CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

PERRY WORLD HOUSE

WORKING PAPER

FEBRUARY 2020

Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads

Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer

Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads

Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer

Carnegie does not take institutional positions on public policy issues: the views represented herein are the authors' own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

+ CONTENTS

Summary

As cyber insecurity has become a growing problem worldwide, states and other stakeholders have sought to increase stability for cyberspace. As a result, a new ecosystem of "cyber norm" processes has emerged in diverse fora and formats. Today, United Nations (UN) groups (for example, the Group of Governmental Experts [GGE] and the Open-Ended Working Group [OEWG]), expert commissions (for example, the Global Commission on the Stability of Cyberspace), industry coalitions (for example, the Tech Accord, the Charter of Trust), and multistakeholder collectives (for example, the Paris Call for Trust and Security in Cyberspace) all purport to identify or operationalize various normative standards of behavior for states and/or other stakeholders in cyberspace. As some of these processes wind down (for example, the Global Commission) and others wind up (for example, the OEWG), cyber norms are at a crossroads where each process's potential (and problems) looms large.

On October 29, 2019, the University of Pennsylvania's Perry World House and the Carnegie Endowment for International Peace convened a one-day workshop titled "Cyberspace and Geopolitics."[1] It brought together three dozen key stakeholders in the cyber norm discourse, including representatives of national governments, international organizations, nongovernmental entities, industry, and think tanks, alongside several chief information security officers and academics from international law and international relations. Participants assessed the various cyber norm processes both individually and collectively. This paper builds on the outcome of those discussions.[2]

The workshop's key takeaway was an embrace of the existing fragmentation of the cyber norm ecosystem. Participants saw the variety of cyber norm efforts not as detrimental but rather as an opportunity to broaden the base of engaged stakeholders and to deepen understandings of normative expectations within relevant communities. At the same time, the workshop highlighted four weaknesses that constrain the effectiveness of these frameworks individually and collectively:

- Inherent characteristics of the cyber domain, especially its low barriers to entry to develop and to use cyber capabilities, that create serious multistakeholder cooperation problems, as states, corporations, proxy actors, and others all would need to adhere to norms
- A lack of transparency about state behavior, which creates an inability to measure norm adherence to differentiate "aspirational norms" from actual "norms" and, within the latter category, to assess the breadth and depth of conformance by relevant actors
- A dearth of great power cooperation to address this global public policy challenge, especially as geopolitics moves from identifying norms to internalizing them within relevant state and other stakeholder communities
- A lack of clear incentives for internalizing norms—that is, articulating concrete benefits for adopting and internalizing one or more cyber norms or the costs that may follow a failure to do so

Four recommendations can address these issues:

1. Focused research on specific cyber norms to measure their alignment with actual behavior in cyberspace and identification of potential gaps between them and among existing accords.
2. A shared global database of cyber processes that can improve transparency on what each process does, who participates, and how its work is received in other processes (that is, what sort of cross-pollination is occurring versus triggering competing or conflicting norm proposals). For example, Carnegie's Cyber Norms Index already tracks existing multilateral and bilateral accords relating to cyber norms.
3. Research efforts to identify a menu of incentives to promote norm adoption and implementation, including a list of potential consequences that can follow cases of nonconformance.
4. More multistakeholder engagement with great powers on exercising their power responsibly to improve the identification and operation of cyber norms for states and other stakeholder groups (for example, industry, civil society).

The paper is divided into four sections. The first section gives a short overview of the manifold forms of cyber threats and the various types of cyber norm processes they have spawned. The next section examines four case studies of cyber norm processes—the GGE, the OEWG, the Global Commission, and the Paris Call—while highlighting the existence of others. The section after that gives a collective assessment of these processes and their interactions. The paper concludes with a section examining the key takeaways and recommendations that emerged from the workshop.

Background: Cyber Threats and Norms

Cybersecurity has become a global problem, whether viewed in economic, humanitarian, or national security terms. In economic terms, the 2017 WannaCry ransomware infected hundreds of thousands of computer networks in 150 countries, with losses totaling up to $4 billion.[3] The White House estimated that the total damages from NotPetya reached $10 billion.[4] According to the U.S. Council of Economic Advisers, malicious cyber activity caused between $56 and $109 billion worth of damage to the U.S. economy in 2016 alone.[5] Individuals, meanwhile, have become all too accustomed to losing access to or control over otherwise confidential information. Researchers identified 5,183 data breaches of 7.9 billion records in the first nine months of 2019, continuing the trend of worsening statistics.[6] Meanwhile, high-profile cyber incidents such as Stuxnet, Russian election interference, and the targeting of an Indian nuclear plant illustrate the national security stakes of cybersecurity.[7]

In response to this threat, many stakeholders have turned to the idea of "cyber norms"—expectations of appropriate behavior in cyberspace—to regulate state behavior and limit damages from malicious cyber activity.[8] To develop and spread these cyber norms, various state and nonstate stakeholders have promoted different processes, including in multilateral, private, industry, and multistakeholder contexts:

- **Multilateral norm diplomacy** involves efforts by states to devise cyber norms for states. The most prominent efforts occur under the auspices of the UN General Assembly's First Committee. Earlier efforts to identify and operationalize cyber norms continue today under a new UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security.[9] At the same time, the UN General Assembly has also constituted a new OEWG with a similar mandate, albeit for a more inclusive grouping of interested member states and UN observers.[10] Other organizations have, moreover, sought to prompt multilateral processes of their own, including the Shanghai Cooperation Organization, the G7, and the G20.[11]
- **Private norm processes** involve groupings of high-profile experts from diverse backgrounds who study and offer recommendations on cyber norms for states or other stakeholders. Even though they may have past or present associations with states, firms, or other institutions, participants work in their individual capacities. The Bildt Commission (formally the Global Commission on Internet Governance) marked an early attempt at this sort of process.[12] The Global Commission on the Stability of Cyberspace and Carnegie's Cyber Policy Initiative are more recent entrants in this category of norm processes.[13]
- **Industry-focused norm processes** involve efforts by industry to identify norms for industry vis-à-vis cybersecurity. The two most prominent examples to date of such processes are the Microsoft-initiated Cybersecurity Tech Accord and the Siemens-led Charter of Trust.[14]
- **Multistakeholder norm processes** refer to inclusive fora that offer multiple stakeholders, including some combination of states, international organizations, industry, civil society, or academia, opportunities to discuss, identify, or advance cyber norms. Sometimes these processes focus on cyber norms indirectly, whether because the process is simply a forum for dialogue (for example, the so-called London Process or the Internet Governance Forum[15]) or because its mission is related to, but separate from, norm making (for example, the Global Forum for Cyber Expertise). In other cases, however, multistakeholder processes have openly campaigned for norms, whether for all stakeholders or specific subgroupings. The NETmundial Initiative did this with a focus on internet governance, the Paris Call focused specifically on trust and security, and the Christchurch Call sought to coordinate normative expectations relating to online violent extremist content.[16]

All these processes share similar goals oriented around forming and/or diffusing shared expectations of proper behavior online. Together, they form a complex web of cyber norm interactions that raise several questions: How are these organizations structured? What strengths (or weaknesses) do they bring to their promotion of cyber norms? How do these apparently competing processes interact? What are the results of redundancy and process fragmentation? Judging each process by its merits, is any one of them ready to consolidate the others?

The October 2019 workshop at Perry World House examined these questions by taking up four case studies of cyber norm processes—the UN GGE, the OEWG, the Global Commission, and the Paris Call—while highlighting the existence of others (for example, industry-led efforts). Workshop participants provided both internal and external perspectives on the structure and strengths and weaknesses of each process.

The UN GGE

The state-driven efforts of the UN GGE have succeeded in the past (especially in 2013 and 2015) in articulating interstate understandings of core cyber norms and the applicability of international law in cyberspace. The GGE's relatively small size and the backsliding evident in its 2017 iteration cut against efforts to identify this process as *the* focal point for cyber norm discussions. Moreover, any such ambition is likely to be further muted in 2019–2020 by the arrival of another cyber norm process at the UN—the OEWG.

Structure

The GGE is one of the more exclusive and state-centric approaches to cyber norms, although it has recently expanded and conducted greater outreach to regional organizations. The original GGE was composed of governmental experts representing fifteen states, which grew to twenty in 2015 and then to twenty-five in 2017. The 2019 iteration will also include governmental experts from twenty-five member states.[17] GGE members include representatives selected by all five permanent members of the UN Security Council. The remaining experts were chosen by their states after the states were selected from a roster of candidates by the Office of the High Representative for Disarmament Affairs on the basis of, among other things, achieving equitable geographic distribution. Brazilian Ambassador Guilherme de Aguiar Patriota chairs the 2019–2021 proceedings.

GGE decisions are made by consensus. The GGE does not publish meeting summaries but may issue a final report. Such reports are subject to word limits that restrict the detail and descriptions they may contain. GGE meetings are closed, and no other governmental or nongovernmental observers are present.[18] Nonetheless, the group has engaged in more regional outreach work recently through six consultations with regional organizations, including the African Union, the European Union (EU), the Organization of American States, the Organization for Security Cooperation in Europe, and the Association of Southeast Asian Nations (ASEAN).[19]

Within the UN, the GGE is part of the First Committee, which deals with "disarmament, global challenges and threats to peace that affect the international community."[20] Given the limits of this committee's mandate, the UN GGE does not focus on cyber issues that member states decided do not fall under the First Committee's purview, including data privacy and espionage.[21]

History

The issue of information and communications technologies (ICTs) in international security has been on the UN agenda since 1998, when Russia first proposed a cyber arms control treaty.[22] Since 2004, there have been six GGE working groups; three of these groups achieved substantive outcomes, which together form the current UN framework.[23] This framework consists of three pillars: (1) recognition of the applicability of international law, (2) nonbinding norms of state behavior in peacetime, and (3) cyber confidence-building measures.

Workshop participants argued that GGE members were talking past one another from 2004 until 2009, with Russia pushing for arms control in cyberspace. In 2009–2010, the conversation became more productive, leading to a joint statement acknowledging the growing risk and paving the way for a more constructive dialogue moving forward. The GGE had its most successful outputs in 2013 and 2015. Several participants suggested that 2013 was a particularly successful GGE, where all participants joined the consensus around the applicability of international law and confidence-building measures.[24] The 2015 UN GGE report added a list of eleven voluntary norms of responsible state behavior in their cyber activities.[25] These include a norm against ICT activity that damages critical infrastructure, a norm against targeting computer emergency response teams, and a norm to respond to requests for help by states whose critical infrastructure has been harmed by a cyber attack.[26] These 2015 norms were later endorsed by the G20.[27]

The 2017 GGE, however, suffered from backsliding, and failed to generate any outcome report.[28] A confluence of factors accounted for the process's collapse. Pressure to be more inclusive had grown the GGE to twenty-five members for whom consensus was more elusive than earlier negotiations among fifteen and twenty experts. The dynamic geopolitical environment of 2016 and 2017 also made agreement more difficult among some of the great power participants. Additionally, certain states appeared to walk back on their commitment to the applicability of international law. In particular, questions of the applicability of international humanitarian law, the availability of the right of self-defense, and whether states could invoke the law of countermeasures to respond to cyber attacks all served as friction points that reportedly prevented consensus.[29] Cuba and Russia were especially opposed to the idea that states may respond to cyber attacks with noncyber means.[30]

Despite the failures of 2017, the United States sponsored a resolution to establish a new GGE from 2019 to 2021. The GGE's mandate includes continuing to study "with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behavior of States, confidence-building measures and capacity-building."[31] The 2019–2021 GGE's first session was held December 9–13, preceded by informal consultations.

Strengths and Weaknesses

The GGE's chief strength lies in its situation within the United Nations and the credibility that UN processes bring to international dialogue. The First Committee's experience with GGEs in other contexts also suggests a time-tested method for mediating consensus among key expert groups. Participation by the major cyber powers (China, Russia, and the United States) creates a venue for meaningful agreement among the actors most engaged in cyber operations. The track record of success, especially in 2013 and 2015, shows that governmental experts can produce concrete outputs that may then diffuse to other contexts. Witness, for example, how other international organizations, like ASEAN and the EU, have endorsed the work of earlier UN GGEs, including the 2015 list of voluntary norms of responsible state behavior in peacetime.[32]

At the same time, the GGE has demonstrated limitations. It is not clear, for example, how widely its list of norms has been internalized by states that have participated in GGEs, let alone states generally. After the 2015 GGE, for instance, Russia reportedly launched a cyber attack on Ukrainian critical infrastructure.[33] The shallow operationalization of GGE norms may be due to the voluntary characterization of the normative outputs. The GGE's closed proceedings and a participation list affiliated with only twenty-five states may also explain difficulties in moving its words on paper to actual practice. More importantly, the GGE's 2017 failure raises questions about the political will to employ the GGE in good faith going forward. It remains to be seen if past successes bridging differences among a diverse group of state experts can be replicated in the current geopolitical context. At the same time, calls by nonstate actors for greater access or input into the GGE process may highlight its exclusionary nature (a feature that works well when those included represent the key intermediaries, but less well on issues where a majority of stakeholders find themselves on the outside of the process).

The UN OEWG

An "open" forum for all UN member states, the recently established OEWG provides an opportunity for states left out of the GGE to engage on issues of cyber norms (engagement that may even extend to nonstate actors through its intersessional consultations). Yet, Russian sponsorship of the OEWG juxtaposed to U.S. sponsorship of the GGE suggests the two processes may operate in tension with each other—progress in one being met by competing proposals, if not outright resistance, in the other.

Structure

Unlike the GGE's twenty-five handpicked member states, the OEWG is open to all interested UN member states. The OEWG's mandate is similar to, yet slightly broader than, the 2019–2021 GGE. It is charged with the following:

- to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States [that is, the 2015 UN GGE norms], and the ways for their implementation;
- if necessary, to introduce changes to them or elaborate additional rules of behaviour;
- to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and
- to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and
- how international law applies to the use of information and communications technologies by States; as well as
- confidence-building measures; and
- capacity-building and [standards for global telecommunications].[34]

In addition to this, the OEWG seeks to institutionalize open-ended dialogue on cybersecurity within the UN, particularly through greater multistakeholder engagement. Thus, the OEWG held an intersessional meeting December 2–4, 2019, that included other stakeholders from industry, academia, and civil society.

History

The failure of the 2017 UN GGE led to competing proposals for next steps. The Russian Federation, in particular, led calls for a new OEWG. The justification for having an OEWG was to provide a "more democratic, inclusive, and transparent" process for cyber norms and related efforts.[35] Rather than voting to endorse one process over the other, UN member states approved both a new GGE and an OEWG in two separate UN General Assembly resolutions.

The OEWG started meeting in June 2019, with the first formal meetings in September chaired by the Swiss ambassador to the United Nations, Jürg Lauber. Almost one hundred states participated in the discussions.[36] There was a lot of optimism among workshop participants about the first set of OEWG meetings. The OEWG's next sessions will be in February and July 2020. Additionally, as noted, the OEWG held an intersessional multistakeholder meeting December 2–4, which marks the first time that states actively sought the input of nongovernmental experts.

Strengths and Weaknesses

Like the GGE, the OEWG shares the strengths—and weaknesses—that come from having a process situated in the United Nations' First Committee oriented toward multilateral agreement and a disarmament mindset. At the same time, however, the OEWG differs from the GGE substantially in allowing for broader participation in a more transparent setting. If the OEWG can reach agreement, this format suggests the possibility of greater (and quicker) diffusion of its outputs. However, having more states engaged in discussions may make it more difficult for participants to negotiate agreement than in the smaller, closed setting of the GGE.

Workshop participants expressed optimism about the OEWG on the basis of its first substantive meeting and its open, multistakeholder structure. Indeed, the GGE and OEWG's overlapping mandates suggest that they could operate as a sum greater than the parts—force multiplying areas of overlapping agreement in positive and reinforcing ways among all nation-states. The two chairs have signaled their awareness of this possibility and a commitment to try to work toward such outcomes consistent with their individual mandates from the UN General Assembly.

But it is important to recall that the OEWG is the product of a Russian proposal designed specifically to substitute for the U.S. call for another GGE. There is a risk that the two processes may thus understand their roles differently and engage in outright competition, if not overt conflict in their outputs. For example, the United States and its allies see the OEWG as a forum for new stakeholders to learn about and spread the extant GGE norms. Russia, in contrast, may prefer to revisit previous GGE reports under the OEWG and revise them to better align with its interests.[37] And while the 2015 GGE agreed on the applicability of the principles of international humanitarian law, this position was not noted in the establishment of the OEWG.[38] In addition to cherry-picking norms, commentators have pointed out that the wording of the UN General Assembly resolution establishing the OEWG is not always consistent with that of the GGE reports.[39] Thus, there are some nascent calls for the OEWG to leverage its mandate to take on broader issues, such as fake news, propaganda, and other information campaigns. Western countries tend to consider such moves as an opening gambit to international regulation of online content in tension with their commitments to free speech. They may thus resist such moves as inappropriate for the OEWG's attention.[40]

The Global Commission

The Global Commission on the Stability of Cyberspace brought together a broad and diverse set of experts on global cybersecurity. Its final report, issued in November 2019, lends legitimacy to the broader cyber norm project and has seeded the content of other norm processes like the Paris Call, but its legacy may be limited as focus shifts to promulgating already established norms.

Structure

The Global Commission was driven by two think tanks, the Hague Centre for Strategic Studies and the EastWest Institute, and funded by several private institutions as well as several states, chiefly the Netherlands, France, and Singapore.[41] The Global Commission was composed of twenty-six prominent commissioners, acting in their individual capacities. It was co-chaired by Michael Chertoff and Latha Reddy and was based in The Hague.[42]

The Global Commission sought to bring together voices with experience in government, industry, academia, and civil society to work on developing and articulating new cyber norms. In addition to the commissioners, a research advisory group drew in additional experts to conduct research to support the group's work. Its norm promotion efforts, including a norm calling on states and other stakeholders to protect the "public core" of the internet from destabilizing cyber behavior, resonated with other cyber norm processes.[43] Several norms in the Global Commission's "Singapore Norms Package" were incorporated in the Paris Call (which the Global Commission signed itself).[44]

History

The notion of global commissions dates to the Cold War, with groups such as the Brandt Commission on International Development, the Palme Commission on Disarmament and Security, and the Brundtland Commission, which introduced the concept of sustainable development.[45] Over the past decade, this framework was extended to address the regulation of ICTs. In the wake of the Edward Snowden leaks, the Centre for International Governance Innovation and Chatham House launched the Global Commission on Internet Governance—also called the Bildt Commission, after its chair, Carl Bildt.[46]

Following this format and the Global Conference on Cyberspace in The Hague in 2015, the Dutch foreign minister, Bert Koenders, launched the Global Commission on the Stability of Cyberspace at the Munich Security Conference in 2017.[47] The Global Commission met regularly between 2017 and 2019, drawing partly on the 2013 and 2015 GGE reports, as well as several other norm-setting processes.[48] Over its lifespan, the commission proposed eight norms, including a call to "protect the public core of the internet."[49] Its final report was released on November 12, 2019, which, beyond reiterating earlier norm proposals, emphasized the need for greater focus on norm implementation.

Strengths and Weaknesses

The Global Commission's chief strength lies in its gathering of expertise from a diverse array of disciplines and backgrounds. The prior work and experience of the commissioners lent credibility to the commission's norm proposals. Having experts with experience in technology, government, industry, and civil society, moreover, meant that its products were not necessarily biased in favor of one stakeholder community (for example, states).

Nonetheless, the Global Commission's funding sources, especially from Western and like-minded governments, could lead some to discount its norm proposals as favoring a liberal democratic vision of cyberspace. Moreover, as an avowedly nongovernmental entity, the Global Commission lacked any formal sources of authority to support its proposals or their implementation. Therefore, the Global Commission's legacy is likely to be indirect, that is, influencing or persuading other cyber norm processes to endorse or adopt its norms as their own.

For workshop participants, moreover, there was a sense that the Global Commission stage may be coming to an end. A number of participants suggested that further elaboration of "norm lists" would have limited utility; the priority for norm processes going forward was said to lie more with norm diffusion and conformance than with continuing to create new norm ideas.

The Paris Call

The Paris Call for Trust and Security in Cyberspace is an effort to build support for nine normative principles to organize the behavior of both states and other stakeholders in cyberspace. Although many of these principles originated in other processes, the Paris Call has broadened support for them with its more than 1,000 signatories and new plans to create communities of interest to investigate mechanisms for further elaborating and improving conformance with these norms. However, until it receives more great power endorsements, the Paris Call may be limited in its impact.

Structure

The Paris Call for Trust and Security in Cyberspace is a multistakeholder initiative led by the French government and supported by Microsoft.[50] Supporters of the call sign on to nine voluntary principles, including principles to protect individuals and critical infrastructure, protect the public core of the internet, and defend electoral processes against cyber activities.[51] According to participants involved in the process, the Paris Call is not meant to be "the one call to rule them all," but rather builds on previous cyber norm processes, seeking to mainstream government and international organization processes beyond state-centered fora. For instance, several of the Paris Call's principles are based on the 2013 and 2015 GGE reports while its call to protect the public core of the internet adopts one of the Global Commission's chief normative proposals. The Paris Call's stated goals are therefore not to replace earlier processes or to create another forum for outlining new norms, but to strengthen existing cyber norm processes.

Signatories of the Paris Call are diverse and are spread across sectors, and the document remains open to additional signatories.[52] Although four of the Five Eyes intelligence alliance (United Kingdom, Canada, Australia, and New Zealand) and all of the EU member states are signatories, the United States is not. Nor is India, China, or the Russian Federation. That said, key stakeholders from companies and tech lobbies in the United States and India have joined the call.[53] The Chinese company Huawei also signed in the summer of 2019, with some organizations raising the question of whether there should be any gate-checking functions for signatory status beyond a stated willingness to support the call's contents.

The idea of a "Paris Call Community" was announced on November 12, 2019, in concert with the call's one-year anniversary. The idea is to form different interest groups dedicated to advancing best practices and building the capacity to conform around each of the Paris Call principles. Microsoft and the Alliance for Securing Democracy have, for example, created the Paris Call Community on Countering Election Interference—a multistakeholder project focused on implementing the third Paris Call principle, working to identify best practices and build capacity to defend against foreign interference in democratic processes.[54]

History

Ideas for a political commitment for cyberspace have existed for some time, including as one of the follow-on ideas to the Microsoft president's original call for a "Digital Geneva Convention."[55] Microsoft found a willing partner in the French government and worked to support French efforts to build a legally nonbinding instrument focused on elaborating a core set of cyber norms for all stakeholders, including states, industry, civil society, and academia.

The Paris Call was formally launched by French President Emmanuel Macron on November 12, 2018, at the opening of the Internet Governance Forum and one day after the centennial observation of the end of World War I.[56] By the time of the conference, the Paris Call had garnered signatures from over 67 countries, 358 companies, and 139 civil society organizations. By January 2020, the Paris Call signatory list had topped 1,000, including 76 countries, 26 public authorities and local governments, 631 companies, and 343 entities from civil society. In addition to nation-states, several subnational governmental actors also joined the call, including the U.S. states of Colorado, Virginia, and Washington.

Strengths and Weaknesses

The Paris Call's chief strength lies in its multistakeholder orientation. It enjoys a broad base of participation from all levels of governments, industry, and civil society. It is also structured to carefully position itself as complementary to other cyber norm processes, lessening the potential for it to be perceived as competing with such processes. This has helped it gain broad adherence.

Workshop participants emphasized that signatories to the Paris Call include many small countries with high ambitions, but high-tech democracies like the United States and India, as well as other great powers, are missing. This may be due to slight variations in the Paris Call's contents to processes such as the GGE that have engendered great power support. This may explain why certain actors such as the United States have not endorsed its formulation. Other aspects of the Paris Call, such as positive support for the Budapest Convention on Cybercrime, may explain the hostility of states like Russia and China.

The issue of membership also goes the other way, as some workshop participants questioned whether the Paris Call should have a stronger vetting process. For instance, with Huawei recently joining the Paris Call, there were concerns about the sincerity of signatory commitments.[57] Other participants questioned whether the Paris Call continued a tendency to emphasize words over action. This may be a weakness of cyber norm processes generally, without further efforts to map current conformance trends or other mechanisms to diffuse these norms in ways that directly affect the behavior of those responsible for cybersecurity.

Other Cyber Norm Processes

Workshop participants focused their attention on cyber norm processes that sought to create rules of the road for states. Thus, the workshop did not devote much attention to industry-led cyber norm processes. But such processes have had increasing visibility in recent years. At the 2018 Munich Security Conference, Siemens and eight industry partners announced and signed a Charter of Trust. Since then, signatories include major German and U.S. actors in ICTs such as AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, SGS, Total, and TÜV Süd.[58] The Charter of Trust contains three major commitments: "protect the data of individuals and companies," "prevent damage to people, companies and infrastructures," and "create a reliable foundation on which confidence in a networked, digital world can take root and grow."[59] Similarly, the Cybersecurity Tech Accord is a group of over one hundred technology companies that publicly commit to "improve the security, stability, and resilience of cyberspace."[60] The Tech Accord contains four core principles for companies: strong defense, no offense, capacity building, and collective response.[61] Notably, both the Charter of Trust and the Cybersecurity Tech Accord have signed on to the Paris Call, suggesting these industry-led processes can cooperate with more state-oriented ones.[62]

In addition, several workshop participants called attention to the statement released September 23, 2019, by the United States and twenty-six other countries.[63] The "Joint Statement on Advancing Responsible State Behavior in Cyberspace" endorsed earlier cyber norm efforts, including the GGE reports from 2010, 2013, and 2015, along with the OEWG, as possible avenues toward an "international rules-based order" to "guide state behavior in cyberspace."[64] It remains to be seen, however, whether the joint statement signatories will use their common ground to advance existing cyber norms or hold others accountable for actions inconsistent with them.

Process Competition, Collaboration, and the Benefits of a Fragmented Norm Ecosystem

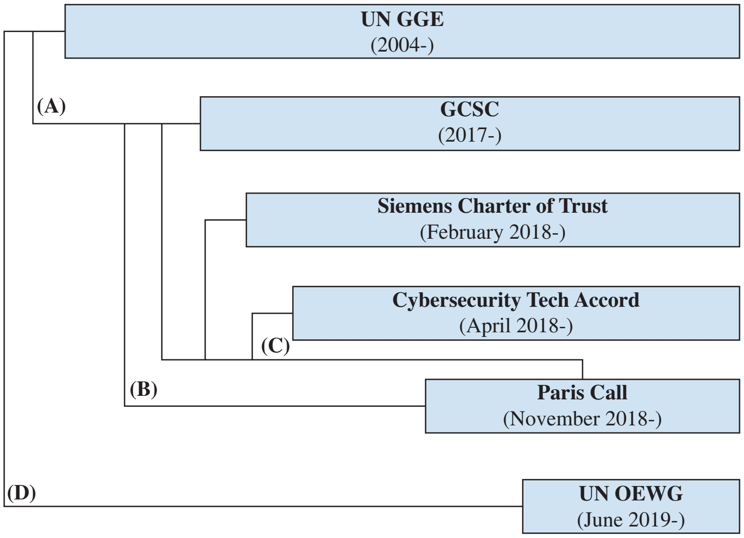
The current fragmentation of the cyber norm ecosystem into various processes may result from different states or stakeholders preferring specific fora that they believe will most align with their interests. This raises the concern of "forum shopping" as well as the potential fragmentation of norm efforts where these processes compete or even conflict in their prescriptions.

For workshop participants, however, fragmentation may be more a feature of cyber norm processes than a bug. Fragmentation may be beneficial in deepening understanding of cyber norms and broadening participation in at least one or more processes. Different processes may be optimized for different kinds of outcomes—in terms of the actors and activities. Norms may be more realistic in some areas than in others, such as peacetime use of cyber capabilities compared with military cyber operations. Having multiple processes can prevent a roadblock in one area from impeding all progress. Taken together, the apparently fragmented processes resemble a "regime complex" for cyber norms, a "loosely coupled set of regimes" as suggested by Joseph Nye, that nonetheless has the potential to function well.[65] Harnessing the benefits of this regime complex, however, requires planned complementarity between processes and creating a race to the top rather than a race to the bottom. Such a race to the top can be achieved both by increasing cross-pollination of processes and by recognizing that different processes serve different purposes.

Cross-pollination is already in evidence across several cyber norm processes, lending credence to the potential for a future race to the top. Various processes have drawn on the norms of other processes, and in some cases have incorporated them into their own projects. As figure 1 illustrates, the norm processes discussed in this paper are intertwined, such that (A) norms from the UN GGE reports were adopted into the Global Commission, (B) norms from both the GGE and Global Commission were adopted into the Paris Call, (C) the Global Commission, the Siemens Charter of Trust, and the Cybersecurity Tech Accord all signed on to the Paris Call, and (D) some norms from the GGE are reflected in the OEWG mandate. More broadly, a class of "cyber norm professionals" connects all these processes, as states, nongovernmental organizations, industry, and civil society have experts who participate in one or more of these processes simultaneously. Together, this web of informal and formal contact connects otherwise disparate processes.

Why favor fragmentation over a hierarchy where some cyber norm process gains authority to trump others? First, fragmentation may be useful because different processes can address different stakeholders. Although multistakeholder efforts may also seek to use broad coalitions to endorse universal behavior expectations, other cyber norm processes may be tailored to relevant communities. Hence, certain cyber norm processes may appropriately focus on creating rules of the road for states while others may emphasize rules of the road for industry.

FIGURE 1
Norm Process Cross-Pollination



Another important distinction for norm proponents is the value of having a "high-ambition coalition" in norm promotion efforts even as others may value processes that enable great powers to have frank discussions over norms. International relations in contexts as diverse as climate change and antipersonnel land mines reveal that certain coalitions of states may generate and diffuse norms of behavior even without great power participation. Thus, the EU was able to rally dozens of countries to sign the Paris Climate Agreement. Indeed, even nonparticipating great power states may modulate their behavior to accommodate these norms, such as the U.S. "policy" to forgo the use of antipersonnel land mines outside the Korean Peninsula.

A third point that helps support fragmentation is the different purposes cyber norms may serve. Workshop participants drew a distinction between broadening the base of participants and deepening understanding of and adherence to existing norms. Some, like the Global Commission and GGE, focus on developing norms and getting concrete agreement on fundamental normative issues. Other processes, like the Paris Call, focus on collecting signatures of like-minded—and, in the case of Huawei, purportedly like-minded—actors that broaden their reach. Notably, these different projects may be linked, if actors take seriously the reputational costs of being outside a cyber norm club.

At present, it appears that high-ambition coalition processes are well suited to the project of broadening, while more exclusive groups are better suited to the project of deepening norms. In the words of one workshop participant, this helps avoid the issue of having too many cooks in the norm kitchen. This also helps explain the failure of the 2017 GGE, where one of the obstacles to consensus emerged from the group's expansion to twenty-five experts. That said, the opposite extreme—too few cooks—may make the product unpalatable to those who were not involved in its creation. Some participants suggested that the United States would have been more likely to join the Paris Call had it been allowed a voice in its formulation.

Although fragmentation may be useful (or at least not a harm) at present and in the short term, the status quo still faces significant challenges. Moreover, process consolidation may be a necessary step if a truly universal set of global cyber norms is to develop, including participation by states in the Global South. These states are often unable to participate in the resource-intensive jet-set diplomacy of the current fragmented processes.

Key Takeaways and Policy Options

The workshop's main message was that process fragmentation may not be detrimental to the formation of cyber norms in the short term, with processes offering opportunities to interact in complementary ways and even achieve force multiplication. At the same time, participants identified several interconnected challenges facing these cyber norm processes.

- **Inherent characteristics of the cyber domain:** The evolving nature of the internet poses challenges for the development of effective norms. First, the domain itself constantly changes, from the underlying physical infrastructure to the networks of actors and institutions that manage it. In addition, low barriers to entry to develop and to use cyber capabilities mean that a large number of actors would need to adhere to norms—enforcement may depend on the actions of states, proxy actors, individual corporations, and others.
- **Lack of transparency about state behavior:** States' cyber activities remain shrouded in secrecy. This obfuscation makes it difficult to identify which cyber norm proposals actually constitute existing cyber norms (that is, they reflect actual shared expectations of appropriate behavior for a particular community of actors, be it states, industry, or others). Moreover, even where evidence supports the existence of a cyber norm, the breadth and depth of conformity within the targeted community is often unclear. Of the norms that have widespread endorsement, some seem to be adhered to (for example, not targeting financial data integrity), while others appear more tenuous (for example, not attacking critical infrastructure).
- **Absence of great power cooperation:** 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.
- **Lack of incentives for internalizing norms:** For states to internalize norms, they must perceive the prospective benefits of adherence (in terms of concrete benefits for adopting or the costs that may follow failure to do so) as outweighing the prospective benefits of remaining outside of normative constraints. The existing balance of incentives poses problems on both sides of this calculus for cyber norms. On the one hand, numerous participants emphasized the lack of incentives for adherence. Only in a few of the most egregious cases have states even called out perceived violations of norms, much less imposed real consequences on perpetrators. On the other hand, states with significant cyber capabilities seem ready and willing to employ them to advance their interests and, in some cases, undermine their adversaries. The perceived utility of cyber tools, particularly for those great powers with the most formidable capabilities, looms large against the hypothetical benefits of cooperating on concrete steps toward implementing norms. For cyber norms to solidify, it may require action

> to shape both sides of the calculus—creating incentives for adherence and addressing the fundamental insecurity of ICTs that makes cyber tools so attractive in the first place.[66]

Four broad recommendations can address these issues:

- Focused research on specific cyber norms to measure their alignment with actual behavior in cyberspace
- A shared global database of cyber processes that can improve transparency on what each process does, who participates, and how its work is received in other processes (that is, what sort of cross-pollination is occurring versus triggering competing or conflicting norm proposals)
- More multistakeholder engagement with great powers on exercising their power responsibly to improve the identification and operation of cyber norms for states and other stakeholder groups (for example, industry, civil society)
- Research efforts to identify a menu of incentives to promote norm adoption and implementation, including a list of potential consequences that can follow cases of nonconformance

More Focused Measurement of Cyber Activity

The aphorism that "to measure is to know" may be applied in cyberspace. Objective, data-driven social science research can help identify which norms already work and where diffusion is needed on others.[67] Do states and other stakeholders operate consistent with the Global Commission's call to protect the public core of the internet? How often do states appear to "conduct or knowingly support" cyber operations that "damage" or "otherwise impair the use" of critical infrastructure contrary to the 2015 GGE norm that purports to prohibit such behavior? Focused research efforts can address such questions.

States can be more proactive in articulating their own practices and understanding of norms, as some have begun to do. However, in general they are protective of the secrecy of their cyber operations, and especially reluctant to reveal their offensive capabilities. This is unlikely to change. Nonetheless, efforts already exist to track such activities.[68] Others may be coming in the near term.[69] Researchers may use these and other resources to distinguish goals from actual norms in cyberspace and, where norms exist, to measure the breadth and depth of conformity among the relevant community.[70]

A Database of Cyber Norm Processes

As noted, there is already an existing field of cyber norm professionals, while cyber norms themselves have become the subject of increasing scholarly attention. States and other stakeholders should devote more attention to the relationship(s) among cyber norm processes. Building a shared global database of cyber processes may improve transparency on the different purposes these processes serve. The Carnegie Endowment for International Peace laid out a possible model for such a database in its interactive Cyber Norms Index, covering bilateral and multilateral accords between 2007 and 2017.[71] The index allows for comparisons of participation in different accords and areas of converging and diverging membership. Expanding and maintaining an up-to-date index would be valuable. It could also reflect how each process's work is received in other processes (that is, what sort of cross-pollination is occurring, or instances triggering competing or conflicting norms).

Major Powers and the Multistakeholder Approach

While fragmentation is acceptable given current conditions, cyber norm processes can—and should—move toward some consolidation in the future. Overlapping functions mean that multiple processes may be inefficient. Thinly stretched personnel and resources might be able to accomplish more with fewer processes (not to mention meetings). Having fewer processes would streamline debate and decrease the costs of participation, lowering thresholds for actors in the Global South to add their voice to conversations that today are often exclusive to those with the time and resources to participate.

A Menu of Incentives for Spreading Cyber Norms

For all the attention to cyber norms, there remains little research or few guides on how to incentivize their adoption and diffusion. There is a need to address both sides of the calculus for internalizing the norms described above. More research is needed to identify (1) ways to make adherence to cyber norms attractive to their targeted community, (2) mechanisms for deterring instances of nonconformity or imposing consequences on those failing to conform, and (3) measures to improve the security and resilience of ICTs to diminish the incentives for malicious activity. In each case these need not be limited to state actions; as one participant noted, standards and best practices for corporations also constitute norms.

States should institutionalize the practice of pointing to cyber norms and applicable international law to socialize their value among interested stakeholders. States should also do more to impose costs on those violating norms (including their proxies), and to follow through with efforts to facilitate and socialize responses to malicious activity. The EU cyber diplomacy tool box is one such promising effort. Both workshop participants and the Global Commission's Final Report emphasize the need to do more to hold norm violators accountable as a way to strengthen the norms themselves.

Conclusion

As the title of the workshop—"Cyberspace and Geopolitics"—implies, norms for appropriate behavior in cyberspace will often mirror the political realities of the international system. Several participants expressed skepticism that much progress could be made in the current geopolitical climate.

There is a need to calibrate expectations for cyber norms. The novel characteristics and complexities of cyberspace create significant hurdles for effective norms. The cyber domain itself represents a relatively new dimension of state activity. While some participants perceived the development of norms to be moving slowly, others suggested cyber norms are emerging rather quickly in comparison with the pace of norms in other historical cases. Absent structural changes in the domain that shift the cost-benefit calculus for malicious cyber activity, cyber norms may yield only modest results.

At the same time, there is room for optimism. As some participants, especially from industry, emphasized, there are opportunities to instantiate norms in computer code. Simply put, technical solutions may exist to advance the adoption or diffusion of certain cyber norms. Doing so may also decrease the vulnerability of crucial systems (for example, election infrastructure) by decreasing the exposure of those systems to cyberspace (for example, through paper ballots).

A third group of participants claimed that no great power would change its behavior in the absence of a major cyber-related shock to the political system—a "cyber Hiroshima" in the words of one participant. Only after such an event clarified the true costs of cyber operations and (perhaps) fostered popular revulsion could cyber norms take hold among actors currently looking to maximize operational flexibility.[72]

In the absence of these developments, there exists an apparently fragmented ecosystem of cyber norm processes. This is not, however, the worst place to be. Having a plethora of multilateral, private, industry, and multistakeholder efforts creates opportunities to both deepen existing normative commitments and broaden their target audience. As one participant suggested, the world may "be flying the plane as it is still being built," but there are ways forward—to measure what norms exist, who conforms to them, and the various processes that promote and distribute such norms along with a catalog of incentives to improve their capacity to have real-world effects on the stability and security of cyberspace.

About the Authors

Christian Ruhl is the program associate for Global Order at Perry World House, the University of Pennsylvania’s hub for global affairs.

Duncan Hollis is a nonresident scholar at the Carnegie Endowment for International Peace and the Laura H. Carnell Professor at Temple Law School. During the fall of 2019, he was in residence as a visiting fellow at Perry World House at the University of Pennsylvania.

Wyatt Hoffman is a senior research analyst with the Nuclear Policy Program and the Cyber Policy Initiative at the Carnegie Endowment for International Peace.

Tim Maurer is co-director of the Cyber Policy Initiative and a senior fellow in Carnegie’s Technology and International Affairs Program.

Notes

[1] The workshop was also funded in part by the Microsoft Corporation. In the interest of full disclosure, it is important to note that one of the authors of this white paper, Duncan Hollis, regularly consults for Microsoft on its "digital peace" agenda. He has contributed to this paper, however, in a personal capacity.

[2] The workshop was held under the Chatham House Rule, which states that "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." "Chatham House Rule," Chatham House, accessed November 4, 2019, https://www.chathamhouse.org/chatham-house-rule. This paper is thus a reflection of the dialogue and the views of the authors on ways forward; its contents should not be attributed to workshop participants individually or collectively.

[3] Jonathan Beer, "'WannaCry' Ransomware Attack Losses Could Reach $4 Billion," CBS News, May 16, 2017. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[4] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 22, 2018, accessed December 19, 2019, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[5] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Executive Office of the President of the United States, 2018), 1, accessed November 13, 2019, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[6] "Number of Records Exposed up 112% in Q3," Risk Based Security, last modified November 12, 2019, accessed November 19, 2019, https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/.

[7] Kim Zetter, "An Unprecedented Look at Stuxnet," *WIRED*, March 11, 2014, accessed November 19, 2019, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; "Russian Hacking and Influence in the U.S. Election," *New York Times*, accessed November 19, 2019, https://www.nytimes.com/news-event/russian-election-hacking; Alexander Campbell and Vickram Singh, "Lessons From the Cyberattack on India's Largest Nuclear Power Plant," *Bulletin of the Atomic Scientists*, November 14, 2019, accessed November 19, 2019, https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/.

[8] See Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 425–479.

[9] UN General Assembly, Resolution 73/266, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/RES/73/266 (December 22, 2018), https://undocs.org/A/RES/73/266.

[10] UN General Assembly, Resolution 73/27, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/73/27 (December 5, 2018), https://undocs.org/A/RES/73/27.

[11] See, for example, "The Charlevoix G7 Summit Communique," Government of Canada, last modified June 9, 2019, accessed December 19, 2019, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-summit-communique-sommet.aspx?lang

=eng (norm against election interference); “Antalya Summit Leader’s Communique,” G20, 2015, accessed December 19, 2019, http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/; Letter dated January 9, 2015, from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, UN Doc. A/69/723, annex (Jan. 9, 2015) (Revised SCO Code of Conduct).

[12] “Global Commission on Internet Governance,” Centre for International Governance Innovation, accessed November 19, 2019, https://www.cigionline.org/activity/global-commission-internet-governance.

[13] “Final Report,” Global Commission on the Stability of Cyberspace, last modified November 2019, accessed November 19, 2019, https://cyberstability.org/report/.

[14] “Tech Accord,” Cybersecurity Tech Accord, accessed November 19, 2019, https://cybertechaccord.org/; “The Charter of Trust Takes a Major Step Forward With Cybersecurity,” SGS, accessed November 19, 2019, https://www.sgs.com/en/news/2019/02/the-charter-of-trust-takes-a-major-step-forward-with-cybersecurity.

[15] “Global Conference on Cyber Space,” Global Forum on Cyber Expertise, accessed November 19, 2019, https://www.thegfce.com/about/gccs; “Internet Governance Forum,” IGF, accessed November 19, 2019, https://www.intgovforum.org/multilingual/.

[16] “NETmundial Initiative,” NETmundial, accessed November 19, 2019, https://netmundial.org/; “The Supporters,” Paris Call, accessed November 19, 2019, https://pariscall.international/en/supporters; “The Christchurch Call,” New Zealand Ministry of Foreign Affairs and Trade, accessed November 19, 2019, https://www.christchurchcall.com/.

[17] The list of 2019–2021 States with GGE members is Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay.

[18] “UN GGE and OEWG,” Geneva Internet Platform Digital Watch, accessed October 27, 2019, https://dig.watch/processes/un-gge.

[19] “OAS Holds Consultations on UN GGE,” Geneva Internet Platform Digital Watch, last modified August 20, 2019, accessed November 19, 2019, https://dig.watch/updates/oas-holds-consultations-un-gge.

[20] “Disarmament and International Security (First Committee),” UN, accessed November 9, 2019, https://www.un.org/en/ga/first/.

[21] Geneva Internet Platform, “UN GGE and OEWG.”

[22] Letter dated September 23, 1998, from the Permanent Representative of the Russian Federation Addressed to the Secretary-General, UN Doc. A/C.1/53/3 (September 30, 1998); Tim Maurer, “Cyber Norm Emergence at the United Nations—an Analysis of the Activities at the UN Regarding Cyber-security,” Belfer Center for Science and International Affairs, Discussion Paper 2011-11, 2011, 17, http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

[23] The six GGEs convened in 2004–2005, 2009–2010, 2012–2013, 2014–2015, 2016–2017, and 2019–2021.

[24] See Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A68/156/Add.1 (September 9, 2013).

[25] See Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 9–15, UN Doc. A/70/174 (July 22, 2015).

[26] Ibid.

[27] "G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015," G20, accessed November 20, 2019, http://www.g20.utoronto.ca/2015/151116-communique.pdf.

[28] Joseph S. Nye, "Normative Restraints on Cyber Conflict," Cyber Security Project, Belfer Center, 2018, 9.

[29] "June 2017 Digital Policy Trends," Geneva Internet Platform Digital Watch, last modified June 2017, accessed November 13, 2019, https://dig.watch/newsletter/june2017#Trends.

[30] Geneva Internet Platform, "UN GGE and OEWG."

[31] A/RES/73/266, section 3. The GGE is also directed to study how international law applies to the use of ICTs by states, with a required report on the results of the study, including an annex containing "national contributions of participating governmental experts on the subject of how international law applies." Ibid.

[32] See, for example, ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, November 18, 2018, https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf; EU Statement–United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security, October 26, 2018, https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-%e2%80%93-united-nations-1st-committee-thematic-discussion-other-siarmament-measures-and_en.

[33] Whether this was a violation of the 2015 GGE norm prohibiting the targeting of critical infrastructure in "peacetime" may depend on whether the situation between Russia and Ukraine in 2015 had risen to the level of an armed conflict (that is, not peacetime). Russian denials of involvement in these cyber attacks, however, have precluded closer analysis of whether its action conformed to the GGE norm.

[34] A/RES/73/27, section 5.

[35] A/RES/73/27, section 5.

[36] Lea Kaspar and Sheetal Kumar, "Cyber Norms in NYC: Take-Aways From the OEWG Meeting and UNIDIR Cyber Stability Conference," Global Partners Digital, last modified June 12, 2019, accessed November 20, 2019, https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/.

[37] Geneva Internet Platform, "UN GGE and OEWG."

[38] Ibid.

[39] "UN GA Resolution on Establishment of OEWG (A/RES/73/27)," Geneva Internet Platform Digital Watch, December 11, 2018, https://dig.watch/instruments/un-ga-resolution-establishment-oewg-ares7327.

[40] Ibid.

[41] "About," Global Commission on the Stability of Cyberspace, accessed November 13, 2019, https://cyberstability.org/about/.

[42] "Commissioners," Global Commission on the Stability of Cyberspace, accessed November 13, 2019, https://cyberstability.org/commissioner/. A third chair, Marina Kaljurand, stepped down into a commissioner role after her election to the EU Parliament in 2019.

[43] Global Commission on the Stability of Cyberspace, "Final Report."

[44] "Global Commission Signs the Paris Call for Trust and Security in Cyberspace," Global Commission on the Stability of Cyberspace, last modified November 16, 2018, accessed November 13, 2019, https://cyberstability.org/news/global-commission-signs-the-paris-call-for-trust-and-security-in-cyberspace/.

[45] Ramesh Thakur, Andrew F. Cooper, and John English, eds., *International Commissions and the Power of Ideas* (New York: United Nations University Press, 2005), x, accessed November 20, 2019, https://collections.unu.edu/eserv/UNU:2456/pdf928081110X.pdf.

[46] CIGI, "Global Commission on Internet Governance," accessed November 20, 2019, https://www.cigionline.org/initiatives/global-commission-internet-governance.

[47] "Minister Koenders Launches International Cyberspace Commission," Government of the Netherlands, last modified February 18, 2017, accessed November 20, 2019, https://www.government.nl/latest/news/2017/02/18/minister-koenders-launches-international-cyberspace-commission.

[48] "Global Commission on the Stability of Cyberspace," EastWest Institute, accessed November 13, 2019, https://www.eastwest.ngo/in-focus/global-commission-stability-cyberspace.

[49] Global Commission on the Stability of Cyberspace, *Norms Through Singapore*, November 2018, https://cyberstability.org/wp-content/uploads/2019/04/singaporenew-digital.pdf.

[50] "Paris Call for Trust and Security in Cyberspace," Paris Call, accessed November 20, 2019, https://pariscall.international/en/.

[51] "The 9 Principles," Paris Call, accessed November 20, 2019, https://pariscall.international/en/principles.

[52] "The Supporters," Paris Call, accessed November 19, 2019, https://pariscall.international/en/supporters.

[53] Arthur P. B. Laudrain, "Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace," Lawfare, last modified December 4, 2018, accessed November 13, 2019, https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace.

[54] John Frank, "Paris Call: Growing Consensus on Cyberspace," Microsoft (blog), last modified November 12, 2019, accessed November 20, 2019, https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

[55] Brad Smith, "The Need for a Digital Geneva Convention," Microsoft (blog), last modified February 14, 2017, accessed November 20, 2019, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[56] "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," France Diplomatie, accessed November 13, 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[57] "Huawei Joins Paris Call for Trust, Security in Cyberspace," Huawei, accessed November 5, 2019, https://www.huawei.com/us/press-events/news/2019/7/huawei-joins-paris-call.

[58] "Siemens Charter of Trust," Siemens, last modified April 4, 2019, accessed November 13, 2019, https://press.siemens.com/global/en/feature/charter-trust-takes-major-step-forward-advance-cybersecurity.

[59] "Charter of Trust at a Glance," Siemens, accessed November 20, 2019, https://assets.new.siemens.com/siemens/assets/api/uuid:9bbe02e9-fcb2-4948-9977-a668cac52e50/version:1567432347/charter-of-trust-presentation-en-20190902-website.pdf.

[60] "About the Cybersecurity Tech Accord," Cybersecurity Tech Accord, accessed November 13, 2019, https://cybertechaccord.org/about/.

[61] Ibid.

[62] France Diplomatie, "Cybersecurity."

[63] "Joint Statement on Advancing Responsible State Behavior in Cyberspace," U.S. Department of State, last modified September 23, 2019, accessed November 13, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[64] Ibid.

[65] Joseph Nye, *The Regime Complex for Managing Global Cyber Activities* (Waterloo, ON: Global Commission on Internet Governance, 2014).

[66] George Perkovich and Wyatt Hoffman, "From Cyber Swords to Plowshares," in *Think Peace: Essays for an Age of Disorder*, ed. Thomas de Waal (Carnegie Endowment for International Peace, 2019), https://carnegieendowment.org/2019/10/14/from-cyber-swords-to-plowshares-pub-80035.

[67] Notably, this sentiment of information sharing was one of the Global Commission's Final Report's six recommendations: that "state and non-state actors collect, share, review, and publish information on norms violations and the impact of such activities." Global Commission on the Stability of Cyberspace, "Final Report."

[68] See, for example, "Cyber Operations Tracker," Council on Foreign Relations, accessed December 19, 2019, https://www.cfr.org/interactive/cyber-operations; see also "Significant Cyber Incidents," Center for Strategic and International Studies, accessed December 19, 2019, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

[69] Among its functions, for example, the new CyberPeace Institute will engage in accountability activities that facilitate "the collective analysis of sophisticated cyberattacks and investigation of the harm they cause" as well as advancement activities that identify and address "potential normative or legal gaps." See the CyberPeace Institute homepage, accessed November 20, 2019, https://cyberpeaceinstitute.org/.

[70] Paul Rosenzweig, "Resources for Measuring Cybersecurity," Lawfare, last modified October 31, 2019, accessed November 13, 2019, https://www.lawfareblog.com/resources-measuring-cybersecurity.

[71] Carnegie Endowment for International Peace, "Cyber Norms Index," accessed November 20, 2019, https://carnegieendowment.org/publications/interactive/cybernorms.

[72] Nye, "Normative Restraints on Cyber Conflict," 17.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org