered these negotiations in a sustained fashion that would allow them either to pin accountability on Indian negotiators or catalyse public discourse, as it has done with other diplomatic endeavours. While experts, including prominent former diplomats and legislators, have written op-eds on cyber norms processes, print and digital media outlets were very limited in their coverage. There were under ten news articles covering cyber norms negotiations published in online or print media since 2017. Further, the articles on cyber norms processes covered

---

40 As of November 20, 2021, Internet Freedom Foundation’s advocacy on facial recognition as displayed on their website: https://internetfreedom.in/tag/facial-recognition/.
41 As of November 20, 2021, IFFs advocacy efforts on cybersecurity: https://internetfreedom.in/dont-penalise-cybersecurity-researchers/.
42 Interview with Raman Chima.
44 Shashi Tharoor, “Kudankulam is Over, but are we Prepared for Next Breach: Tharoor,” The Quint, October 31, 2019, https://www.thequint.com/voices/opinion/kudankulam-cyber-attack-spy-pakistan-china#read-more%20
45 Thanks to Rajat Mishra for his research assistance on this question.
bilateral agreements between India and another country, rather than the negotiations themselves. There was no coverage in the media of the successful conclusion of either the GGE or OEWG consensus reports earlier in 2021. A notable exception is MediaNama, an online news portal dedicated to technology which has both covered cyber norms discussions and questioned Lt Gen. Pant on the OEWG discussions.

With the other stakeholder groups being non-committal, experts have also had limited space for interventions. Notwithstanding some notable contributions to cyber norms debates from civil society, the extent of engagement has paled in comparison with engagement on domestic cybersecurity issues and domestic policy formulation. There continues to be much more public discourse and interest in researching data breaches or attacks to information infrastructure. These issues impose greater short-term costs on the government, private sector and individuals, thereby capturing public imagination more potently than slow-paced discussions at global forums. Further, the government itself has not invested significantly in seeking formal inputs from experts or publicly discussing their contributions either with traditional media or social media – something it has done much more with other bilateral or multilateral diplomatic engagements.

INDIA’S NEGOTIATING STANCES AT GLOBAL CYBER NORMS PROCESSES

In this section, I evaluate the extent to which the passivity of all stakeholder groups shapes the Indian delegation’s approach at UNGA First Committee negotiations. India has adopted a largely non-committal stance on contentious issues at all fora that make up the cybersecurity regime complex.

In the First Committee, India has voted for resolutions that set up both parallel processes on norms formulation for responsible state behaviour in cyberspace.


48 Interview with Raman Chima.

49 This section has been adapted from Arindrajit Basu and Karthik Nicholson, “Will India negotiate in cyberspace?” (forthcoming in Hybridity, Conflict and the Global Politics of Cybersecurity) [file on source with author].
space. Despite being a member of five out of the six UN GGEs at the time of writing, India has not yet released a consolidated public statement articulating its position on how specific points of international law, such as self-defence or International Humanitarian Law, apply to cyberspace. However, India has made some references to international law. During a speech in 2016, Deputy National Security Advisor Dr Arvind Gupta made a reference to the Tallinn Manual and opined that “In India’s point of view, while [it was] a useful exercise, does not reflect the existing law on the subject because of the absence of state practice which is critical for development of customary international law.”50 At the OEWG, India has endorsed the need for UN members to develop a common understanding of how international law applies to cyberspace under the auspices of the UN. At the 2022 OEWG deliberations, India stated that extra-territorial cyber operations might constitute a breach of sovereignty,51 which has already been recognised by a number of other states.52 However, India has not waded into the controversial normative debates on whether sovereignty is a rule or principle of international law or opined on the specific kinds of cyber operations that may constitute a breach of sovereignty.

Indian delegations made non-specific statements at the 70th53 and 71st sessions54 of the UN General Assembly but again did not touch on any substantial points of debate. India’s interventions at the OEWG have also stuck to issues that are not controversial and affirmed the need for consensus on points being

54 “Subject: UNGA Resolution 70-237 Entitled Developments in the Field of Information and Telecommunications in the Context of International Security.”
debated by other states and made suggestions on the language of the final reports.56

India has been firm and persistent at OEWG conversations on trusted supply chains, and protection of critical information infrastructure, and has also advanced a coherent and well-designed agenda for capacity building, including through the development of a Global Cyber Security Cooperation Portal.58 This emphasis stems from a convergence of state interests with that of the private sector. These topics were core issues discussed by the DSCI in its submission on the National Cybersecurity Strategy, which means that these are core issues for industry. While the DSCI does not explicitly mention cyber norms regimes, domestic interest in these issues may have been a factor in shaping India’s negotiating stance. In addition, trusted supply chains have been a crucial focus of India’s security policy, especially after growing tensions on the Sino-Indian border.59 The fact that industrial players critical to India’s economy are stressing the same factors enables Indian delegations to sidestep other debates at cyber norms forums, such as those on international law, and concentrate on issues which align with more short-term domestic cybersecurity priorities. This specific example demonstrates that core domestic interests can be furthered through the First Committee processes, but these interests cannot be shaped by industry alone. There is a need for sustained engagement with a broader range of stakeholders, as I discuss in the final section of this chapter.

55 For example, see statement made by the Indian delegation at the First Substantive Session of the OEWG where they acknowledged the lack of consensus on the applicability of International Humanitarian Law, self-defence and definition of cyber attack and noted the importance of forging that consensus but refrained from adopting a specific view on these questions. Andrijana Gavrilović, “Open-Ended Working Group (OEWG) – First Substantive session,” September 2019, https://dig.watch/resources/1st-meeting-first-substantive-session-open-ended-working-group-oewg.


57 These have been stressed on by the Indian delegation right from the first substantive session in September 2019 to the Explanation of Position on the final report in March 2021, in addition to being referred to in India’s comments on the Zero Draft circulated in February 2020.

58 Permanent Mission of India to the UN, “Statement on ‘Existing and Potential Threats’ Cluster.”

India had referred to and endorsed a norm condemning offensive cyber operations at the first substantive session of the OEWG, with Indonesia, Iran, Pakistan, Cuba, and Nigeria. However, there was no further commitment to this by Indian delegations at subsequent sessions. The absence of this norm in the final OEWG report elicited no mention from the Indian delegation’s Explanation of Position or comments on the Zero Draft submitted by the Indian delegation towards the end of the process in 2021.

Beyond the UN, India has been a recalcitrant participant in multistakeholder processes on cybersecurity. India has not yet endorsed the Paris Call for Trust and Security in Cyberspace championed by Microsoft and the French government in 2018. Some claim that the reason for this is a reference to the Budapest Convention, a treaty which India has not signed, in the text of the Paris Call. Despite calls from industry leaders such as Microsoft’s President Brad Smith to join the Paris Call, there has been no public justification advanced by New Delhi for its refusal to endorse it. This should not be strictly interpreted as India’s rejection of multistakeholder cyber diplomacy. Instead, it is a result of internal processes within India’s diplomatic machinery that requires consultation for India to join any global process. India has been a member of other multistakeholder forums focussing on cybersecurity such as the Global Forum on Cyber Expertise (GFCE) since 2015 – a multistakeholder endeavour focussing on capacity building. Notably, the Indian government has not made a public statement about its membership or reported on its engagements within the GFCE framework, even though the GFCE was first announced through the Delhi Communiqué at the conclusion of the GCCS in 2017.

Despite clear economic and security interests in cyberspace, India does not view the outcome of normative debates as a priority to further these interests yet. Instead, India prefers focussing on building a resilient domestic cybersecurity architecture, cooperation on capacity building abroad, and man-

---

63. Interview with Arun Sukumar and one anonymous stakeholder.
64. As of November 20, 2021, the page here describes the GFCE: https://thegfce.org/about-the-gfce/.
aging bilateral relationships with competitors and allies.\textsuperscript{66} India’s non-specific stance arguably enables capacity building at home without the constraints of long-term commitments or being boxed into an ideological corner at this stage.

Existing institutions working on cybersecurity and cyber diplomacy are aplenty, but there is no clear coordinating mechanism operationalised yet, which prevents India from pushing forth a robust “all of government” stance.\textsuperscript{67} The push for coordination would be much stronger if the negotiations were seen as a strategic priority, as has been the case with India’s data localisation push that has seen strong coordination from the MEA, Ministry of Commerce and several other ministries both on domestic and foreign policy clarity.\textsuperscript{68}

Further, there has been limited public engagement driven by either the government or media on cybersecurity processes. There have been very few press briefings or widely disseminated information on global cybersecurity processes, and India’s role in shaping them. Advocacy groups have neither exerted pressure on the government nor built public sentiment in a bid to demand more accountability. The media has rarely asked questions or shaped public discourse in a manner that would compel the government to amend its negotiating stances.

While there have been limited instances of synergy between the positions articulated by industry and India’s contributions to global debates, there is no impetus for the government to negotiate consistently on behalf of a certain domestic constituency or to further domestic political interests, as has been the case with digital trade negotiations where both industry bodies and civil society voices have been far more active.

While it is too early to brand India’s approach to global cyber norms negotiations, a passive multistakeholder ecosystem has certainly played a role in how India has negotiated, in confluence with the government’s appreciation of policy priorities and the institutional machinery galvanised to serve these priorities.

\textsuperscript{66} For a cogent evaluation of India’s bilateral cyber relationships both with the United States and China, see Arun Mohan Sukumar, “Look West or Look East?: India at the Crossroads of Cyberspace” in Paul Cornish (ed.), \textit{The Oxford Handbook of Cybersecurity} (Oxford: Oxford University Press, 2021).

\textsuperscript{67} See, for example, Cyber Solarium Commission set up in the US to reform the functioning of government cybersecurity institutions. As of November 20, 2021, their website is here: https://www.solarium.gov/.

RECOMMENDATIONS FOR MULTISTAKEHOLDER ENGAGEMENT

As transnational threats to India’s cyber infrastructure proliferate, the country’s stakes in shaping global rules and accountability frameworks will increase. India’s strategy and approach to cyber norms formulation will require frequent evaluation and course alteration, given the rapidly evolving technology and security developments at home and abroad. For this, vibrant multistakeholder engagement from a variety of stakeholder groups will be critical.

Yet, the implications of global norms formulation processes are not immediately apparent to all stakeholders and the present state is unlikely to change soon. This is somewhat of an inevitability. Domestic digital rights concerns and cybersecurity challenges impose immediate costs on businesses and civic space and perhaps rightly serve as a priority for multistakeholder engagement. However, a continued lack of engagement will result in rules getting shaped globally with limited input from Indian stakeholders, thereby limiting the bargaining room available should stakeholders have a clearer picture of opportunities and costs in the future.

Therefore, work can be done to alter the passive approach in the multistakeholder ecosystem. I conclude with three recommendations. First, the government itself needs to communicate its role in these processes more effectively to the public and incubate a more transparent process for driving widespread, meaningful and genuine engagement with a range of stakeholders. As a best practice, the Australian Department for Foreign Affairs and Trade (DFAT) put out a public call to inform Australia’s engagement at both the UN GEE and OEWG and has regularly made public its positions on the cyber norms debates, circulating these interventions both on official websites and social media handles. DFAT is able to engage in this manner and consequently substantively engage with ongoing negotiations because of both expertise and empowerment. There is a need to empower an individual or a body within the government to front public engagement on cybersecurity regimes and coordinate multistakeholder efforts. The portfolio of the present National Cybersecurity Coordinator extends to all cybersecurity efforts – both domestic cyber resilience and cyber hygiene maintenance, and cooperation with the MEA on global governance issues. The newly established New and Emerging

69 Conversations with Arun Sukumar, Trisha Ray, Udbhav Tiwari, Akriti Bopanna and Raman Chima were useful in shaping this section.
Strategic Technology Division in the MEA is well primed to play this role and can “can help aid India’s presence at multilateral and multistakeholder forums by continuing dialogue even while these forums are not in session.”

Greater engagement with a range of experts tracking the debate, including those critical of traditional government stances on technology issues, is also vital to enable India to formulate a nuanced and robust negotiation strategy that fairly represents all national stakes globally. As I detailed in this chapter, several experts have contributed in their individual or institutional capacity to global norms formulation processes already, and this experience should be tapped into to bridge information asymmetries. Greater demand for expertise would also attract more funders in the space as they would be able to assess the “impact” of their funding on policy-making.

Second, as with any global governance regime, the media plays a vital role. As detailed above, these processes have received negligible coverage from both print and media houses, compared with the more extensive coverage that they have received in leading US newspapers such as The Washington Post.

While the progress of these negotiations might not attract public attention, underscoring their significance by meshing them with coverage of key cyber or diplomatic events might boost public interest both in the overall state of play and India’s engagement with these processes. This would also attract greater interest from funders and push the government towards greater transparency and accountability in their stances.

Third, civil society actors should continue to engage with counterparts abroad through multistakeholder fora like the GCSC or through networks revolving around multilateral processes such as the OEWG. Transnational advocacy networks can help crystallise norms across jurisdictions by exchanging ideas and experiences, coordinating activities, and making joint proposals. Government representatives often engage directly with stakeholders through global forums, which serves as an additional avenue through which Indian stakeholders can engage, and introduce their ideas into the workings of global processes.

To exercise diplomatic clout commensurate with its demographic and economic heft, India should abandon the hitherto non-committal approach to cyber norms negotiations, and ferment a coherent negotiation strategy. Robust
engagement backed by a vibrant multistakeholder ecosystem will enable the crafting of a global cybersecurity regime rooted in India’s strategic and diplomatic needs.
INTRODUCTION

The role of governments and other actors (technical community, academia, private sector, and civil society) in Internet governance has long been a central point of contention. There were those that proclaimed that governments have no place in cyberspace, of which the most famous screed was the 1996 “A Declaration of the Independence of Cyberspace” by John Perry Barlow, which urged States not to interfere in Internet governance and allow an open and free development of the network. “Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours,” declared Barlow.

This view, however, faced significant challenges stemming from pressing issues such as cybercrime, national security, cybersecurity, privacy (and surveillance), intellectual property, and taxation of e-commerce activities. The Internet has quickly turned into an essential part of how people worldwide communicate and access knowledge and entertainment. At the same time, companies transformed the Internet into a new global marketplace as governments began to render public services online. A demand for a more formal governance mechanism for the Internet emerged.

National and international initiatives have dwelt on how to institutionalize Internet governance both domestically and internationally. Whether governments should have a central role (top-down) and the extent to which

other actors should partake (more bottom-up) became crucial questions. On several occasions in the last 30 years, multistakeholder approaches – where different actors including the technical community, academia, civil society, and the private sector participate alongside governments – were proposed and gained some success: from the development of the Internet Corporation for Assigned Names and Numbers (ICANN) to the institutionalization of the United Nations’ Internet governance Forum (IGF). Yet, on the global level, the governance ecosystem remains fragmented, and in need of an effective cooperation and coordination mechanism, particularly for cybersecurity and for developing norms to deter or protect against cyber attacks. Although debates on multistakeholder Internet governance have a long history and those on cybersecurity are relatively new, they are related.

The multistakeholder approach towards Internet governance taken by Brazil highlights its opportunities and pitfalls in the field of cybersecurity as well. Domestically, Brazil has championed multistakeholderism from the outset, establishing an inclusive organization to advance Internet policy. The “Snowden Revelations” prompted Brazil’s defense of a similar approach internationally, culminating in the coordination and statement at the NETmundial Conference in 2014.

The Brazilian experience illustrates the challenges facing multistakeholder Internet governance and cybersecurity diplomacy in terms of maintaining a delicate balance among the participating stakeholders. Domestic and international shifts in power, combined with swings in the perception of how the Internet – particularly large technology companies – impacts the information ecosystem (affecting not only national democratic processes but also citizens’ sense of community) have led to a changed scenario for Internet governance compared to what it was in 2014. The country showcases as well how a multistakeholder regime for Internet governance may translate into both an opportunity and a challenge for international cybersecurity.

This chapter is divided into three main parts. The first aims to describe the Brazilian domestic and international approaches to Internet governance...
Building an international cybersecurity regime

with particular attention to the formation of the Brazilian Steering Committee (“CGI.br,” “Comitê Gestor da Internet”); the development and implementation of the Port 25/TCP management (anti-spam policy); the drafting of the “Brazilian Internet Bill of Rights” (“MCI,” “Marco Civil da Internet”); and the organization of the NETmundial Conference and its multistakeholder proposal. The second focuses on developments since 2015 and the consequences of the fragmented cooperation and coordination of the international ecosystem for Internet governance. Special attention is paid to the cybersecurity regime in the National E-cyber Strategy and how multistakeholder aspects appear indirectly as a “support regime” within the strategy. Additionally, this chapter considers the rise of unilateral governmental actions towards governing cyberspace and how they negatively impact the cooperation regimes necessary to implement coordination against cyber threats. Finally, based on lessons learned from the past few years, the third part suggests a starting point for a path forward.

MULTISTAKEHOLDER GOVERNANCE AND BRAZIL: THE FORMATION OF A SYSTEM

For over twenty-five years, Brazil has developed a unique model of multi-stakeholder Internet governance. It is based on two supporting pillars: the CGI.br and the MCI. Together, they structure an open participatory process, based on consensus building and common implementation of Internet standards and policies.

On the international level, the Brazilian traditional defense of multilateral diplomacy guided its foreign affairs. In 2013, Brazil was caught in the revelations made by Edward Snowden, concerning the global espionage program, as the Brazilian President Dilma Rousseff’s phone was reported to have been tapped. As such, at that time, the government needed to be seen as providing a strong response to the revelations. The government not only took national actions but proposed a bolder approach to global Internet governance. The

---


6 Brazil started a project to diminish the reliance on the connection to the Internet through the North-American infrastructure; an encrypted email service and even proposed data localization obligations. The last one was later dismissed.
proposed model was based on its own multistakeholder experience and resulted in a multistakeholder statement with wide support at the international conference NETmundial, held in Sao Paulo in April 2014.\(^7\)

This section will examine domestic multistakeholder practices on cybersecurity and Internet governance in Brazil, as well as its participation in international fora, particularly in the UN General Assembly and at the NETmundial conference of 2014.

The Domestic Scenario

The development of the Internet in Brazil was a collective effort from the technical community, civil society, the private sector, and the government. On the one hand, the connection of the country to the global Internet was the result of a domestic process led by universities towards the creation of an information network.\(^8\) A permanent fixed line between the Brazilian network and the US Internet backbone was established in 1991 through the influence of academics and members of the technical body that persuaded the public telecom company to install the cable connection.

On the other hand, the fact that the government did not define Internet access as a telecommunications service, but as a value-added service,\(^9\) provided Brazil with the opportunity to set a different governance regime not subject to the agencies and regulations of the telecom sector. The CGI.br, formed with an advisory function for Internet-related matters, fostered the basis for the domestic multistakeholder governance regime.

CGI.br – the Brazilian Internet Steering Committee

The CGI.br was created in 1995 by the Ministry of Science and Technology and the Ministry of Communications.\(^10\) The body was designed to be open and inclusive with the participation of different sectors, and several of the Brazilian Internet’s pioneers (from the technical community and civil society)

---


\(^9\) One should note that the development of the Internet in Brazil coincided with the democratization of the country and its process of opening up its internal market for foreign products and capital. Thus, there was concern both of state surveillance and state monopoly, which are embedded in the choice of arrangements.

even served as part of its staff. In 2003, a Decree reformed the Committee,\textsuperscript{11} increasing the participation of different sectors, and thus strengthening its multistakeholder cachet. CGI.br’s composition was raised to include 21 representatives, including from the Federal Government, state-level governments, the private sector, representatives of civil society (nonprofits and non-commercial entities), representatives of technical and academic communities, and one renowned expert.

It should be noted that besides the government representatives, all other members are chosen through open elections, in which members of the sector-group that they represent can participate.\textsuperscript{12} This is a departure from the North American model of multistakeholder governance as it is structured in such a way that the different sectors are guaranteed to have representation as part of the sector tracks they represent.\textsuperscript{13}

Two other aspects have proven relevant for the success of CGI.br’s multistakeholder model. It is a consensus-driven forum focused on the expertise and particular role of the actors it represents. The Committee itself serves both to set the agenda and to funnel the different views towards a solution considered acceptable by all the stakeholders. It is not dependent on funds from the government nor of any particular company, as it collects fees from the administration of the Brazilian ccTLD (.br), making it less susceptible to capture by a specific stakeholder, which reinforces its autonomy.\textsuperscript{14}

Thus, the achievements of the CGI.br multistakeholder model are a result of the legitimacy generated by its institutional arrangement.

**Port 25/TCP management: anti-spam**

The adoption of Port 25/TCP management of the Brazilian Internet provides a complex and in-depth illustration – pertinent to domestic and international cybersecurity – of CGI.br’s multistakeholder decision-making process in practice.

Spam was a major issue in Brazil, with the National Computer Emergency Response Team (CERT.br, a part of the CGI.br) indicating in its first reports

\textsuperscript{11} Presidential Decree no. 4,829/2003. Available at: http://cgi.br/pagina/decretos/108.
\textsuperscript{12} For the composition, see CGI.br website: http://cgi.br/membros/. For elections see: https://www.cgi.br/processo-eleitoral/.
\textsuperscript{13} An interesting comparison can be found in a report from the Brookings Institutions: Trinkunas, H. and Wallace, I. “Converging on the Future of Global Internet governance: The United States and Brazil.” Foreign Policy, Brookings Institutions, July 2015, 20.
\textsuperscript{14} It has to be mentioned that its legal standing, based on a Presidential Decree and not in a piece of legislation, remains a source of potential instability.
that 80% of spam was due in high probability to “botnets.” The reports noted an abuse of the Brazilian infrastructure as international spammers used the network against victims in the country but mostly overseas. This created the need to find both a technical and a normative solution to the problem.

Hence, in 2005, CGI.br, through its Anti-Spam Working Commission (CT-Spam), began addressing the issue of spam in Brazil. Initial efforts focused on the technical aspects of limiting spam, such as regulating Port 25/TCP, the port used by the Simple Mail Transfer Protocol to send and receive e-mail. This technical effort had limited effect, as it was not being adequately implemented by all players. A shift in tactics, however, yielded more results. Instead of treating spam as a purely technical Internet infrastructure problem, CGI.br addressed it as a regulatory issue that concerned consumer rights, freedom of speech regulation, and commercial competition. This approach led to the 2013 implementation, by Telecommunications Operators (Telcos) and Internet Service Providers (ISPs), of the technical recommendation developed.

Implementing the TCP port management required collaboration between three categories of players: telecommunication companies (who mostly control the Internet’s infrastructure), broadband providers and ISPs (who provide connectivity and IP addresses, authenticate users, and provide services such as e-mail and web browsing), and Internet users. Thus, the challenge was for key domestic stakeholders to participate in the multistakeholder process. A solely technical approach was not enough. Only a few ISPs had voluntarily regulated Port 25/TCP, while major players were mostly reluctant to accept the change. Telecom companies, for example, insisted that ANATEL – their regulatory agency – should support the initiative. Only after the Committee Board officially requested its support, did Telcos begin to change their position. Telcos and ISPs also requested support from the Ministry of Justice, including its consumer rights group, and the judiciary.

These requirements pushed the blocking of the Port 25/TCP project to gradually become more and more multistakeholder. In 2010, for example, CGI.br and ANATEL signed a cooperation agreement, which resulted in a formal commitment by the telecom companies to support CT-Spam’s recommenda-


16 More at “Comissões de Trabalho – Antispam.” Available at: http://www.cgi.br/acoes/antispam.htm#a4.

tions.\textsuperscript{18} In 2011, the Department of Defense and Protection of Consumers of the Ministry of Justice issued a technical note to inform judicial institutions about the block of Port 25/TCP, freeing telecom companies and ISPs of major consumer rights responsibilities (and at the same time assuring that, when necessary, users could request their Port 25 be opened).\textsuperscript{19}

Whereas there was reluctance previously, all players voluntarily implemented the solution that had been arrived at through multistakeholder dialogue. The outcome was not only that Brazil was dropped from the top of the list of spammers, improving the security of its network, but also and even more important, participants were more willing to support additional future initiatives. It created an added layer of legitimacy both to the process and the initiative itself.

**MCI – “the Brazilian Internet Bill of Rights”**

Highlighting Brazil’s regulatory process that culminated in the MCI helps explain both the success of the domestic multistakeholder model and its current challenges vis-à-vis Internet governance and cybersecurity.

Participatory governance – where different stakeholders (particularly citizens, civil society organizations, and private sector) take part in shaping policy and regulation – is not new in Brazil, nor is it restricted to Internet policy. In fact, the country has a tradition of solving regulatory conflicts through negotiation. In terms of regulations specifically, government-run consultations have been institutionalized since at least the early 2000s (D4176/2002).\textsuperscript{20} Public agencies and organs – besides CGI.br – provide opportunities for stakeholder participation in setting up the regulatory agenda and influencing and advising on regulatory proposals, and in some cases, even to partake in the supervisory processes.

The drafting process of the MCI draws from this practice, yet it has unique features. In contrast to other draft bills intended to regulate Brazil’s Internet, it was drafted neither through a purely top-down nor through a bottom-up process. Instead, the Marco Civil was drafted through a collaborative effort that involved civil society, government (executive and legislative branches), academics, the technical community, and the private sector. As such, it was the

\textsuperscript{18} Ofício no 195/2010-PR-ANATEL.

\textsuperscript{19} Nota Técnica – NT no. 65 CGSC/DPDC/SDE. Available at: http://www.antispam.br/porta25/brasil/notatecnica65.pdf.

\textsuperscript{20} Later, the decree was revoked by decree no. 9.191/2017. In both cases, there is a procedure that allows for online public consultations prior to the proposal of a new piece of regulation. The new decree is available at: http://www.planalto.gov.br/CCIVIL_03/_Atos/2015-2018/2017/Decreto/D9191.htm#art59.
product of an open and collaborative effort that used the Internet itself as a tool for drafting the legislation.

The process started with two rounds of structured consultation, supported by the Ministry of Justice, in partnership with academic institutions, back in 2009.\(^{21}\) The first round of the debate tested a set of normative standards, predefined by those sponsoring the initiative, that was considered important to include in future legislation. In contrast, the second round focused on receiving feedback on the draft legislation itself.

The project made use of several “web 2.0 tools” (mainly the WordPress platform, Twitter, RSS feeds, and blogs), which lowered the barriers of entry, allowed for more inclusiveness, and ultimately increased the number of opinions. They also provided for broad transparency and channels for dialogue, which in turn helped to reduce information asymmetry and facilitate negotiations.\(^ {22}\)

Examples of compromises achieved include the Ministry of Justice’s change of position on log records; ISPs and telecommunications companies agreeing to disagree on net neutrality; and civil society coping with copyright being exempted from the generic intermediaries’ liability immunity clause. This suggests that no stakeholder achieved its desired result on every issue – and there was no policy issue where there was a clear alignment among all stakeholders – yet the multistakeholder approach created an opportunity for stakeholders to collaborate and achieve a text that all could accept. Additionally, the community forged by the process provided an instance of support for the legislation long after it was enacted.\(^ {23}\)

**The International Scene**

Brazil has been an active participant in the international debate on Internet governance. The country was engaged in the foundation of the ICANN and took part in early international discussions at the International Telecommunication Union (ITU) and The World Summit on Information Society. Brazil raised

\(^{21}\) The contributions were received through the website: http://culturadigital.br/marcocivil.


\(^{23}\) One should mention that after the MCI, other bills were proposed through a process of consultation. Examples of that were proposals to reform the Copyright Law, the Age Rating System, the Civil Procedures’ Code, and a Data Protection Bill.
a series of concerns in terms of the role played by governments at ICANN. The country was also one of the first to propose a coordination forum, modelled on its own Internet steering committee (CGI.br). This proposal is at the genesis of what today is the IGF (Internet governance Forum). This critical position of Brazil rendered it possible to work with a wider group of countries in order to examine different avenues for Internet governance.

In 2013, the revelations of mass surveillance brought forth by Edward Snowden prompted, beyond a domestic response, international calls to review global Internet governance. Brazil convened, in partnership with other organizations, the Global Multistakeholder Meeting on the Future of Internet governance, known as NETmundial, which followed an alignment of goals present at the speech of President Rousseff at the 68th session of the UN General Assembly and the release of the Montevideo Statement on the Future of Internet Cooperation. Both positions called for a reorganization of the structures of the Internet governance ecosystem.

**Brazil at NETmundial**

Brazil’s position at the conference was very clear from the start. The definition of the actors and the agenda showcased its open and participatory approach – considering stakeholders from different areas. Even the committees running the event reflected the execution of a multistakeholder concept. There were four of them, all composed of representatives from relevant stakeholders chosen from within their respective stakeholder groups.

---


27 In order to showcase the commitment to multistakeholderism, even in terms of participation of the audience in the event, there were four mics, one for each stakeholder: (1) civil society; (2) private sector; (3) academia (and technical community); and (4) public sector (government and international organizations).

28 Varon, J. *Combate ao spam na Internet no Brasil: histórico de reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da*
Importantly, the experiences from the Brazilian Internet Steering Committee and the Internet Bill of Rights proved significant starting points and models both for the convention itself and for the proposal to reshape the international Internet governance ecosystem. Four matters were highlighted in the opening speech of President Rousseff: (i) human rights, including privacy and freedom of speech, should be an intrinsic part of Internet governance; (ii) equality among states was a guiding principle;\(^{29}\) (iii) in order to achieve an equal footing among states, developing nations should be included in the discussion; and (iv) different sectors perform different roles, have different responsibilities, and should participate in the governance process.

As for outcomes, the process of the conference itself is noteworthy.\(^{30}\) It was in several ways a testament to the possibility of an open and inclusive structure with stakeholders being able to participate in an orderly manner. The final statement (“NETmundial Multistakeholder Statement”)\(^{31}\) showcased, among others, the following commitments: (i) promotion and protection of human rights; (ii) proper balance between duties and rights of intermediaries; (iii) multistakeholderism as a basis for Internet governance; and (iv) the need to strengthen the IGF in order to be more outcome-oriented and to foster discussions and deliberations in a plural environment.

The document was seen as a symbol of the potential of the multistakeholder approach to bringing different viewpoints together and articulating a common position, a “roadmap” for the future of Internet governance.\(^ {32}\)

---

\(^{29}\) It is important to note that the traditional position of the country was present as well. Arrangements that exclude sectors or that in turn are subject to oversight by one or a small group of states are not only not democratic but should not be accepted.

\(^{30}\) This was highlighted at the 2015 IGF in João Pessoa, Brazil. See final report: http://www.intgovforum.org/multilingual/filedepot_download/3367/208.


\(^{32}\) The statement of the United States a few days before the conference to review the structure of ICANN so that the IANA system would be more open and less in control of the Department of Commerce yielded a sense of accomplishment. It resonated with the open and inclusive spirit of the NETmundial. NTIA Announces Intent to Transition Key Internet Domain Name Functions, National Telecommunications and Information
THE AFTERMATH OF THE NETMUNDIAL AND THE CURRENT STATE OF THE INTERNET GOVERNANCE ECOSYSTEM

The success of a large multistakeholder conference such as NETmundial, where it was possible to structure a basic common understanding in terms of both a set of principles and a basic structure for the Internet governance ecosystem, generated a sense of optimism. The following years, however, made it apparent that the success of NETmundial alone was not sufficient. The spirit of cooperation and coordination that characterized NETmundial did not materialize in the development of a new multistakeholder Internet governance mechanism. The ecosystem remains fragmented and lacking in sufficient coordination.\textsuperscript{33}

A series of national and international events exposed even further the fragile institutional arrangement of the global ecosystem. The increased levels of misinformation and disinformation online, the Cambridge Analytica scandal, and even incidents of violence amplified by the Internet, such as the Christchurch shooting and US Capitol attack, have had an impact on the perception of the Internet that compelled a reaction.\textsuperscript{34} These incidents have spurred calls for more government action, stronger regulation, and greater responsibility for Internet intermediaries.\textsuperscript{35}

The pendulum that, during NETmundial, had moved in the direction of more actors, openness, and inclusion, swung to a more top-down approach, with governments having a central role.\textsuperscript{36} In fairness, the private sector and civil society have promoted several initiatives as well.\textsuperscript{37} The reality however is that,

\textsuperscript{33} Under more recent governments, Internet governance as a part of foreign policy went from appearing front and centre to less so. One short and slightly dated analysis of that “lost centrality in the agenda” is available here: Canabarro, D. “Onde Foi Parar a Internet nos Discursos do Brasil na Assembleia Geral da ONU em 2015 e 2016?” Revista Conjuntura Austral, 8, no. 42 (2017): 4–11.

\textsuperscript{34} They have had an impact even on the perception of the functioning of democratic institutions. For that, see: Anne Applebaum and Peter Pomerantsiev, “How to Put Out Democracy’s Dumpster Fire,” The Atlantic (2021). Available at: https://bit.ly/31bvNEi.

\textsuperscript{35} Internet intermediaries are understood here \textit{lato sensu}, meaning particularly platforms, but not restricted to them.


\textsuperscript{37} See, for instance: Manila Principles; Santa Clara Principles; Christchurch Call; Charter of Human Rights and Principles for the Internet; African Declaration on Internet Rights and Freedoms; Change the Terms; Paris Call; Facebook’s Charting
aside from certain actions by the European Union, even multilateral efforts failed to achieve a sufficient level of coordination, cooperation, and cohesion.\textsuperscript{38} The consequence has been the rise of unilateral governmental actions putting in check the multistakeholder edifice of Internet governance.\textsuperscript{39} Those trends have serious implications for international cybersecurity as well.

From the standpoint of Brazil, certain international trends had roots in the domestic Internet governance regime with consequences for cybersecurity arrangements. First, the extraterritorial reach of both regulation and judicial orders became more common. Second, the initiatives to govern the Internet have moved from consensus-based standardization to more direct government regulation (and in terms of security, also militarization), which weakens the multistakeholder consultation approach.

**Unilateral Action**

**Increasing the geographical reach of national laws**

Questions pertaining to states’ jurisdiction over people, activities, and infrastructure on the Internet are as old as the Internet itself. In recent years, governments have had a greater appetite to claim wider jurisdiction over cyberspace, either through regulation or judicial decisions. This trend is notable in areas of data protection, content moderation, and law enforcement requests for access to data stored overseas.\textsuperscript{40}

In Brazil, too, this trend is apparent despite the legacy of its multistakeholder Internet governance regime. The consequence is an erosion of confidence in the multistakeholder approach and disarticulation of Internet policy in Brazil which impacts foreign policy as well\textsuperscript{41} as its cybersecurity diplomacy. A closer look sheds light on the matter.
Several countries have claimed an extraterritorial extension of their jurisdiction, despite the unlikely prospect of enforcement.\textsuperscript{42} It seems as if these countries intend to unilaterally close the lacunae in international Internet governance. Their purpose seems to be to apply their national rules (privacy rules, usually) to foreign entities providing services to their citizens. This is clearly a strategy of relative success, as not all countries are capable of imposing their rules beyond their territory.

Not only Brazil but Colombia,\textsuperscript{43} Mexico\textsuperscript{44} and Peru,\textsuperscript{45} to name a few from the region, following the European example, have added an extraterritorial dimension to their data protection regulation. In the case of Brazil, the General Data Protection Legislation (“LGPD,” “Lei Geral de Proteção de Dados Pessoais”) borrows substantially from the European GDPR in art. 3.\textsuperscript{46}

The trend does not end with data protection. A bill aimed at regulating disinformation (called the “Fake News Bill,” PL 2630/2020) proposed to regulate tech companies even if they are overseas when they offer services to a Brazilian audience, or at least one company in the economic group is established in the country.\textsuperscript{47}

This approach to increase the reach of legislations can be criticized for (i) potentially leading to arbitrary enforcement (not necessarily enough resources to pursue all actors); (ii) impairing legal certainty; and what is more important, (iii) potentially leading to transboundary conflicts, both in terms of compliance (companies may be required to comply with overlapping legal obligations) and between countries (causing a potential legal arms race\textsuperscript{48}).

the UNGA is also an indication of this phenomenon. (See, for instance: Canabarro, D. “Onde Foi Parar a Internet nos Discursos do Brasil na Assembleia Geral da ONU em 2015 e 2016?” Revista Conjuntura Austral, 8, no. 42 (2017): 4–11.)

\textsuperscript{42} For a global overview of such claims, see for instance Internet & Jurisdiction Global Status Report 2019, 49 ff. Available at: https://www.internetjurisdiction.net/news/release-of-worlds-first-Internet-jurisdiction-global-status-report


\textsuperscript{44} See National Institute for Social Development, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Mexico City, 2010; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Mexico City, 2011; Secretariat of Economy, “Lineamientos del aviso de privacidad,” Diario Oficial de la Federación, Mexico City, 17 January 2013.

\textsuperscript{45} Peru, Law No. 29.733 of 2011, Personal Data Protection Act.

\textsuperscript{46} See: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

\textsuperscript{47} See: https://legis.senado.leg.br/sdleg-getter/documento?dm=8128670&ts=1612 303015028&disposition=inline.

The extraterritorial reach of states does not necessarily impact their domestic governance regime *per se*. The process of formulating new pieces of legislation, however, is affected. Bills impacting the Internet, which had previously been drafted through open and consultative processes with the participation of the CGI.br and contributions of different stakeholders, have been proposed and discussed with little or no multistakeholder presence. The community formed through the guidance of the CGI.br and following the MCI crowdsourcing process lost some of its political clout, illustrating the delicate political balance necessary for multistakeholder approaches to succeed. This trend has spilled over into cybersecurity policymaking. Brazil’s legal-institutional cybersecurity structure suffers as new proposals arise reflecting a more centralized arrangement, with bodies such as the Institutional Security Office (GSI) gaining more relevance.49

Finally, it is worth noting that such unilateral movements tend to hinder the necessary solutions that depend on global governance frameworks to provide a space for dialog, regulatory and standard convergence and dispute resolution.

**Global content/account removal orders**

Another trend that imposes even more barriers to an international, cooperative ecosystem for Internet governance and cybersecurity is the scaling of global content or account removal orders. Judicial – and in some cases even administrative – decisions aim at imposing obligations that are beyond their borders.

In terms of content moderation in different contexts, orders have been issued to take down or maintain certain content 50 worldwide. A similar situation happens with suspensions of accounts on platforms – particularly social networks.

A recent case from the Brazilian Supreme Court (“STF,” “Supremo Tribunal Federal”) illustrates these dynamics. During a criminal investigation concerning the distribution of alleged “fake news,” Justice Alexandre de Moraes ordered Facebook and Twitter to block access to 16 accounts of individuals accused of spreading disinformation and hate speech. It was reported that the magistrate requested to block all global access to their accounts. When platforms noted the wide scope of the decision and mentioned they would comply only within the country’s territory, the judge imposed hefty fines

---


and issued veiled threats to impose criminal charges against the company’s executives (for non-compliance with the judicial order).\textsuperscript{51} Recently, when Brazilian judges decided to suspend WhatsApp in the country (as a sanction for non-compliance with their law enforcement’s request for data), it impacted the messaging service in Argentina and Chile as well.\textsuperscript{52}

Most of the situations that have impacted international cooperation concern data stored overseas. In several cases, magistrates glossed over the place of storage and demanded access to data regardless. Notably, reference was made to Article 11 MCI, which is the Brazilian law applicable to data collected locally.\textsuperscript{53} It does not establish the reach of the applicable instrument (“warrant”) to request data. There is no specific law that empowers law enforcement agencies to demand data beyond the territory of Brazil. There are several MLATs, which set judicial cooperation mechanisms, however. As a consequence, the Supreme Court was called upon to adjudicate the constitutional status of the cooperation agreement between the US and Brazil in terms of criminal matters (the MLAT), a decision still pending.\textsuperscript{54}

Unilateral actions of the sort highlighted above not only undermine existing mechanisms of cooperation between states but also domestic multistakeholder governance. Internet platforms and access providers are increasingly being demanded by states to take action with regional or global consequences without consideration of other countries’ institutions, regulations, and the rights of their citizens. Such unilateral actions seldom have domestic multi


\textsuperscript{53} \textit{Verbatim}: “Article 11 All operations involving the collection, storage, retention, or processing of records, personal data, or communications by Internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records if any of those acts occur in Brazilian territory.

§1. The provisions of this article apply to all data collected in Brazilian territory and to the content of communications if at least one of the terminals is located in Brazil.

§2. The provisions of this article apply to activities conducted by foreign-based legal entities if they offer services to the Brazilian public or at least one of the members of the legal entities’ economic group has an establishment in Brazil.” (Translation available at: https://itsrio.org/wp-content/uploads/2018/02/v5_com-capacpages_miolo_Brazil -Internet-Bill-of-Rights-A-closer-Look.pdf)

\textsuperscript{54} Brazil, Supreme Court (STF), “\textit{Ação direta de constitucionalidade},” No. 51. See http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.
stakeholder processes backing their legitimacy or validity. Viewed from the lens of cybersecurity, attempts by states to reach extraterritorially will not only have significant consequences for the integrity of digital networks and infrastructure globally, but also limit the utility of non-governmental actors participating in the creation and implementation of domestic and international cybersecurity norms.

From Consensus-based Standardization to Direct Government Regulation

The unilateral nature of aforementioned state actions tends to undermine consensus-based dynamics developed under multistakeholder regimes for Internet governance, with implications for cybersecurity as well.

The Brazilian case illustrates this challenge. The Brazilian Senate’s approval of the “Fake News Bill” without an open and inclusive consultative method highlights a new and different dynamic from previous years, especially in contrast to its debate and final approval of the MCI. Notably, Article 32 of the bill also institutionalized the possibility of unilateral extraterritorial actions.56

This trend is reflected as well in the Brazilian e-Cyber Strategy, which, despite having been opened for consultation with different sectors, continues to base the national cybersecurity architecture on centralized arrangements – particularly under military control. Recent bills, announced by the government, seem to follow a similar path, concentrating the arrangement within bodies with little or no multistakeholder participation.57

55 Article 32, as it was approved, would create at least two obligations: companies should either have a physical presence in the country or appoint a representative and an obligation to provide remote access to data independently of where it is stored or the legal requirements it may entail. For the original text of the bill (in Portuguese) and discussion of it, see: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. For a discussion on the impact of art. 32, see Souza, C. A. and Perrone, C. “Fakenews’ e acesso a dados armazenados no exterior,” JOTA, 2020. See: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020.

56 A portion of the domestic community was able to move the rapporteur of the House of Representatives to propose to adjust the text to diminish the potential impact on Brazil’s international cooperation. See the text proposed by the rapporteur after consulting with civil society organizations: https://www.poder360.com.br/midia/pl-das-fake-news-propoe-ate-5-anos-de-prisao-a-quem-integrar-milicia-digital/.

All this showcases the swinging of the cybersecurity and Internet governance pendulum much closer to a top-down, government-centric approach, denying not only avenues for domestic input through multistakeholder participation but also limiting Brazil’s multistakeholder cyber diplomacy abroad.

MULTISTAKEHOLDER DIPLOMACY: ELEMENTS FOR A PATH FORWARD

The challenges for multistakeholder Internet governance regimes highlighted in preceding sections are also relevant for the creation and implementation of cybersecurity arrangements, both globally and domestically. Trust and political will have eroded as governments pursue unilateral action without cooperative mechanisms, either with state or non-state actors. Pushing for laws with extra-territorial reach and concentrating on more “public sector centred” architectures does not solve, in the long run, the necessities of a secure network. There is, however, some light on the horizon. Quite paradoxically, the impact of the pandemic – which has shut many borders – has led to intense developments in the digital sector as millions of people and thousands of businesses were pushed towards using the Internet. The notion of a shared “commons” where both the bonus and the onus are divided among nations has gained traction.

Coupled with that, the renewed pressure towards Internet intermediaries playing a more significant role in regulating behavior online and more intense scrutiny around “Big Tech” furthers the cause of building institutions that provide stability for the digital space.

The increase in cyber threats, risk of cyber warfare, and weaponization of cyberspace that led to several intergovernmental and multistakeholder norms initiatives in the field of cybersecurity and cybercrime before the pandemic, have also reinforced the need for effective cooperation. Such alignment of interests among actors provides an opportunity for renewed multistakeholder engagement in cybersecurity and Internet governance. The questions now are whether this spirit can be maintained and what lessons have been learned.

If developments in Brazil are any indication, multistakeholder initiatives depend on a delicate balance between participation, perceptions of independence of the institutions (i.e. not captured by one group or sector), and effectiveness in terms of the capacity to act in a timely manner when necessary. All that should go together with a baseline of shared principles.

The complexity of questions has only increased after the forced digitalization of individuals, companies, and governments during the Covid-19 pandemics. The sense of urgency for more coordination on how to handle the different aspects of Internet governance must not hinder the demand for multistakeholder input and decision-making. What this chapter has sought to do is firstly, to emphasize how foreign policy considerations can affect domestic
multistakeholder governance, and *secondly*, highlight how trends in cybersecurity and Internet governance towards greater centralization and unilateral government action can impede multistakeholder processes, even if they have been long entrenched in the policymaking process, as is the case with Brazil.

The Internet is not fully independent from governmental regulation, as envisioned in the 1990s, but reliance on different perspectives and types of expertise brought to the table by different actors is a key component to ensure that the fate of the global network of networks will not depend on the decisions of one government or large corporation. This reality is as true for cybersecurity as it is for Internet governance. As the Internet is ultimately a network of networks, the design of its governance should also be the product of the different contributions that different stakeholders can provide. Cybersecurity depends on the many links in the “network.”
11. Taking stock of Estonia’s multistakeholder cyber diplomacy

Marina Kaljurand

INTRODUCTION

Estonians are proud to have one of the world’s most “digitalized” governments and of their digital way of life – and rightly so. Estonia has been the first and, in some cases, the only country to introduce Internet voting, digital signatures, X-Road, e-taxation, e-Health, and thousands of other online services.\(^1\)

This digitalization, dubbed “E-Estonia,” is among the most ambitious projects in technological statecraft, and its success has been recognized internationally. The country has even been described as the “ultimate digital democracy.”\(^2\) Referring to the Obama administration’s struggles to set up its “Healthcare.gov” website for digitalized health services, President Obama once jokingly noted that he should have “called the Estonians when we were setting up our health care website.”\(^3\)

It is not technology that makes Estonia stand out, but the high percentage of people using the country’s public and private digital infrastructure. The number of online services exceeds 5,000, and the country has even granted some of the online services to non-residents. Estonia is the first country to offer non-residents “e-Residency,” “a government-issued digital identity and status” that enables access to “Estonia’s transparent digital business environment.”\(^4\)

---

E-Residency allows digital entrepreneurs to manage business from anywhere, entirely online. According to official estimates, more than 100,000 people from over 170 countries have reportedly sought e-Residency, establishing approximately 25,000 Estonian companies.

Estonia has been named “the most advanced digital society in the world” as a result of its long-term whole-of-society (e-Estonia) policy. The initiative grew out of the partnership between a forward-thinking government, a proactive ICT sector, and a switched-on, tech-savvy population. It has developed into an efficient, secure and transparent ecosystem that saves time and money. Estonia has built its digital society and national cyber resilience system through various public–private partnerships (PPPs), with the private sector, IT community, civil society and academia actively involved each step of the way. Collaboration between the private and public sectors has always been at the center of Estonian innovation. In the 1990s, the government started several IT programs to catalyze the vision for a digital society, but only in a few cases was it the main sponsor.

For example, the government-funded Tiger Leap Program was launched in 1997 in order to provide Estonian schools with information and communication technology (ICT) infrastructure. Nearly 4,000 teachers participated in a 40-hour computer basic training course as part of this program, with thousands more trained in the following years.

Since the early nineties, the government’s philosophy has not been to hire programmers, but to use the services of private companies, which have in turn increased the competitiveness of the Estonian IT sector. It was called an “all-nation” approach. Today, many terms are used to describe the approach: PPPs, inclusiveness, multistakeholderism, and the multistakeholder model.

This paper traces Estonia’s experience and success in applying the multistakeholder model of digital and cybersecurity governance – starting with Estonia’s road to e-Estonia, the evolution of PPP, and lessons learned from

---

9 In the context of this chapter, the terms PPP, multistakeholder model and multistakeholderism are regarded as synonyms.
2007, when Estonia became the first nation in the world to be subject to politically motivated cyber-attacks by another nation. The paper also analyzes legal and organizational national frameworks that have supported multistakeholderism. It highlights the Cyber Defence Unit as a unique example of a PPP. Finally, the paper addresses the importance of global and regional multistakeholder cooperation from an Estonian perspective, and the need to promote and raise awareness about PPP globally.

ESTONIA’S PATH TO E-ESTONIA

After regaining independence from the Soviet Union in 1991, there was a desire in Estonia (as well as an urgent need) for a new method of government. It was the public and private sectors together that decided to transform Estonia into a nation based on digital solutions and e-services.

Cooperation between the public and private sectors intensified at the turn of the century when, in 2002, the country’s first digital ID card was issued. Each Estonian ID card has a digital supplement called the Digital-ID, which is a state-issued digital document for electronic identification and the use of digital signatures. Digital ID cards are issued to all Estonian residents and can be issued to non-residents.

The electronic identity system is the vital cornerstone of Estonians’ e-state. As in the physical world, there are also cases online when public and private service providers need to know who is accessing specific online services, such as voting, taxation, and medical services. At the same time, users need to feel confident that their identity is protected, and online services are safe and secure. Besides being an excellent technical solution, it is a reflection of trust – trust between citizens and state, state and the private sector, consumers and service providers. Estonia’s e-success has arguably been possible owing to the high level of trust of citizens towards their government.\(^\text{10}\) In addition, trust of the private sector and service providers is an important factor.\(^\text{11}\)

A possible security risk in the ID card chips became apparent in 2017 when it was discovered and reported to the Estonian Government by Petr Švenda, a researcher on cryptography and security at Masaryk University in the Czech Republic. This information was made public, and developments were regularly communicated to the public. This incident did not undermine citizens’ trust in the government and online services. On the contrary – 10 million digital


signatures were issued in February 2018, compared with 6 million in the same month the previous year. Moreover, during the security flaw crisis, the i-voting system in Estonia registered a new record: 31.7% of the voters chose their candidate with a click from their laptops.

Digital ID is one of the best examples of PPP, together with X-Road – an interoperable data exchange platform that allows registered databases and information systems to automatically share information without human involvement. The combination of digital ID and X-Road in Estonia has laid the foundation for the first truly digital society. Even if X-Road is a government platform, it has become a ubiquitous network that many major private firms use and thrive upon, either to identify their customers using e-ID-based authentication or to connect to X-Road to offer their services more securely. It has been estimated that X-Road saves over 844 years of working time for Estonia each year.

MULTISTAKEHOLDER CYBERSECURITY GOVERNANCE IN ESTONIA

The focus of e-Estonia has been clear from the beginning – to improve the efficiency and the transparency of the government, to fight corruption, and to make services easily accessible to citizens.

This approach was strongly supported by Estonia’s political leadership, the private sector, and citizens. Even if some e-services were not greeted with much enthusiasm at first (for example, e-school by teachers or e-health by big hospitals), there was wide support for Estonia’s digital society from the public as a whole. This support only increased with time as new online services were introduced and as people became more acquainted with digital transactions. Who wants to stand in long queues for voting, banking, hospital or taxation if these services can be accessed online quickly and safely? For example, filing the annual personal tax return online in Estonia takes only 3–5 minutes.

13 Pihlak, “What we learned from the eID card security risk?”
In 2005, Estonia introduced Internet Voting (i-voting) in national elections. It took a single visit to the national election website – the process involved downloading and installing the voting application, inserting one’s national identity card into one’s computer card reader for authentication, and filling out the digital ballot – to digitally sign and submit the e-ballot.\textsuperscript{18}

While Estonians benefited from digital services, they understood the attendant challenges of digitalization. For example, the i-voting system and similar models have a high probability of becoming attractive targets. As preparations for the 2007 national elections were underway, it became apparent that, sooner or later, a cyber-attack on the system would take place.

In the end, the elections passed smoothly without jeopardizing the online voting system. Indeed, the 2007 elections were regarded as a success story for large-scale online elections. So far there have been no serious incidents since i-voting was introduced in 2005, mainly owing to the high standard of security measures that are used to safeguard the integrity of the system and, most importantly, the security and secrecy of the votes.

In the spirit of transparency and accountability, Estonia has published the source code for i-voting and has invited analyses and critiques of the i-voting system. There have been some politically and financially motivated entities with conflicting interests and values, who are against i-voting for their own reasons but not for technical reasons.

It has to be underlined that no service is 100% secure – neither offline nor online. Risks always exist, starting with the simplest one – human error. However, no one has proved so far that online services are less safe and secure than offline services. At the same time, it has to be recognized that risks exist, that they are different online and offline, and that they have to be taken just as seriously online as offline – assessed, mitigated and minimized, if not completely eliminated.

Preparations for the 2007 elections, including joint cybersecurity exercises, laid the ground for the next level of PPP collaboration. These preparatory exercises raised awareness about cybersecurity, helped to put people at the senior levels of government in the right mindset, and created links with other stakeholders. Digital and cybersecurity topics moved from company basements (where IT experts usually work) to the executive and decision-making floors of government and industry. The high level of private sector and citizen participation in the digital society made them stakeholders, from which engagement in the development of policy – and ultimately cybersecurity diplomacy – followed naturally.

The late Lieutenant General Johannes Kert – former Commander of the Estonian Defence Forces and the brain behind NATO’s early cyber defense initiatives – used to say that “there are no good solutions when you are under cyber-attack, there are only bad and very bad solutions. All you can do is to train, train and then train some more – to train for the known and educate for the unknown.” Some months later his words were tested in practice. The links with the private sector and other stakeholders paid off during the 2007 cyber-attacks.

LESSONS LEARNED FROM THE 2007 CYBER-ATTACKS ON ESTONIA

In April 2007, hacker groups coalesced to launch massive distributed denial of service (DDoS) attacks aimed specifically at Estonia’s government, infrastructure, and media outlets. DDoS attacks are designed to overload and take down servers and websites through repeated and simultaneous requests for information, typically carried out with the use of botnets. The attacks subsided after a few weeks and left no permanent damage, but it ensured Estonia would never underestimate the value of cybersecurity or the danger of failing to protect vital assets.

The attacks prompted state agencies and the private sector to work closely to identify and reduce the nation’s online vulnerabilities – work that had already begun to take shape.

Estonia’s cyber resilience was tested, and valuable lessons were learned from those banner attacks, some of which are outlined below.

• First, the importance of bold political decision-making and prioritizing cybersecurity on the political agenda.
• Second, the importance of having one’s house in order, which entails creating a strong legal framework for cybersecurity, and implementing strategies/action plans with a clear division of responsibilities embedded into the working plans of Ministries/agencies with annual reporting obligations.
• Third, the importance of international cooperation. Cyber-attacks do not respect borders and nor should cybersecurity measures. As such, international cooperation at all levels and in different formats is crucial in order to face and to tackle existing and emerging cybersecurity challenges.

Finally, the importance of an inclusive approach. The attack reinforced the view that governments cannot be effective in the cybersecurity sphere without the support and cooperation of other stakeholders, whether they are industry/private sector, academia, civil society, or the technical community.

It has been argued persuasively that the key factor to have enabled a successful response to the attacks was effective horizontal public-private cooperation.21

ESTONIAN LEGISLATION SUPPORTING MULTISTAKEHOLDER CYBERSECURITY GOVERNANCE

The digital revolution has had an impact on every state and every society. Yet because cyberspace is a relatively new domain of activity and governance, it needs to be addressed properly from a regulatory perspective. The widespread use of ICTs and their attendant security needs implicate the responsibility and accountability of different stakeholders operating in this space. In some cases, the line of responsibility can be ambiguous or overlapping – for example, in Estonia the role of the Ministry of Foreign Affairs and the Ministry of Defence in international cooperation, or the role of the Ministry of Economic Affairs and Communications and the Government Office in coordinating cybersecurity activities. Therefore, it is important to have in place appropriate legislation that regulates the activities, responsibility and accountability of different stakeholders.

National cybersecurity strategies could strongly promote the development of PPP projects across different sectors. Often recognized as horizontal documents, national cybersecurity strategies can play a role in supporting cooperation between government institutions, academia, civil society, and the private sector. Whereas national cybersecurity strategies could promote PPPs by raising awareness of such cooperation, they could also help to set up relevant clusters and cooperation formats within a state.

Estonia has, from the outset, followed the principle of inclusiveness in developing strategy, recognizing the need to engage a wide range of stakeholders in both the strategic planning and implementation phases. This has to do with Estonia’s established approach to public policy and administration, in which those impacted by a policy choice must be given a chance to voice their

views. The approach also recognizes the role of private-sector stakeholders as providers of essential services, and their unique knowledge and expertise. Viewing cybersecurity strategy as a process, rather than simply an outcome document, strengthens connections both between the government agencies involved and with non-government stakeholders that represent an essential pillar of national cybersecurity.

Estonia’s first National Cybersecurity Strategy was adopted in 2008. It was driven by a manifest and well-recognized national need: lessons learned from the large-scale cyber-attacks of 2007. The 2008 cybersecurity strategy was based on a firm recognition that national cybersecurity is a comprehensive task comprising public–private action, various domains, and technical, organizational and legal measures. It clearly defined cybersecurity roles and accountability across the “whole of the system.” Subsequently, PPP became one of the underlying principles of all later cybersecurity strategies: 2014–2017 and 2019–2022.

At the time of writing, Estonia is implementing its third National Cybersecurity Strategy for 2019–2022. It contains a strong element of cooperation with the private sector and academia. The goal is to ensure that the cyber sector workforce required by the state and public sector is developed by training talented youth in formal education and non-scholastic activities as well as cybersecurity specialists for this purpose and according to the demands of the workforce.

---


The strategy also prioritizes the need to cooperate with small and medium-size enterprises, as they comprise the majority of cybersecurity-related companies in Estonia. The goal of the state is to ensure the optimum environment for the inception and growth of companies developing digital technologies – that also means supporting activities aimed at the sector’s start-up community.

For example, the strategy foresees close cooperation between Startup Estonia – a governmental initiative aimed to promote the Estonian ecosystem to enable the country to be the birthplace of many more start-up success stories to come27 – and the Ministry of Economic Affairs and Communications in order to support various initiatives, including seminars, dialog, and mentorship programs. It also envisages the creation of an accelerator for companies in the cyber sector that are past their first development phase, in order to expand globally.

The strategy underlines the importance of systematic risk assessment and provides advice to public and private sector institutions on matters related to future technologies. The effectiveness of cybersecurity depends largely on the unified functioning of the cybersecurity community. The latter depends on the effective flow of information, strong partner relations and personal contacts between and among experts from different fields, encompassing government institutions, the private sector, and academia. PPP is also regulated by other national laws like the Cybersecurity Act28 and the Emergency Act.29

Today, it is fair to say that the cybersecurity ecosystem fosters different types of PPPs.30 The multistakeholder model is a natural part of Estonia’s wider Digital Agenda 2020, which similarly espouses public–private collaboration as a mindset and encourages “new ways of involving private companies” in developing cybersecurity solutions.31

---

ORGANIZATIONAL AND ADMINISTRATIVE CYBERSECURITY FRAMEWORK IN ESTONIA

Cybersecurity is a vital part of Estonian defense systems and planning. Most importantly, it is needed to protect the Estonian e-lifestyle and thus, the main responsibility lies not within military, but civilian structures. Since 2011, the Ministry of Economic Affairs and Communications\textsuperscript{32} has been responsible for the general coordination of cybersecurity policy.

The Cyber Security Council of the National Security Committee of the Government was founded in 2009 and is regulated by the Security Authorities Act.\textsuperscript{33} It assesses progress in implementing the National Cybersecurity Strategy, while the Government endorses the strategy and implementation plans. The Cyber Security Council is led by the Permanent Secretary of the Ministry of Economic Affairs and Communications. It includes representatives from seven Ministries, appropriate government agencies, the Government Office, and the Estonian Defence Forces. The Council is served by an expert-level interagency coordination group that meets regularly. Based on need, the meetings can be extended to include private sector, academic, and research institutions.

One such key institution – the Estonian Information System Authority (RIA)\textsuperscript{34} – is situated within the jurisdiction of the Ministry of Economic Affairs and Communications. RIA coordinates the development and administration of information systems, ensuring the interoperability of the state’s information system, organizes activities related to information security, and handles security incidents in Estonian computer networks. As such, RIA is the primary governmental body to assist the private sector in bolstering the cybersecurity of essential services. RIA organizes the protection of critical information infrastructure (CIIP), fulfils Computer Emergency Response Team tasks at the national level, and conducts state and administrative supervision of compliance with the Cybersecurity Act.

The national CIIP system could be viewed as an example of institutional PPP with the RIA overseeing the smooth functioning of CIIP, including ensuring the cybersecurity of providers of vital services. RIA controls the implementation of security measures in the information systems of state and local government agencies, essential services, communication services, trust services, and digital service providers. RIA distributes instructional materials,
organizes training programs, and addresses queries from companies. It is important to stress that RIA does not implement cybersecurity measures on behalf of others – its role comprises monitoring and providing guidance to all essential service providers.

An important aspect of RIA’s role is to raise awareness of cybersecurity risks and issues among the public sector, the private sector, and citizens. Since 2013, RIA has been publishing annual cybersecurity reports (assessments). RIA also publishes regular updates on the situation in cyberspace as well as overviews of its activities. RIA’s early warning system issues alerts enabling different stakeholders, including individual persons, to take measures that would prevent or reduce the impact of the cyber incident. The efficiency of this system was demonstrated by the impact of the WannaCry and NotPetya ransomware in 2017. While these significant cyber incidents cost the global economy billions of euros, in Estonia, the losses were minimal. According to RIA, damage prevention was the result of both systematic preventive measures and rapid response.

RIA has close communication and information exchange with essential service providers. They also offer free-of-charge security tests, facilitate the exchange of best practices, and offer cybersecurity advice to the private sector. As an example of its hands-on support, in 2019, RIA offered free penetration testing to companies, including hospitals, electricity and water companies. In 2020, its focus was on healthcare providers and the energy sector. RIA also offers training with the aim of sharing best practices as well as broadening the cyber community. At a time of crisis, this would enable the best experts to be convened from a pool of cyber specialists in the public and private sectors in Estonia.

RIA is also cooperating closely with Enterprise Information Security Architecture (EISA) – an association founded in 2018 to boost cross-sectorial cooperation between academia, the private sector and the government. All the founding companies of EISA have notable examples of cross-sectorial collaboration, and EISA intends to further enhance research and development activities in the information security and cybersecurity field in Estonia. The EISA–RIA collaboration could be seen as a goal-oriented PPP.

---

CYBER DEFENCE UNIT OF THE ESTONIAN DEFENCE LEAGUE

One of the most unique examples of PPPs that owes its origins to the 2007 cyber-attacks is the Cyber Defence Unit (CDU) under the Estonian Defence League. The Estonian Defence League is a voluntary national defense organization affiliated with the Ministry of Defence that not only possesses weapons but also conducts military exercises. The purpose of the Defence League is to “enhance the readiness of the nation to defend the independence of Estonia and its constitutional order by relying on free will and self-initiative.”

CDU is a format that, according to EISA-set PPP categories, falls under the goal-oriented PPPs. PPPs of this type are created for the purpose of building a cybersecurity culture in a state. There is usually a platform or council established, which brings the private and public sector together to exchange knowledge and best practices. The CDU unites cyber experts from the public and private sectors under military command. Legally, the CDU operates under the direction of relevant governmental agencies, for example, the RIA and the Cyber Command of the Estonian Defence Forces.

Membership in the CDU is strictly voluntary and comprises experts with different backgrounds and experience. Besides IT experts, there are lawyers, economists, professional military personnel, doctors, etc. CDU is a unique structure to test different ideas and solutions. Most importantly, it provides confidence that in times of crisis, the best assets are in place to counter any attacks. In cases of (military) cyber activities, the CDU provides a vehicle to handle a situation that could escalate from peacetime to an emergency or wartime crisis.

The CDU focuses mainly on training and exercises for its volunteer members, but it also carries out international cybersecurity cooperation projects, such as cooperation with the Maryland Air National Guard. Alongside the US, other international engagements have taken place with partners in Latvia, Ukraine and Georgia, among many others. The CDU has also been included in certain tabletop exercises, penetration testing, or open-source monitoring and analysis.

In addition to formal PPPs, it is important to have less formal ones. Informal cooperation formats can contribute to more effective information sharing between relevant actors and create trusted partnerships for cooperation in times of crisis. All relevant stakeholders must be confident that they are invited to contribute not only because it is politically correct to do so, but because their experience and commitment are truly valued. Only then can we talk about the natural development of PPPs and long-term partnerships.

INTERNATIONAL COOPERATION AND PROMOTING MULTISTAKEHOLDER MODEL

Cyberspace does not have borders, and Estonia considers international cooperation, as well as multistakeholderism, of utmost importance. The importance of international cooperation was also one of the lessons learned from the 2007 attacks. Therefore, Estonia participates in and contributes to different forums, from the UN Group of Governmental Experts (UN GGE) on ICT security to regional forums for cooperation between Baltic and Nordic states. They all have an important role to play, depending on their focus and objective. One of the priorities of Estonia has been the promotion of PPPs and raising awareness about different forms of cooperation with stakeholders.

Estonia has participated in five GGEs, including the sixth (2019–2021). From the very beginning, an informal group of experts from very different fields and institutions, including the private sector and academia, has advised Estonian GGE experts. Following the advice of this informal group, Estonia’s contribution to the third UN GGE (2014–2015) underlined the importance of the protection of critical financial infrastructure. Estonia proposed “to focus particularly on the issue of stability and security of the financial system, which we consider to be in the interest of all states due to its centrality for the functioning of individual economies as well as the global economy as a whole.” Estonia also suggested consulting with academia and experts on the issue of the applicability of international law to cyber issues. Both topics have since received strong international support. The protection of financial systems against cyber threats has been studied by experts such as Tim Maurer and

---

40 The UN Group of Governmental Experts on Advancing Responsible State behavior in Cyberspace in the context of international security was established by the UN Secretary-General and has had six sessions since 2004. Estonian experts have participated in five sessions; they did not participate in the first session (2004/2005). Marina Kaljurand was the Estonian expert in 2014/2015 and 2016/2017.

Taking stock of Estonia’s multistakeholder cyber diplomacy

Arthur Nelson,

as well as governments (e.g. G20 finance ministers)

The Tallinn Manual,

written by leading international law experts, is an influential

It is encouraging that the Report of 2020–2021 GGE

also underlines the

importance of cooperation with “other stakeholders such as the private sector, academia, civil society and the technical community” and recommends future

work on “identifying mechanisms that facilitate the engagement of other

essential stakeholders, including the private sector, academia, civil society and the technical community in efforts to implement the framework of responsible

behavior, where appropriate.”

It can be argued that the multistakeholder approach has finally been estab-

lished and recognized internationally as a new reality of digital cooperation,

also in the field of cybersecurity. At least, this seems to be the conclusion to be
drawn from various political statements. The Paris Call for Trust and Security

in Cyberspace launched by President Macron in 2018, “calls for all cyberspace
actors to come together to face digital threats endangering citizens and infra-
structure” and “encourages states to cooperate with private sector partners and
civil society.”

The Report of the UN Secretary-General’s High-level Panel

on Digital Cooperation, “The Age of Digital Interdependence,” considered
“models of digital cooperation to advance the debate surrounding governance in the digital sphere.” The Report states in the Executive Summary that “effect-
dive digital cooperation requires that multilateralism, despite current strains, be
strengthened. It also requires that multilateralism be complemented by mul-
tistakeholderism – cooperation that involves not only governments but a far
more diverse spectrum of other stakeholders such as civil society, academics,


technologists and the private sector.” This understanding is one of the cornerstones of the Report and was reiterated in the UN Secretary-General’s Roadmap for Digital Cooperation.

One of the practical examples of multistakeholderism is the Global Commission on the Stability of Cyberspace (GCSC), that I chaired from 2017 to 2019, and that was chaired by Michael Chertoff and Latha Reddy until 2020. GCSC was launched by the Dutch Government in 2017 and comprised 26 prominent Commissioners representing a wide range of geographic regions, as well as a diverse group of stakeholders. GCSC promotes multistakeholderism particularly strongly in its final report, Advancing Cyberstability (2019).

Besides global forums, Estonia is actively contributing to regional cooperation – NATO and the EU, in particular. Both organizations are strong supporters of PPP, within the organizations but also globally.

Tallinn is the home of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) – an operationally independent international military organization that was set up in 2008. The CCDCOE is funded as well as directed by voluntarily participating states. It is a multinational and interdisciplinary cyber defense hub that focuses on cyber defense research, exercises, training and education in both the technical and non-technical aspects of cyber defense. The Tallinn Manual has long been the flagship research product of the CCDCOE, with the first edition (1.0 on the international law applicable to cyber warfare) published in 2013, the second (2.0 on the international law applicable to cyber operations) in 2017, and a third on the way.

---

50 Until Kaljurand was elected to Riigikogu (Estonian national parliament) and the European Parliament.
As for the EU, it is paying more attention to public–private partnerships in cybersecurity. The EU Commission has joined with key industry partners to work on the grand challenges of tomorrow, including investing jointly in research and innovation.

Another important regional initiative of PPP is the OSCE Confidence-Building Measures, in particular Confidence-Building Measure 14 (CBM14) which promotes public-private partnerships. The implementation of most cybersecurity CBMs presumes the existence of relevant cyber capacities within a state, both in the public and the private sector. Therefore, the common aim of states adopting CBM14 would be to share best practices across the OSCE region in order to learn from each other and contribute to the wider capacity-building efforts within the region. The OSCE provides a robust platform to promote such cooperation models in its 57 participating states.

Finally, regional cooperation among Baltic (Estonia, Latvia, Lithuania) and Nordic (Finland, Sweden, Denmark, Norway, Iceland) states is also important.

Estonia has made considerable effort to bring high-level political attention to the importance of PPPs in cybersecurity. In September 2017, when Estonia held the EU Presidency, Estonia organized a strategic-level cyber exercise for the EU Defence Ministers, EU High Representative and NATO Secretary General with a timely scenario – a cyber-crisis unravelling before their eyes. It started with what seemed to be a minor cyber incident and developed into a real blockade of communications systems that stopped a naval operation in the Mediterranean. The exercise brought to the Ministers’ attention various questions – for example, how to effectively share classified information across borders, between NATO, and the EU; how and when to inform civilian partners, for example, ports and power stations, of an attack; and if the EU has to ask for NATO assistance, how exactly to make the request.

It is important to understand that cybersecurity is not only a matter for technology professionals or technical experts to address. It is necessary to raise awareness among politicians and civil servants, as well as the private sector and wider population, at the national and international levels. In that regard, Estonia has contributed significantly to capacity and confidence-building measures. Digital cooperation is a significant part of Estonia’s overall devel-

opment cooperation agenda, and Estonia is focusing on good governance and the digital transition of societies.56

CONCLUSION

The digital revolution is here to stay. It brought the benefits of ICTs as well as challenges that were not known before. The digital ecosystem changed the traditional and often exclusive role of states in providing online services to the population and subsequently, the distribution of responsibilities with respect to national and international cybersecurity. States and governments remain at the center of digitalization and have a unique role. But governments alone cannot be successful in the use of ICTs. They must establish effective and operational ways of cooperation with other actors, including industry, the private sector, the IT sector, academia and civil society. In addition, the timely engagement of politicians and parliamentarians is crucial as they influence critical political and financial decisions. Digital literacy should be a lifelong learning process starting from the earliest stages of a child’s education.

In summary, Estonia’s championing of multistakeholder cyber governance and diplomacy was supported by three important domestic factors. The first was the political will and bold decision-making of Estonia’s government. Two such historic decisions are worth highlighting – the decision to go digital, and the decision to invest in the private sector’s digital capacity. Also, starting with the very first digital strategies, digital PPP has been an important part of Estonian legislation. Second, Estonia had luck with timing. From the late 1980s to the early 1990s, Estonia was undergoing democratic reforms. At the same time, the Internet ceased being an isolated island for IT geeks, and the digital revolution went global. It allowed Estonia to develop what was, at the time, a very innovative digital society, which is known today as e-Estonia. Third, Estonia has always promoted practical, trust-based cooperation between different stakeholders on cybersecurity, which was seriously challenged during the 2007 cyber-attacks. Estonia’s Cyber Defence Unit of the Defence League is a unique structure that developed from close cooperation with the private sector before and during the 2007 attacks.

The Estonian experience (and success) with multistakeholderism is unique. There is no general rule or framework of PPP that suits all states, but there are policy fragments and best practices that could be used as models. Every state has its own road to PPP. It starts with recognition that PPP is of real value and

---

not simply a political slogan. Effective PPP is built on trust and must include all relevant stakeholders. The importance of multistakeholderism has been recognized nationally and internationally. Now it is time to move from slogans to real cooperation. The ball is in the court of states and their governments.
PART IV

Conclusion
12. The way ahead for multistakeholder cyber diplomacy

Ian Johnstone, Arun Sukumar and Joel Trachtman

As the virtual Symposium that led to this edited volume itself highlighted, robust and international exchange of ideas and perspectives among various actors today are commonplace and reflect the gradual acceptance of multistakeholder dialogue in international cybersecurity. Private actors seeking to influence the articulation and implementation of cyber norms have not only been able to engage more frequently – the COVID-19 pandemic’s making many such meetings virtual has drawn bigger and diverse groups together – but also have been able to strategically identify allies, and collectively improve their bargaining power vis-à-vis states. The heightened visibility of these non-governmental actors and their persistent efforts at gaining entry into otherwise closed multilateral forums have also emboldened states to engage and even co-opt them to further their own interests in this domain.

France’s attempts during the last lap of UN Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) discussions to generate multistakeholder support for its “Programme of Action” (PoA) proposal is a case in point. The PoA, co-sponsored by France and Egypt, with nearly 40 states endorsing the proposal, was billed primarily as a mechanism for regularized institutional dialogue on cybersecurity at the UN. Notwithstanding political deadlock on the issue of creating binding instruments for state behavior in cyberspace, the PoA did not shy away from holding itself up as the prospective forum where deliberations towards a cybersecurity treaty could begin. To non-state actors, however, the PoA was highlighted as a mechanism and opportunity to cement private participation in otherwise closed discussions at the UN. In other words, multistakeholder participation was the carrot dangled by the PoA’s state sponsors in return for the support of non-state actors for the proposal. It is also notable how France marshalled the support of the multistakeholder community that it had already helped create under the Paris Call framework and working groups towards the PoA proposal. Similarly, Freedom Online Coalition (FOC), a group of 34 governments, issued a statement in October 2022 against Iran’s shutting down of the Internet following protests.
Building an international cybersecurity regime

by women in the country.\footnote{FOC Joint Statement on Internet Shutdowns in Iran" (Freedom Online Coalition, October 2022), https://freenlinecoalition.com/wp-content/uploads/2022/10/FOC-Joint-Statement-on-InternetShutdowns-in-Iran_October-2022.pdf.} FOC calls itself a multilateral coalition,\footnote{“Terms of Use,” Freedom Online Coalition (blog), accessed October 30, 2022, https://freenlinecoalition.com/terms-of-use/.} but its legitimacy is bolstered by its expansive network of multistakeholder task forces – including on Internet shutdowns – and advisory boards, which will probably be rallied to support such statements.

While acknowledging such developments and noting how a growing number of states have accepted private participation and inputs in the development of the international cybersecurity regime, participants at the Fletcher Symposium also identified three reasons why multistakeholder cyber diplomacy is far from being the norm.

First, as one diplomat perceptively noted, even the states open to multistakeholder participation in this domain were “more comfortable with informal cooperation” with private actors, rather than formal mechanisms of engagement. In his chapter on the multistakeholder cyber diplomacy of the United States government, Christopher Painter makes precisely this point and calls on the US to be more accommodating of formal processes.

Second, the shadow of geopolitics still looms large over multistakeholder cyber diplomacy. The instance of Russia and Ukraine summarily rejecting the requests for participation by a large number of non-government organizations (NGOs) in the 2021–2025 OEWG illustrates this point. Although the NGO accreditation process in the OEWG, as the introductory chapter notes, has been streamlined and made modestly more transparent owing to pressure from multistakeholder coalitions, this did not stop both countries from rejecting those actors based respectively in Western states and Russia. Caught in the crosshairs of the Ukrainian conflict were private actors with global interests, such as Kaspersky, Microsoft, the CyberPeace Institute, Cybersecurity Tech Accord, and the Global Forum for Cyber Expertise. Other NGOs excluded were technical and academic bodies that have sought to identify and implement rules and norms for the domain – prime examples being the Oxford Institute for Ethics, Law and Armed Conflict, which convenes the Oxford Process on International Law Protections in Cyberspace, as well as the Forum for Incident Response and Security Teams, an important coordination body for CSIRTs (cybersecurity incident response teams) that includes members from Asia, Africa, and Latin America. Whatever their affiliations, it is difficult to conceive of effective multistakeholder cyber diplomacy without the participation of these important actors with global stakes. Yet, as international relations go through a period of turbulence – the Ukraine conflict has been a major cause
of such turbulence, as is the prospect of Great Power conflict between the US and China – their participation will probably hinge on extraneous geopolitical factors.

Third, disparities of resources and capabilities can skew multistakeholder cyber diplomacy towards the preferred priorities of powerful non-governmental actors. As multistakeholder dialogues on international cybersecurity gain visibility and influence, their legitimacy will be closely scrutinized. It is already the case that UN-centric multistakeholder initiatives are organized largely by companies and NGOs based in the Global North. At the June 2021 Symposium, some participants underlined that the legitimacy of multistakeholder diplomacy should not be seen solely as a matter of form, evaluated on the basis of representation (or the lack thereof) at the negotiating table. Even if a multistakeholder initiative has pro forma representation from a diverse set of actors, it could be the case that many participants do not have equitable access to relevant information about specific proposals, or their “buy-in” may be sought simply as “last-mile” supporters or signatories.

Others supported the view that an inclusive norms process, while appearing to be legitimate, may impede efforts to meaningfully address cybersecurity concerns, with broad participation resulting in more frequent deadlocks. In that case, it may be helpful to begin with a “beachhead” group that consolidates negotiated outcomes and builds support for those outcomes from affected constituencies. As Josephine Wolff notes in her analysis of cyber norms initiatives for this volume, the Paris Call, OSCE CBMs, and even the Tallinn Manual represent such beachhead initiatives, aiming to develop and consolidate common understandings around responsible state behavior in cyberspace. However, “as more norms processes have emerged around cybersecurity,” she concludes, “it’s not clear that they’ve necessarily fragmented the international normative structure so much as they have created additional forums for generating streams of input into the GGE and OEWG processes.”

The chapters in this edited volume evaluate these concerns from national, comparative, and global perspectives. Josephine Wolff and Arun Sukumar survey, respectively, the landscape of multistakeholder cyber diplomacy (Wolff) and evolving approaches of Great Powers as well as major cyber powers to the participation of private actors in norms articulation and implementation (Sukumar). Their chapters serve as an important reminder of the centrality of states to the form and substance of multistakeholder cyber diplomacy.

As Wolff notes, multistakeholder initiatives appear to be proliferating in number, but most still continue to revolve around the UN processes. If, as the introductory chapter to this volume highlights, some initiatives like “Let’s Talk Cyber” aim to make the UN OEWG more accountable to non-state stakeholders, others such as the Paris Call have mirrored or consciously sought
to influence the work of the UN GGE and OEWG. With both processes “borrowing” the vocabulary of international law to articulate voluntary norms of state behavior, the UN GGE and OEWG have also arguably influenced processes that apply or identify existing rules for the domain, such as the Tallinn Manuals or the more recent Oxford Process for International Law Protections in Cyberspace.

Yet, as Sukumar argues, the geopolitics of multistakeholder cyber diplomacy is complex and fluid, permitting no easy categorization of states as its allies or foes. Even as Russia has consistently sought to prevent the opening up of the UN General Assembly’s First Committee discussions on cybersecurity, it has orchestrated multistakeholder diplomacy under the National Association for International Information Security umbrella. China has tolerated multistakeholder engagement in international cybersecurity but held non-state participation in First Committee discussions at arm’s length, ostensibly to separate “multistakeholder” and “multilateral” diplomacy. However, given its own proposal to raise “data security” as an issue for the First Committee’s consideration, China may have to revisit this strategy. Any attempt to tackle complicated questions around the security of cross-border data flows or the sovereign prerogatives of states with respect to the data of its subjects held extra-territorially requires some cooperation from multinational companies. Beijing may therefore be inclined to craft multistakeholder initiatives of its own, with Chinese technology companies taking the lead as norm entrepreneurs or signal greater willingness to engage with private actors on the articulation of international cybersecurity norms. China has declared its Global Initiative on Data Security (GIDS) is open to multistakeholder inputs, but it remains to be seen how those inputs will shape the initiative.

The United States’ reluctance to support multistakeholder cyber diplomacy, despite longstanding domestic initiatives to absorb private sector input on the topic, stands out as surprising and dissonant with the positions of its Western allies and partners. Yet, even the traditional US view that states are exclusive interlocutors in matters of disarmament and arms control – the remit of the First Committee – is evolving in the face of strident Russian opposition to multistakeholder participation at the OEWG. Microsoft, with whose positions on cyber norms and rules the U.S. government has sometimes clashed, was integrated into the US delegation to the OEWG in 2022 following Russian rejection of the company’s participation in the group. In another indication of geopolitics influencing the outcome of multistakeholder diplomacy, the

---

US endorsed the Paris Call in 2022 after staying away from the initiative for nearly four years – this decision was probably an attempt at rapprochement with France following a US–Australia agreement to transfer nuclear submarine technology that undercut negotiations between Paris and Canberra.

The evolution of Great Power attitudes towards multistakeholder cyber diplomacy has been gradual and instrumental. To be sure, this is not necessarily a bad outcome. As Great Powers jostle to orchestrate the participation of favored non-state actors or thwart those affiliated with their adversaries, cyber diplomacy emerges as a competitive arena that offers opportunities for private actors to build strategic coalitions to their advantage. The Ukraine conflict and rising US–China tensions have undoubtedly made it more difficult for Great Power consensus to steer and pave the way for regime development in cybersecurity. But it is equally a glass-half-full moment for private actors who want to develop their agenda with other like-minded states, especially middle powers such as Australia, Canada, France, Japan, and the EU, who may be frustrated by deadlock at the high table.

If multistakeholder cyber diplomacy has a future, an equally important consideration is the form that it takes within the international cybersecurity “regime complex.” Joel Trachtman and Ian Johnstone’s chapters emphasize the importance of effective regime design, by highlighting why states may support multistakeholder cyber diplomacy and how multistakeholder institutional arrangements may be imagined. Trachtman draws attention to power, legitimacy, and expertise-based considerations that compel the creation of multistakeholder arrangements on international cybersecurity. His review of comparable arrangements in other domains such as global health, labour, and standards-setting, presents interesting conclusions. Multistakeholder cyber diplomacy could have a higher chance of success when it is mission-focused and oriented towards specific tasks (the “GAVI model”). Given the expertise and legitimacy of non-state actors such as the private sector and Internet bodies in developing technical standards, multistakeholder engagement is also likely to be fruitful (the “ISO model”) in the articulation and implementation of technical cybersecurity norms – an aspect Wolff also highlights. On the other hand, it is a reality that governments still enjoy the trust of domestic constituents over market actors in many parts of the world, including developing countries. Private sector actors will pursue their own self-interest and may capture governance processes in a way that is inconsistent with the public interest. Therefore, it may be prudent to develop state-centric multistakeholder arrangements (the “Codex Alimentarius model”) – featuring advisory inputs from non-state actors and expert groups – to articulate and implement norms on such matters as critical infrastructure protection or supply chain integrity.

Johnstone bookends his chapter on the range of mechanisms that could be established for implementing cybersecurity norms with two connected
observations that are especially relevant for practitioners of multistakeholder cyber diplomacy. “Just as soft law can harden, hard law can soften,” he argues, challenging the view that the evolution of cyber norms is always progressive. If the push for implementation mechanisms in international cybersecurity gets ahead of their political context, it is likely that such arrangements not only fail to induce compliance with norms but also discourage their wider adoption among states or industry. Johnstone’s concluding observation is therefore that the development of a single, universal international cybersecurity regime is unrealistic. Developing a sliding scale of implementation arrangements, ranging from non-intrusive information-sharing practices to highly intrusive collective sanction mechanisms, he also identifies ways in which multi-stakeholder participation can strengthen these tools. The good news is first that a fragmented cybersecurity regime complex provides non-state actors a number of opportunities to meaningfully contribute and strengthen its legitimacy as well as “compliance pull.” Second, implementation mechanisms (for example, coordinated attribution) can help to crystallize inchoate norms and even lead to the development of new norms. The not-so-good news is that the design of these institutional arrangements will be determined by the art of the politically possible and technically feasible. It is conceivable that some elements of the regime – capacity building, monitoring and attribution – may pull ahead of other contentious ones – sanctions and dispute settlement. This raises two questions: how effective will a partially developed regime with few enforcement mechanisms be? Second, will first-movers who develop some crucial elements of the regime also orchestrate the creation of other mechanisms to the exclusion of late entrants?

The evolution and future of multistakeholder cyber diplomacy, and its impact on the international cybersecurity regime is not a factor of global considerations alone. Domestic considerations play an equally important role in influencing the approaches of states and the priorities of private actors. To this end, the chapters in this volume on China, Russia, the United States, Brazil, Estonia, and India offer the following indicators:

1. the constellation of domestic actors who are likely to shape the cyber diplomacy of those states;
2. discernible moments in the timelines of these states that have tipped the balance towards or against multistakeholder participation domestically and internationally; and
3. issues that are likely to be championed by cyber powers through multistakeholder diplomacy.

Notably, some common strands and cross-cutting themes emerge from the analyses of national approaches. One such commonality is the historical role
and influence of private actors, especially the technical community, in the governance of the Internet in both developing and developed countries.

- Jinhe Liu outlines the evolution of the Internet governance and cybersecurity ecosystem in China, noting in particular the early roles of the Internet Society of China, the Cybersecurity Association of China, and the country’s academic and technical communities in articulating and implementing policies. Private actors even played a crucial role in the governance of key institutions like China’s Internet Network Information Centre (now managed by the government) and National Computer Network Emergency Response Technical Team.

- In Russia, Andrey Shcherbovich notes, Internet companies like Kaspersky, Yandex, and mail.ru, as well as universities and NGOs such as HSE, MGIMO, Internet Protection Society, and Roskomsvoboda, are all actors with independent and powerful interests, and not “under direct government control” despite heavy-handed regulation by the state.

- Brazil has always had robust private participation in the articulation and implementation of Internet policies through the CGI.br and Marco Civil frameworks, argue Carlos Affonso de Souza and Christian Perrone. Brazil’s legacy of domestic multistakeholder internet governance also led it to host NETmundial in 2014, a seminal and pioneering exercise in multistakeholder cyber diplomacy.

- In Estonia, meanwhile, the “Tiger Leap Program” of the nineties was instrumental not only in training the country’s cybersecurity specialists but also in fostering a high degree of trust between Estonians and Internet services: an attribute Marina Kaljurand highlights as critical to multistakeholder digital governance in Estonia.

- Civil society and private sector actors in the United States have been active and longstanding participants not only in domestic cybersecurity debates but also international cyber diplomacy, as Christopher Painter outlines. A notable feature of US diplomacy has been a “multistakeholder component” in bilateral and regional “all of government dialogues” with other states.

- Arindrajit Basu highlights the visible and growing presence of private actors in India’s domestic cybersecurity debates, as well as their direct engagement with multistakeholder processes abroad. However, he argues, this does not seem to correspond to a clear articulation by the Indian government or non-state actors, for that matter, of their roles and responsibilities in multistakeholder cyber diplomacy.
Some chapters also interestingly highlight specific moments that singularly altered a state’s approach to multistakeholder participation in domestic cybersecurity governance as well as multistakeholder cyber diplomacy.

- Liu flags the “milestone marking the beginning of the post-centralization period” of cybersecurity governance in China as the setting up of the Central Leading Group for Cyberspace Affairs under Xi Jinping in 2014. Under the Group, the CAC emerged as a vehicle for “top-level design of cyberspace policy” as well as a prolific issuer of cybersecurity regulation from this period. It is not that multistakeholder involvement in China gave way to a state-centric approach overnight, argues Liu, but that the participation of non-state actors became more streamlined, managed, and guided by state priorities following this moment.

- De Souza and Perrone highlight the Brazilian state’s attempts at extraterritorial regulation of data – as evidenced in a recent Supreme Court ruling and the draft “fake news” bill being considered by the Brazilian lower house – as the beginning of an “erosion of confidence” in Brazil’s multistakeholder model and diplomacy. Their argument, that the need to regulate cross-border Internet activity that has bearing on Brazil is prompting the government to circumvent established multistakeholder processes, has interesting implications for other states as well. With current trends in cybersecurity regulation decisively in favor of “cyber sovereignty,” it remains to be seen whether states similarly dispense with multistakeholder diplomacy – and its attendant checks and balances – to strike intergovernmental agreements on the extraterritorial governance of data.

- On the other hand, Kaljurand highlights the 2007 cyber attacks on Estonian critical infrastructure, widely attributed to Russia, as the catalyst for greater multistakeholder engagement within the country, and a key moment that sensitized Estonia to the need for multistakeholder cooperation globally.

- In Russia, meanwhile, the passage of the “Law on the Sovereign Internet,” which came into effect from 2021, may well constitute that decisive moment from where Russia’s multistakeholder cyber diplomacy (if any) will be tightly orchestrated by the government. However, as Shcherbovich notes, the Russian government will have to balance its domestic imperatives against its hosting of the IGF in 2025 – weighing too heavily against multistakeholder participation in Internet governance and cybersecurity may raise legitimacy concerns about the 2025 edition, which Russia may be keen to avoid for reasons of international prestige.

Multistakeholder cyber diplomacy, then, is likely to be the outcome of two phenomena clashing against each other: the fact that private actors own or manage critical Internet resources around the world versus the reality
that states have increasingly attempted to stamp their authority over those resources, or at least manage the effects of cyber operations on those resources in their territory. It is clear that private actors with global interests are not content with simply backing their governments’ proposals and want actively to chart the creation of rules in international cybersecurity that align with their agendas. The modest successes of the multistakeholder coalition that has sought to make the UN OEWG accountable to private actors are proof that governments must accommodate their concerns. It is, however, also clear that ICANN-like institutions – multistakeholder Internet governance bodies in which private actors set policies, and states play a subsidiary role – are unlikely to manifest in international cybersecurity governance. In fact, it is likely that cybersecurity could be used as a reason by states to diminish the traditional roles of the “I* organizations” in the development of certain standards. The “New IP” proposal floated by Huawei at the ITU – itself a subtle exercise by China in multistakeholder diplomacy, given the proposal had the government’s support – is, for an example, an attempt to bring “deterministic” routing and forwarding to the Internet. In at least some use cases, the proposal is likely to lead to governments having greater control over the security and other operational aspects of Internet infrastructure on their territory.

The participation of private actors in international cybersecurity governance is therefore no guarantee that its outcomes will always favor private interests: multistakeholder cyber diplomacy orchestrated by states can counterintuitively lead to greater state control in some pillars or institutions of the regime complex. The chapters in this edited volume provide a lens through which to analyze such outcomes, combining top-down analyses relevant to the design of the international cybersecurity regime with bottom-up case studies tracing the approaches of important states towards multistakeholder participation in domestic and international cyber diplomacy.

Index

Aaken, Anne van 115
academic community 45, 172, 173, 175, 185, 188, 224
academic institutions 50, 101, 148, 151, 177, 195, 226
accountability 2, 3, 15, 16, 89–90, 92, 108–9, 151, 162, 164, 216, 218, 242, 244, 245
accreditation 5, 6, 9, 10, 152, 154
Address Supporting Organization (ASO) 97, 98
Adler, Emanuel 26
administrative cybersecurity framework, Estonia 246–8
Aliyev, V.M. 170
arbitration 135, 136
attribution 52, 53, 86, 125, 126, 130–33, 136, 138–40, 162, 262
Australia 6, 7, 9–11, 40, 56, 64, 155, 159, 160
Australian Department for Foreign Affairs and Trade (DFAT) 159, 160, 217
Barlow, John Perry 165, 220
Barmpalou, Panagiota-Nayia 50
Basu, Arindrajit 263
Binxing, Fang 36
Biological Weapons Convention (BWC) 129, 134
bottom-up cybersecurity norms 62
Brazil 11, 203, 221–9, 231–6, 263, 264
Brazilian Internet 223, 224
Bureau of International Cyberspace Policy 44
business interests 98, 207
Calderaro, Andrea 14
capacity-building assistance 133
CGI.br 222–8, 233, 263
Chertoff, Michael 252
China 16, 34, 37–9, 55, 167, 185–92, 194, 195, 197–9
China Internet Governance Forum 195
China Internet Network Information Center (CNNIC) 186, 188, 189, 192, 197
China's cybersecurity governance 191, 194
China's reluctance 38
Chinese cybersecurity governance 16, 190–91
model 184–5
post-centralization period 193–5
pre-centralization period 191–3
Chinese cybersecurity norms 16, 185
see also cybersecurity norms
Chinese governance 185, 200
Chinese governance, positions 185–90
governmental actors
cyberspace administration 186
Ministry of Foreign Affairs (MFA) 186
Ministry of Industry and Information Technology (MIIT) 186–7
private sector
Cyber Security Association of China 188
industry associations 187
Internet Society of China 187–8
technology companies 187
technical and academic community
China Internet Network Information Center 188–9
National Computer Network Emergency Response Technical Team/Coordination Center of China 189
scientists 189–90
Tsinghua University 189
Chinese Internet 187, 190, 191, 196, 197, 199
Chinese model 184, 185
Chinese multistakeholder governance cybersecurity, rethinking 184–200
Chinese-style multistakeholder governance model 16, 199
civil society organizations 25
Codex Alimentarius 92, 97, 104–6, 261
collaborative governance architecture (CoGov) 177
collective countermeasures 53, 137, 140
collective mechanisms 125, 137, 139
collective sanctioning mechanisms 137
Community of Practice (CoP) 25, 26
Community Talks on Cyber Diplomacy 7, 8
competition 83, 84, 188, 193
compliance theories 14, 15, 25, 111, 114–18, 126, 127, 135, 207, 234, 262
enforcement model 115–16
legal and diplomatic discourse 118–20
managerial model 117–18
penalties and rewards 114–15
rational choice theory 116–17
confidence-building measures (CBMs) 26, 44, 50–52, 61, 70–73
consensus report 22, 63, 64, 70, 71
constructive dialogue 127, 128, 132, 138
Cooperative Cyber Defence Centre of Excellence (CCDCOE) 252
coordinated attribution 130, 132, 133, 138, 262
Craig, Anthony 133
cross-pollination 83–4
capabilities 87
cyber-attacks, Estonia (2007) 243–4
cyber capacity building 50, 118, 134, 161, 162
cyber conflict 62
cybercrime 50, 82, 166, 167, 186, 220, 236
Cyber Defence Unit (CDU) 248, 249
Estonian Defence League 248–9
cyber diplomacy 5, 8, 9, 11, 13, 20, 23, 45, 46, 51, 127, 201, 215, 258–65
Cyber Diplomacy Act (CDA) 9, 44
Cyber Diplomacy Toolbox (CDT) 23, 51, 52, 58, 118, 119, 125, 127, 137
cyber have-nots 122, 123, 128
cyber haves 122
cyber norms 4, 12, 14, 33, 60, 123, 151, 202, 204–7, 209, 211, 212, 214, 217
collapse 205, 206
formulation 202, 209, 217
negotiations 36, 204, 211, 218
processes 16, 77, 202, 204, 207, 211, 212
cybersecurity 11, 13, 15–17, 60–62, 74–6, 79, 87, 92, 188, 190, 194, 198, 245, 246
CBMs 70–72, 253
ecosystem 246, 263
fragmentation and MSD in 92–3
governance 16, 170, 176, 177, 185, 187, 190, 193–5, 199
negotiations 16, 174
policymaking 170, 173, 185, 233
regulation 186, 264
strategy 50, 52, 126, 245, 246
summit 134
threats 22, 51
treaty 178, 257
see also individual entries
Cybersecurity Act 246, 247
Cyber Security Association of China (CSAC) 187, 188
Cyber Security Council 247
cybersecurity diplomacy 11, 13, 17, 87–90, 186, 189, 221, 231
interests in 87–8
legitimacy in 89–90
power in 88–9
cybersecurity norms 59–62, 65, 66, 71, 72, 74, 75, 77, 78, 85, 87, 115, 121, 149
development 61, 71, 74, 76, 79, 82–4, 91, 122, 149
formulation 108, 202, 204
government, NGO and private sector actors 147–50
implementing 111–40
Building an International Cybersecurity Regime

multistakeholder diplomacy,
Russia’s participation 165–78
processes 59–84
cybersecurity regime 11–18, 24, 123,
125, 139, 212, 217, 222
formulation 201, 202, 205
cybersecurity regime, building
considerations, underlying 120–25
implementation mechanisms 125
collective sanctioning
mechanisms 137–9
dispute settlement 135–7
financial and capacity-building
assistance 133–5
information-sharing and
dialogue 126–8
monitoring and attribution
128–33
Cybersecurity Tech Accord (CTA) 21,
22, 41, 61, 75–7, 79, 80, 84, 86,
149, 152
cyber sovereignty 34–7
cyberspace 5, 13, 40, 43, 44, 47, 48, 64,
70–73, 93, 145, 147, 150, 158,
160, 163, 168, 194, 196, 213, 220
stability, Global Commission 73–5
Cyberspace Administration of China
(CAC) 36, 104, 186, 188, 191,
194–6, 264
cyberspace policy 194, 264
cyber stability issues 143–64
data security 38, 55, 260
democracy deficits 3, 108–9
DeNardis, Laura 92
digital commons architecture (DCA) 177
Digital Geneva Convention 21
digital information 14
digital society 239, 241, 242
dispute settlement 113, 114, 123, 125,
135, 136, 140, 262
DNS governance 55, 56
domestic interests 110, 214
domestic multistakeholder governance
234, 236
domestic non-state actors 53
drafting process 66–8, 226
Drezner, Daniel W. 27
due diligence 49
economic sanctions 115, 137, 171
economy 14, 170, 171, 232
education 107, 172, 173, 188, 252
e-Estonia 238–41, 254
e-governance 50, 203
enforcement model 115, 123
engage-all approach 37
engagement 10, 11, 14, 16, 44, 46, 66,
156, 157, 208, 209, 212, 217–19
enhanced USG–multistakeholder
interaction 158–63
Enterprise Information Security
Architecture (EISA) 248
e-Residency 238, 239
Estonia 17, 121, 238–42, 244–6, 248,
250, 253, 254, 263
Estonian Information System Authority
(RIA) 247–9
Estonia’s multistakeholder cyber
diplomacy 238–54
European Union 2, 3, 13, 22, 47, 50, 51,
66, 104, 123, 127
Fake News Bill 232, 235
financial assistance 133
Finnemore, Martha 60, 113
fragmentation 43, 91, 92, 140, 170
France 13, 22, 23, 33, 34, 41, 44–9, 57,
257, 261
Freedom Online Coalition (FOC) 257,
258
GAVI, Vaccine Alliance 4, 92, 97,
101–2, 110, 124, 261
Generic Names Supporting Organization
(GNSO) 97–9
geopolitics 12, 13, 20, 21, 23–5, 27, 29,
31, 33, 35, 37, 39, 260
Global Commission on the Stability of
Cyberspace (GCSC) 61, 73–9, 82,
84, 91, 93, 96, 150, 252
norms 74, 77, 96
global cyber norms processes 202, 204,
212
global cybersecurity 113, 170
regime 201, 207, 219
Global Forum for Cyber Expertise
(GFCE) 50–51, 134, 140, 155, 215
global governance 23, 46, 108, 123, 133, 136, 170, 199, 204
global Internet governance 17, 166, 177, 178, 195, 222, 224, 228
Russian perspectives 166–70
global norms 59, 60, 84
formulation processes 210, 217, 218
global processes 16, 170, 171, 178, 215, 218
governance 16, 17, 23, 36, 173, 176, 184, 185, 187, 190, 191, 193, 195, 199, 203, 221, 222, 228, 229
government agencies 28, 157, 196, 245
governmental actors 124, 186
government engagement 146, 156
government experts, UN group 62–6
government institutions 244, 246
government-led model 16, 196
government policy 42, 145, 205
government representatives 11, 69, 71, 74, 218, 224
Great Powers 83, 119, 121, 259, 261
Grigsby, Alex 81
Group of Governmental Experts (GGE) 6, 8, 22, 31, 33, 39, 51, 61, 63, 65, 66, 68–70, 72, 77–9, 86, 93–4, 155, 203, 250, 260
norms 93, 94
process 64, 69, 74, 78, 93, 154
Hollis, Duncan 60, 113
Huawei 37, 55, 187, 197, 207, 208, 265
Hu Qiheng 189
implementation mechanisms 14, 110, 113, 121, 123, 125, 128, 139, 262
independent cybersecurity experts 131
India 29, 155, 201–7, 209, 211–19
Indian delegations 202, 203, 213–15
Indian diplomacy 16, 201
Indian government 201, 207, 215, 263
Indian stakeholders 16, 217, 218
industry associations 149, 187, 209
industry capture risks 89–90
industry stakeholders 81, 96, 204
information 35, 70, 71, 100, 101, 107, 108, 118, 125–8, 140, 171, 239
security 34, 62, 78, 93, 122, 174, 186, 247, 248
sharing 126
society 100, 174, 176, 227
sovereignty 34
sphere 34, 35
systems 16, 35, 241, 247
technologies 167, 168, 171, 175, 194
information and communications technology (ICT) 100, 111, 124, 132
input legitimacy 89
intelligence 83, 130, 132
interactions 83, 86, 113, 117, 143, 146, 147, 150, 151, 156, 158, 163, 164
intergovernmental diplomacy 21, 26
intergovernmental organizations 2, 4, 37, 113, 116, 120, 129, 132–4, 136
intermediaries 24, 25, 60, 229
intermediary orchestration 25
international agreements 3, 99, 114, 125, 167
international cooperation 12, 44, 48, 102, 165, 173, 175, 235, 243, 244, 250
international cooperation, Estonia 250–53
international cyber diplomacy 263, 265
international cyber norms 151
international digital strategy 46–8
international engagements 43, 146, 249
international humanitarian law 49, 64, 65, 213, 214
international information security 28–30, 72, 174, 260
international institutions 111–40
International Labor Organization (ILO) 106–8
international labour standards 106, 107
international law 21, 64–6, 86, 109, 114, 116, 118, 123, 127, 137, 155, 213, 252
international organizations 27, 29, 69, 74, 96, 97, 102, 112, 118, 120, 123, 124, 196–8
international peace 85, 137, 139, 148, 203
international relations 3, 21, 26, 28, 51, 92, 110, 112, 116, 129, 222
International Standards Organization (ISO) 86, 92, 97, 103–5, 261
model 261
International Strategy for Cyberspace 145
international treaties 78, 92, 166
Internet 97, 168–70, 173–5, 178, 190–93, 220–22, 228, 230, 231, 233, 237
corporations 38, 188, 196, 263
development 190, 194
International Corporation for Assigned Names and Numbers (ICANN) 28, 29, 55, 56, 97–100, 173, 174, 196, 197, 227–9
Internet Engineering Task Force (IETF) 28, 37, 190, 197, 198
Internet governance 15, 17, 28, 36, 37, 145, 173, 176–8, 195, 203, 220–22, 228–31, 236
debates 15, 143, 203
models 31, 36
Internet governance ecosystem 228, 230
Internet governance ecosystem, Brazil 230–31
unilateral action
consensus-based
standardization 235
direct government regulation 235
geographical reach, national laws 231–3
global content/account removal orders 233–5
Internet Governance Forum (IGF) 31, 33–4, 53, 55, 73, 176–8, 221, 227, 229, 264
Internet Governance Forum Plus (IGF+) 177, 178
Internet intermediaries 230
Internet Security Conference 196, 197
Internet Society of China 187, 263
Internet Voting (i-voting) 242
intersessional meetings 6, 7, 31, 78
Kaspersky 7
Klynges, Casper 46
Krutskikh, Andrei 30
Lauber, Jürg 32
Laudrain, Arthur 48
Law on the Sovereign Internet 168, 264
legislation 14, 110, 176, 192, 195, 224, 226, 227, 232, 233
legitimacy 69, 71, 72, 88, 89, 91, 92, 104, 105, 108–9, 132, 258, 259, 261, 262
Lewis, Jim 151
like-minded countries 43, 69, 79, 153, 154
Liu, Jinping 263
low-cost multistakeholder initiatives 25
Macron, Emmanuel 46
major cyber powers 12, 13, 22, 259
malicious cyber activities 51, 69, 127, 148
Marco Civil da Internet (MCI) 222, 226, 227, 234, 235
market actors 17, 24, 261
Markoff, Michele 42, 43, 65, 156
Martinon, David 46, 48
mass digitization 44
member state consensus 104, 153
Montevideo Statement 228
MSD 89–93, 96, 97, 108–10
accountability 108–9
in cybersecurity 109–10
democracy deficits 108–9
design elements of 90–92
legitimacy 108–9
power 108–9
multinational corporations 25
multistakeholder 5, 11, 16, 17, 23, 27, 38, 145, 152, 155, 185, 199, 203, 204, 209, 236, 259–61, 264
approach 12, 15–17, 34, 36, 44, 47, 55, 57, 227, 229, 231
characteristics 59–84
cooperation 17, 264
initiatives 8, 18, 21, 22, 24, 38, 236, 259
inputs 57, 145–7, 163, 203, 236, 260
institutions 37
involvement 7, 15, 27, 143, 145, 152, 264
mechanisms 17, 128
participation 144–7, 163
processes 178, 206, 215, 225, 236, 263
multistakeholder cyber diplomacy (MCD) 13, 20–24, 27, 29, 31, 34, 38, 40, 50, 53, 55, 56, 257–65
augment diplomatic and coercive tools 50–53
China and 34–40
European Union and 50–53
France and 44–9
geopolitics of 20–58
initiatives 13, 22, 33, 34, 40, 41, 44, 45, 47–9, 53, 55, 56, 58
Russia and 27–34, 177–8
U.S. government 40–44
multistakeholder cyber governance, China 195
government-led model 196
hybrid model 198–9
IETF/ICANN conference 197–8
Internet Security Conference 196–7
private sector-led model 196–7
Sino-US cybersecurity dialogue 198–9
technical community-led model 197–8
World Internet Conference 196
multistakeholder cybersecurity governance 170, 187, 241, 244
Estonian legislation 244–6
multistakeholder cybersecurity governance, Estonia 241–3
multistakeholder dialogue 7, 226
multistakeholder diplomacy 2–18, 23, 27, 44–9, 53, 260
for cybersecurity norms 85–92
cybersecurity norms development 79–81
opportunities and limitations, states 23–7
outcome 16, 260
political economy 85–92
politics, processes, and prospects 2–18
Russia’s participation in 165–78
multistakeholder diplomacy, Brazil 220–37
multistakeholder engagement 9, 13, 140, 144, 146, 158, 159, 205, 217, 261, 264
multistakeholder governance 23, 28, 30, 184, 185, 187, 189–91, 193, 195, 197, 199, 222–4
multistakeholder governance, Brazil 222–3
CGI.br, Brazilian Internet Steering Committee 223–4
domestic scenario 223
international scene 227–8
MCI, Brazilian Internet Bill of Rights 226–7
NETMundial 228–30
port 25/TCP management, anti-spam 224–6
multistakeholder governance structure 99, 199
multistakeholder Internet governance 17, 27, 28, 34, 221
regimes 231, 236
multistakeholderism 12, 13, 203, 206, 228, 229, 239, 250–52, 254
multistakeholder model 77, 79, 184, 185, 190, 191, 195, 196, 239, 246, 250–53
multistakeholder structures, cybersecurity norms 85–110
Munich Security Conference 73, 75
naming and shaming 27, 116, 123, 127, 130, 131, 138, 162
National Association for International Information Security (NAIIS) 29, 30, 33–4, 53–4
national cybersecurity 36, 245
National Cybersecurity Strategy 188, 214, 247
National Digital Security Strategy 45
national governments 4, 14, 17, 89, 90, 92, 107, 110, 124
national sovereignty 167, 168, 193
NATO CCDCOE 67, 68, 72
NETMundial 17, 36, 203, 221–3, 228–30, 263
neutral Digital Switzerland 21
non-compliance 116, 117, 125, 135, 207, 234
non-governmental actors 3, 11, 111, 124, 129, 140, 178, 195, 235, 257, 259
non-governmental entities 20, 32, 102
non-governmental stakeholders 8, 9, 32, 90, 95, 146
global cyber norms processes, negotiating stances 212–16
non-government organizations (NGOs) 2, 4–6, 9, 10, 29, 54, 88, 89, 93, 94, 103–5, 108, 113, 117, 129, 132, 134, 147, 149, 152, 258
non-government stakeholders 146, 151, 158, 245
participation of 20, 23, 31, 166, 264
non-state stakeholder participation 147, 153
non-state stakeholders 79, 95, 152, 153, 159, 259
NotPetya 52
Nuclear Non-Proliferation Treaty (NPT) 134, 137
Nye, Joseph 82, 151
operations of 20, 23, 31, 166, 264
online services 238, 240, 242, 253
operational autonomy 48, 49
Operation Cloud Hopper 52
organizational cybersecurity framework, Estonia 246–8
Organization for Security and Cooperation in Europe (OSCE) 2, 4, 29, 61, 70–76, 78, 79, 147, 252, 253
Painter, Christopher 38, 40, 41
Paris Call 7, 8, 41, 42, 44–8, 56, 57, 76–9, 93, 150, 152, 161, 215, 259, 261
principles 8
Paris Call for Trust and Security in Cyberspace (PCTC) 97
Paris Peace Forum 46, 47, 57
passive multistakeholder cyber diplomacy, India 201–19
actions and engagement 202
civil society and media 209–12
government 202–6
private sector 207–9
peaceful dispute settlement 135
Penalties 26, 114–19, 121, 126, 129, 137–40
power 12–15, 17, 36, 88, 89, 91, 92, 97, 98, 108–10, 121
powerful states 87, 117
pre-centralization period 16, 190–92, 199
private actors 5, 6, 8, 10, 11, 23, 56–8, 257–9, 261, 263, 265
private sector actors 11, 86, 147, 198, 261, 263
private sector interests 99, 100, 109
Programme of Action (PoA) 57, 163, 257
public attribution 116, 130, 131, 162
public–private engagement 144
Public private partnerships (PPPs) 239–41, 245, 246, 248–50, 252–4
reasonableness 89–90
Reddy, Latha 252
regime complex 3, 86, 113, 114, 125, 140, 212, 261, 262, 265
regional organizations 25, 26, 95, 99, 101, 115, 123, 136, 138, 156, 163
responsible state behavior 43, 44, 57, 78, 119, 148, 259
Roskomnadzor 168, 169
Ruhl, Christian 77, 83
Russian Federation 28, 34, 166–8, 170–76
Russian Internet Governance Forum 176, 177
Russian non-governmental stakeholders 172
academic community 172–3
civil society 172
in global cybersecurity and Internet governance 170–73
private sector 171
Russian stakeholders 10, 170
Russia’s cybersecurity diplomacy 173–7
Russia's MCD initiatives 29, 30

Ian Johnstone, Arun Sukumar, and Joel Trachtman - 9781835301546
Downloaded from https://www.elgaronline.com/ at 05/17/2024 02:05:10PM via Open Access. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 License
https://creativecommons.org/licenses/by-nc-nd/4.0/
Sabbah, Cedric 82
Sachkov, Ilya 54
sanctions 26, 27, 51, 52, 58, 114–17, 125, 126, 137, 138, 140, 169
scientists 189, 191, 192
shaming 138
sham standards 27
Shcherbovich, Andrey 263
Sherstyuk, Vladislav 30
Simsek, Betül 115
Single Market program 3
Smith, Brad 21, 46, 130, 151
Snowden revelations 17, 186, 221
soft law 112, 113, 262
sovereign equality 89, 101
sovereignty 34–7, 122, 125, 166–70, 173, 193, 213
breach of 213
stakeholders 14, 15, 17, 25, 59, 61, 62, 66, 79, 81, 83, 84, 143, 154, 156, 157, 161, 163, 217, 227, 244
accountability and 162
Chinese governance, positions 185–90
engagement 15, 72, 144, 145, 158, 161
groups 99, 104, 157, 158, 196, 201, 202, 204–6, 210, 212, 217
interaction mechanisms 159–61
non-government stakeholders 151–2
United Nations stakeholder activity 152–4
U.S. entity participation 152–4
U.S. government stakeholder interaction 154–6
state actors 22, 23, 26, 27, 34, 44, 117, 120, 124, 128, 136, 139
state behavior 56, 154, 257, 260
state interests 78, 214
state policy 29, 172
state responsibility 53, 137
state self-reporting 127
state sovereignty 44, 170
state-to-state diplomacy 2
step-up multistakeholder engagement 161–2
strategic autonomy 44–9
Streltsov, Anatoly A. 28, 29
Sukumar, Arun 260
supply chain integrity 39
support multistakeholder cyber diplomacy 260, 261
Tallinn Manual 53, 61, 66–74, 77–9, 155, 213, 251, 252, 259
Tallinn Manual on the International Law Applicable to Cyber Warfare 66–70
technical community 23, 24, 94, 95, 189, 193, 195, 197, 198, 220, 221, 223, 226, 251, 263
technical cyber norms 81–3
technical standards 27, 82, 100, 101
technological autonomy 48
telecommunications 3, 62, 63, 128, 174, 175, 186, 208, 213, 221
Tiger Leap Program 263
Tikk, Eneken 82
traditional diplomacy 2, 3, 22, 89, 90
transnational cyber activities 3
transnational networks 2
transparency 89–90
transparent process 9
tripartite governance 106, 107
Tsinghua University 189, 190, 197, 198
UN Economic and Social Council (ECOSOC) 4–6, 9–10, 54
U.S. government 28, 37, 40–43, 56, 66, 97, 99, 171
U.S. government–multistakeholder interaction 156–7
U.S. multistakeholder engagement 143–64
doctrinal commitment 144–7
U.S. Strategy for Securing Cyberspace 144
Vaïsse, Justin 45, 46
Verdier, Henri 46, 47
voluntary norms 146, 148, 154, 157, 177
Wang Yi 38
WannaCry 52
weapons of mass destruction (WMD) 134
Wolff, Josephine 259
workers 106, 107
working groups 7, 8, 47, 57, 152, 198, 257
World Internet Conference (WIC) 194–6