G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Policy Paper

September 2019 | No.23

SHAPING INCLUSIVE GOVERNANCE IN CYBERSPACE

BRUNO LÉTÉ

Please direct inquiries to:

The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

The views expressed in GMF publications and commentary are the views of the authors alone.

Cover photo credit: Drop of Light (Shutterstock)

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

About the Author(s)

Bruno Lété is a senior fellow at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international security and defense policy. His research focuses primarily on the EU Common Security and Defense Policy, NATO affairs, developments in Central and Eastern Europe, and cybersecurity.

This publication is the product of a partnership between The German Marshall Fund of the United States and Microsoft.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Microsoft

Executive Summary

The United Nations remains the best platform to shape global norms on state behavior in cyberspace. But, despite its achievements, the UN's intergovernmental process struggles to make progress, not least because of deep divisions within the international community about which rules should apply in cyberspace. There is a need to reevaluate cyber governance efforts and to think of new practices that adopt a multi-stakeholder model, instead of relying solely on the current rigid intergovernmental approach. There may be renewed energy for such discussion now that the UN's First Committee has endorsed two parallel processes on cyber norms—the Open-Ended Working Group (OEWG) and a sixth round of the UN Group of Governmental Experts (UNGGE).

Other international organizations have already successfully institutionalized multi-stakeholder models involving NGOs or business in their policymaking processes. Their best practices and lessons learned for stakeholder input could be adapted and used at the UN level. This paper looks at the experience of several intergovernmental organizations active in various non-cyber domains, including the Arctic Council, the European Union, the International Atomic Energy Agency, the North Atlantic Treaty Organization, the Organization for Economic Cooperation and Development, the Organization for the Prohibition of Chemical Weapons, the Organization for Security and Cooperation in Europe, and the World Health Organization. They vary widely in form and function, and they are not comparable to the UN. Nonetheless, studying them identifies the following types of multi-stakeholder inclusion:

- stakeholders as opinion-shapers,
- stakeholders as problem-solvers,
- stakeholder selection and trust-building,
- a role for stakeholder associations in decision-making,
- multi-stakeholder engagement at the national level, and
- stakeholders as whistleblowers.

Based on these findings, this paper makes six recommendations on how to include non-governmental stakeholders in the UNGGE and OEWG process so as to make progress toward an open cyber governance model.

Include external subject matter expertise in OEWG and UNGGE discussions

The OEWG can organize a regular briefing platform for external experts, but first it will need to state which stakeholders it plans to engage with. The UNGGE members and chair are already exploring how to engage with stakeholders in informal ways, but a structured, strategic approach is still missing. The UNGGE and OEWG could also task their secretariats to produce ad hoc food-for-thought papers that summarize external debates on a specific topic.

Create an engagement framework to preselect stakeholders and introduce observers to the OEWG

The OEWG can introduce criteria that stakeholders must meet in order to engage with or become observers to the group. Such a framework will introduce transparency toward stakeholders. It can also help the OEWG to narrow down the number of stakeholders it engages with and ensure that these are credible.

Convene like-minded stakeholders into larger interest groups

Groups or associations of stakeholders seeking a common purpose carry more weight to influence policy. They are also easier for intergovernmental organizations to interact with since they aggregate many different views into one voice. Such interest groups might include like-minded business actors or NGOs.

Organize independent events that gather UNGGE member states and stakeholders

Each member state of the UNGGE can hold informal consultations with local non-state actors in their own capital. More roundtable discussions, or a major annual event, can be organized independently from the UN context, and could support the UNGGE's regional consultation process.

Develop an 'Aarhus Convention for cyberspace'

Cyberspace needs a multilateral agreement, similar to the UN Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (also known as the Aarhus Convention'), through which opportunities for non-state actors to access information are increased and reliable regulation procedures are secured. The OEWG and UNGGE could use such an initiative to engage outside actors who have valuable expertise to offer.

Engage the UN through multi-stakeholder dialogue in national and regional platforms

Other international platforms, beyond the UN, often gather diverse key players, and have more experience working with external stakeholders. Ideas developed inside such platforms, such as the OECD, the OSCE, or the EU, could then be more easily transferred to an institution like the UN. Such diplomatic sequencing creates options for stakeholders to be heard at the global level too.

Shaping Inclusive Governance in Cyberspace

BRUNO LÉTÉ

The United Nations remains the most important platform for shaping global norms on state behavior in cyber space. Serious efforts have been underway since 2004 with the creation of a Group of Governmental Experts (UNGGE). But as the world grows divided over what kind of cyber rules should apply, finding consensus through intergovernmental negotiations becomes increasingly difficult. A more diverse, multi-stakeholder model—that is, one that includes non-governmental actors—may have more potential to bridge the growing gap between some countries' approaches to cyber.[1] With the UN's First Committee having endorsed in December 2018 two parallel processes on cyber norms, a sixth round of the UNGGE and a new Open-Ended Working Group (OEWG), there is a good opportunity to think how to move toward a multi-stakeholder model instead of relying solely on the current rigid intergovernmental approach.

This paper therefore studies a relevant sample of intergovernmental organizations in non-cyber domains to that end. These were chosen specifically for their ability to include the voices of multiple actors (for example, non-governmental organizations, universities, businesses) in their decision-making processes. The organizations surveyed are the Arctic Council, the European Union, the International Atomic Energy Agency (IAEA), the North Atlantic Treaty Organization (NATO), the Organization for Economic Cooperation and Development (OECD), the Organization for the Prohibition of Chemical Weapons (OPCW), the Organization for Security and Cooperation in Europe (OSCE), and the World Health Organization (WHO). Based on interviews with representatives of these organizations and on research, the paper explores how their experiences and models can be applied to ongoing international efforts to shape state behavior in cyberspace.

The first part of the paper describes how the international community has attempted to shape responsible state behavior in cyber space and points at the limitations of the intergovernmental approach. The second part takes a closer look at the surveyed international organizations and describes their best practices and lessons learned for multi-stakeholder input. It identifies clear patterns of multi-stakeholder engagement, such as external stakeholders as opinion-shapers, problem-solvers or whistle-blowers. The third part of the paper makes recommendations as to how to implement these best practices at the level of the UNGGE and OEWG. It calls for measures to be taken that would allow external stakeholders to share expertise, to become observers of the decision-making process, to have better access to information, and to convene more regularly with the governmental experts outside the UN context.

Recognizing the Problem

Over the past two decades, rapid advances in computers, software, communications, and sensing technologies have connected billions of individuals across the globe, integrated economies through connected supply chains, and spurred new efficiencies through the Internet of Things. All

[1] The importance of multi-stakeholder models was noted in Bruno Lété and Peter Chase, "Shaping Responsible State Behavior in Cyberspace", German Marshall Fund of the United States, May 2018.

the while, this has stimulated the development of additional new technologies and ways of doing things that have brought great advances in health, education, agricultural production, economic growth, and general human welfare.

These advances, however, also bring challenges, including the now nearly absolute dependence of all developed and many developing countries on the integrity of digital networks and systems. Despite the general resilience of network-based systems, deep digital integration has also created vulnerabilities to cyberattacks by individual hackers, organized crime, terrorist groups, and even states.

> “ Only a relatively small body of specialized law applies to cyberspace.

Rogue governments intending harm are perhaps the greatest threat. Experts from the public and private sectors work continuously to mitigate the risks of cyberattacks, but they are continuously tested by governments that can bring immense financial, technical, and military resources to developing new cyber tools for exploiting the product or human vulnerabilities that are inevitable in any complex system. An attack by one state seeking to bring down the financial, energy, or other systems of another could provoke untold economic damage and potentially extensive loss of civilian life.

Such attacks are all too real. Starting with Russia's denial-of-service attacks on Estonia's government and financial system in 2007, they have become more numerous and more destructive. For example, the WannaCry ransomware attack in 2017 affected hundreds of thousands of computers in 150 countries. The NotPetya attack that same year, which the United States publicly attributed to Russia, was deemed by the White House to be the costliest cyberattack in history. By one estimate, the world experienced 13 significant cyber incidents in the first quarter of 2019.[2]

Seeking Global Solutions

Following the two world wars of the last century, governments developed a framework of international law and organizations to try to avoid war, and to constrain the ability of governments to use violence. While experience over the past seven decades has demonstrated that the instruments of international law do not stop governments, not even from genocide, these international legal frameworks still set necessary standards against which actions by governments can be judged, condemned, and eventually sanctioned by the international community.

There are many mechanisms aiming to prevent irresponsible state behavior in traditional domains such as nuclear, chemical, and biological warfare so as to sustain global peace and security. This is much to the credit of international organizations such as the IAEA, the OPCW, and the WHO, which have developed a sophisticated cooperation with governments, civil society, and businesses allowing them to create legal conditions for verification and attribution. But such cooperation and legal conditions to stop governments from engaging in malicious cyber activities are still limited. Only a relatively small body of specialized law applies to cyberspace, including in particular the 2004 Budapest Convention on Cyber Crime and the regulations adopted by the International Telecommunications Union.[3] The *Tallinn Manual* and *Tallinn Manual 2.0*, published by the NATO Cooperative Cyber Defence Centre of Excellence, attempt to close this legal gap by reviewing a wide range of treaties, court judgments, and state practices, and by exploring the application of

[2] “Significant Cyber Incidents Since 2006”, Center for Strategic and International Studies, May 2019

[3] Anthony Rutkowski, “The Digital Geneva Convention Exists, Just Use It” CircleID, December 16, 2017.

international law in cyber warfare. The manuals are helpful, but they are not a substitute for regulations, orders, treaties, or similar legal instruments.

The most significant platform to shape the application of legal frameworks in cyberspace remains the United Nations. The General Assembly's First Committee, which deals with disarmament and international security, has considered cybersecurity-related issues since 1998 when Russia first introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security". The First Committee broadly addressed cybersecurity by considering norms, rules, and principles of responsible behavior of states in cyberspace. In 2004 it also set up the UNGGE to look more deeply into these issues.

Since its inception the UNGGE has held five sessions and has put forward various global norms and standards aiming to contribute to peace and stability in cyberspace. The third session in 2013 agreed, for instance, that international law and the UN Charter are applicable to state behavior in cyberspace, and that the rights and obligations that flow from the concept of sovereignty apply in that case too. Critically, it also found that "states must meet their international obligations regarding internationally wrongful acts originating from their territory."[4] More significantly, the fourth UNGGE report in 2015, which was endorsed by the General Assembly, reaffirmed the application of international law to cyberspace and also recognized the right of states to "take measures consistent with international law," implicitly recognizing the right to take countermeasures in response to a cyberattack.[5]

As concerns about cybersecurity have skyrocketed, the urgency and tensions over this topic have also grown. In 2017, discussions in the UN First Committee broke down. The fifth UNGGE session was not able to produce a consensus report as Cuba, fronting for countries such as China and Russia, argued against the previously acknowledged right to take countermeasures in self-defense and against the application of international humanitarian law to cyber warfare.[6]

Limitations of Intergovernmentalism

With the UNGGE in deadlock, negotiations on further steps became even more divisive. But in November 2018, in a surprising turn of events, the UN First Committee approved proposals for the creation of two working groups aiming at developing rules for states regarding responsible behavior in cyberspace. The Russian-led Resolution 73/27 established an open-ended working group (OEWG) accessible to the entire UN membership and tasked with submitting a report on the results of its study to the General Assembly at the end of 2020. The U.S.-led Resolution 73/266 established a sixth session of the UNGGE and will lead to the convening of a group of 25 countries tasked with reporting their conclusions to the General Assembly at the end of 2021.[7]

While both resolutions recognize the conclusions of the 2013 and 2015 UNGGE reports, they also reflect a recurrent divergence in visions of state behavior in cyberspace. Some states advocate the protection of fundamental freedoms in cyberspace and the use of legal instruments in response to cyber threats, as reflected by the U.S.-led resolution. Others are more concerned about their capacity to control ICT infrastructures and to regulate activities within their domestic online environments, as reflected by the Russian-led resolution.[8] Considering the

[4] The Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, June 24, 2013.

[5] The Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, July 22, 2015.

[6] Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance International Norms," Just Security, June 30, 2017

[7] UN Press Release: "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct", United Nations, 8 November 2018

[8] Samuele De Tomas Colatin, "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace", NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

proliferation of processes for debating cyber policy issues, the addition of new work streams within the UN will only challenge the capacity of countries to simultaneously engage in these discussions and will split the UN's attention and coherence on this issue. Moreover, the UNGGE and the OEWG are meant to work on a consensual basis but the volatile relations on cybersecurity between major powers such as China, the European Union, Russia, and the United States mean that finding compromise and achieve consensus through an intergovernmental process very much remains an open question. There is therefore a need to re-evaluate cyber-governance efforts and to think of new practices that also adopt a multi-stakeholder model, instead of relying solely on the current intergovernmental approach. Other stakeholders can help bridge the gap.

Multi-stakeholder Approaches in Intergovernmental Processes

Cyberspace and state behavior associated with it constitute a complex and interdisciplinary area. It demands approaches to policy development that are inclusive, expertise-driven, and engage a broad range of stakeholders. This need was recognized by the UNGGE in 2013.[9] Nevertheless, multi-stakeholder approaches inside the UN's policymaking regarding the cyber domain exist but are still rare. But now that the UN First Committee has endorsed two parallel processes on cyber norms, there may be new energy for discussing what states should and should not do in cyberspace. While these discussions acknowledge the importance of stakeholder engagement—for instance, the UNGGE's intention to hold regional consultations—there are still considerable questions how to make this happen.

Some international organizations have already successfully institutionalized multi-stakeholder models in their policymaking processes.[10] Their best practices and lessons learned can be transposed to the UN level. Several existing models of multi-stakeholder engagement within intergovernmental organizations are looked at below.

Stakeholders as Opinion Shapers

Inviting non-governmental stakeholders to share their expertise in formal or informal settings is becoming the norm in intergovernmental processes.

The IAEA has open-ended working groups that work with its secretariat to produce non-papers that often serve as the base for policymaking. The secretariat in many cases will actively engage with external stakeholders to infuse these non-papers with new insights and ideas.

The OSCE secretariat feeds member states with topical "food-for-thought" papers that are based on external literature, opinions, debates, and analysis. These papers are produced at the request of member states or when the secretariat perceives a need.

The Arctic Council chairmanship holds informal breakfast meetings with non-governmental observers to collect their thoughts and concerns on the organization's activities and agenda setting. A similar tradition exists with countries holding the presidency of the Council of the European Union, with practitioners and experts regularly invited to advise the presidency on pressing policy priorities.

NATO has created a culture in which external experts are regularly asked to brief its North Atlantic Council on current issues. These briefings most often result from interactions between external stakeholders and the NATO secretariat or member states.

Clearly, intergovernmental organizations increasingly value formal or informal consultations, but the process is most successful when it is driven

[9] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", Report A/68/98, United Nations, June 24, 2013

[10] Organizations such as the IAEA or the WHO have adopted stakeholder engagement strategies which are being discussed in this paper

by a member state, the secretariat, or the chair. It is therefore equally important for multi-stakeholders to actively engage with these different entities if they desire to shape opinions inside the organizations.

Stakeholders as Problem-solvers

Multi-stakeholder engagement sometimes helps address a specific problem, usually because the intergovernmental institution does not possess the necessary in-house expertise. For this purpose, experts from civil society or business can be included in formal advisory boards or technical working groups together with governmental experts.

The WHO has established technical activities with external stakeholders that fall within its General Program of Work, including product development, capacity-building, operational collaboration in emergencies, and contributions to the implementation of WHO policies.

> “Multi-stakeholder engagement sometimes helps address a specific problem, usually because the intergovernmental institution does not possess the necessary in-house expertise.

The OPCW has a Scientific Advisory Board of 25 private-sector and academic experts who serve in a personal capacity and enable the director-general to advise on specialist issues such as chemical-making processes or on quotas for by-products that can become precursors of chemical weapons.

IAEA intergovernmental working groups that develop important safety standards or security guidelines can include external experts in their work. The working groups, on highly specialized topics such as nuclear-waste management or nuclear-transport safety, independently invite the external stakeholders they wish to talk to.

The European Union, the OSCE, and the OECD all have created issue-specific working groups or task forces that that include external experts to generate policy recommendations. This approach enables the intergovernmental process to secure expert information or advice from external sources having special competence in different fields.

Stakeholder Selection and Trust-building

Intergovernmental organizations are increasingly concerned about who they engage with and how. In many cases non-governmental stakeholders are asked to join an engagement framework or go through a pre-screening. Such frameworks usually involve criteria a stakeholder must meet to be allowed to interact with the institution.

The WHO and the IAEA have similar framework procedures. The WHO, where a culture of intergovernmentalism has long existed, established in 2016 a Framework on Engagement with Non-State Actors to foster cooperation between multi-stakeholders and the secretariat. This has established a transparent process in which stakeholders can apply to the WHO Executive Board for admission. Once the application is reviewed and accepted stakeholders can be included into issue-specific working groups and receive the right to participate and make statements in sessions of the WHO’s governing bodies. The IAEA’s “Rules on the Consultative Status of Non-Governmental Organizations with the Agency” are comparable. Stakeholders wishing to obtain consultative status must submit their application to the director general who refers it to the Board of Governors. Consultative status includes a variety of privileges, including access to the IAEA General Conference.

The OSCE Secretariat, for its part, began the process of developing an internal framework to advise its departments on how to partner with third parties, such as the private sector, and to see how these actors can help the organization think through policy issues and identify deliverables.

Introducing such systems offers several benefits. It offers the intergovernmental organization guarantees that it can identify and trust the stakeholders it engages with. For the stakeholder it offers transparent ways to enter into official relations with the organization.

A Role for Stakeholder Associations in Decision-making

There is a clear trend that access to the decision-making process of intergovernmental organizations is most often granted to sectorial or topical associations of stakeholders. In some cases, intergovernmental organizations give these associations a formal status. This can include advising on draft resolutions, making statements at ministerial meetings, being part of working groups, being granted full observer status, and proposing projects through a member state.

IAEA member states can include NGO and business representatives in their delegations attending the General Conference, and the IAEA Board of Governors also grants access to a small number of NGOs to observe the General Conference.

The experience of the NATO Industrial Advisory Group (NIAG) shows that stakeholders can contribute to an intergovernmental process on sensitive issues like national security. The NIAG can bring direct business advice to the Conference of National Armaments Directors, a senior NATO committee for defense-procurement officials that reports to the North Atlantic Council. As such NATO fosters through NIAG government-to-industry and industry-to-industry armaments cooperation within the alliance.

Another example is Business at OECD (BIAC), a private industry network that, through topical policy groups, builds consensus among industry views and injects private-sector insights into the OECD's policy instruments. BIAC is invited to comment on draft resolutions or white papers, can make a statement at the Annual Ministerial Meeting, and has year-round access to various consultations and working groups. BIAC thus directly interacts with and influences decision-making processes in the OECD.

> “ *Non-governmental stakeholders engage directly with national governments most often when there is a lack of engagement channels at the intergovernmental level.*

The Arctic Council has gone further and has granted 12 stakeholder associations full observer status. Ranging from the Association of World Reindeer Herders to the International Work Group for Indigenous Affairs, they are invited to attend meetings and can make statements during these, develop relevant ideas through working groups, and can actively propose projects through a member state.

Associations bringing together stakeholders to act with a common purpose, to solve concrete problems, and to develop norms on a consensus basis can thus act as “shadow structures” to the intergovernmental organizations. Moreover, from the organizations' perspective such groups carry more weight when it comes to influencing policymaking and are easier to interact with since they aggregate many different views into one voice.

Multi-stakeholder Engagement at the National Level

Non-governmental stakeholders engage directly with national governments most often when there is a lack of engagement channels at the intergovernmental level. Individual governments, in this case, are seen by stakeholders as a potential champion or sponsor of their agendas. Engagement between them can be formal or informal at the level of member states' permanent delegations to the intergovernmental organization. Stakeholders can also engage with decision-makers in the member state's capital. In both cases, engagement can include private conversations, informal roundtable discussions, or public events to raise awareness.

Governments can also use stakeholder engagement to promote at the intergovernmental level topics of national interest. Especially in those organizations with a more advanced open-governance culture, including the European Union, the OECD, and NATO, permanent delegations regularly engage and develop partnerships with preferred NGOs or businesses. The aim is not only for these stakeholders to provide expertise on issues the member state cares about, but also to generate visibility for these issues for other member states and the organization itself. Their efforts can take the shape of briefings, publications, or informal and public events.

Inside international organizations that embrace open-governance principles, the practice of member state-stakeholder dialogue is widely accepted and often transparent. In those where open governance is still limited, this practice remains more sensitive and often informal in nature. In both cases, however, "national lobbying" remains an unavoidable factor and it is rare that stakeholder will rely only on institutional channels.

Stakeholders as Whistleblowers

Intergovernmental organizations sometimes rely on non-governmental stakeholders to expose developments, violations, crises, or conflicts that their member states are reluctant to report.

The chemical industries in OPWC member states must report on their activities, but other member states can contest these declarations and submit a request to the director-general to verify suspicious plants or to mandate the director-general to coordinate with the UN if the alleged violation involves a non-member state. Member states sometimes rely on external stakeholders—that do not have a mandate to submit verification requests to the OPWC—to gather evidence or expose violations. For instance, in response to persistent allegations by civil society of government forces using chemical weapons in the war in Syria, the OPCW fact-finding mission was set up in 2014 with an ongoing mandate to establish facts surrounding allegations of the use of toxic chemicals for military purposes in the country. The mission is required to study available information relating to allegations of use of chemical weapons, including information provided by the government and other stakeholders.

> *" Inside international organizations that embrace open-governance principles, the practice of member state-stakeholder dialogue is widely accepted and often transparent.*

Similar verification and safeguard mechanisms exist at the IAEA, which transformed nuclear energy into one of the most transparent sectors in the world. The IAEA conducts ad hoc, routine, or special inspections of nuclear facilities of member states where safeguards apply. In a speech in April, Director-General Yukiya Amano recognized that "third party information related to undeclared nuclear material or activity can play an important role in identifying issues that the IAEA may need to address." He added that "the use of third-party information has enabled the Agency to take follow-up actions with several countries to address issues related to the correctness and completeness of their declarations".[11]

[11] Yukiya Amano, "Challenges in Nuclear Verification", Speech given at the Center for Strategic and International Studies, April 5, 2019

The WHO works regularly with external stakeholders to deal with medical emergencies. During the 2014–2016 Ebola outbreak in West Africa, it relied partly on informal information provided by NGOs and the private sector to identify infected communities, mainly because some governments in the region maintained weak surveillance systems or were reluctant to report an outbreak[12] out of fear of economic consequences (even though early information-sharing may have prevented the disease from spreading as fast).

External forensics or stakeholder intelligence are valuable to intergovernmental institutions, but too often these lack the official mandate to engage with such information. The situation is improving, but in many cases non-governmental stakeholders still rely on member states to push the matter forward inside the institutions.

Toward Open Global Cyber Governance

Multi-stakeholder models are often seen as a single solution, but they should be considered as a set of evolving and changing tools. The following recommendations are based on the best practices and lessons learned discussed above. They suggest how a multi-stakeholder model could be put in practice at the UNGGE and OEWG.

Include External Subject Matter Expertise in OEWG and UNGGE Discussions

Skewed discussions on state behavior in cyberspace can be avoided by ensuring that perspectives that are not shaped by geopolitical or national security concerns are heard. The 73rd session of the UN First Committee provided opportunities to do so. The OEWG has a clear mandate to hold consultative meetings between sessions with industry, non-governmental organizations, and academia.[13] The UNGGE has a mandate to hold consultations with regional organizations, including the African Union, the European Union, the Organization of American States, the OSCE, and the Regional Forum of the Association of Southeast Asian Nations.[14] The Office for Disarmament Affairs provides secretariat support to the OEWG and the UNGGE in this regard. The chairmanship of the UNGGE plays an equally important role by coordinating with the UN General Assembly. This type of structure meshes well with the multi-stakeholder models seen in other intergovernmental bodies.

The OEWG planning session last June reiterated the group's intention to engage externally. At its next planning session, in September, it could adopt multi-stakeholder best practices, such as regular invitations to external stakeholders to brief the OEWG on specific issues. To realize this, it will also need to state which stakeholders it wants to engage with. Moreover, the fact that the UNGGE has no official mandate to engage with non-governmental stakeholders should not stop its members or the chair from doing so. Small steps in this direction are already being taken. For example, the UNGGE chairman attended a roundtable discussion with experts on the sidelines of EU-UNGGE consultation in Brussels in June.[15] Yet, a structured, strategic approach to involve external stakeholders in the UNGGE is still missing. Overall, the OEWG and UNGGE still need to think of transparent and systematic methods to give these a voice.

Moreover, members of the OEWG or UNGGE could task the Office of Disarmament Affairs to produce intelligence and work with external experts on topics where this is needed. The OSCE secretariat's practice of circulating "food-for-thought papers" to member states could serve as a good model. Assuming that neither the OEWG or the UNGGE will want to lag behind in terms of new ideas and breakthrough decisions, both should favor active cooperation with external actors. For non-governmental stakeholders this would mean more opportunities to be listened to by both bodies.

[12] Similar motives sometimes govern state behavior in cyberspace, hiding cyberattacks or malware infections.

[13] "UNGA Resolution A/Res/73/27", United Nations, December 5, 2018

[14] "UNGA Resolution A/Res/73/266", United Nations, December 22, 2018

[15] "EU-UNGGE Regional Consolations - Meeting with Research Community and Civil society Representatives", Brussels. June 20, 2019

Create an Engagement Framework to Preselect Stakeholders and Introduce Observers to the OEWG

While the UNGGE has already clearly defined which external actors it wishes to engage with, the situation is less clear for the OEWG, which has been given a mandate to interact with many different stakeholders. The risk is that the OEWG's engagement is inefficient and not sufficiently focused on policy priorities, and that it involves stakeholders that are less relevant. To avoid this, the OEWG can introduce criteria that stakeholders must meet in order to engage with the group. Some of the guidelines described in the WHO's Framework of Engagement with Non-State Actors could serve as initial example to create a sustainable engagement model.

Such a framework would introduce clear rules and transparency for stakeholders on how to engage with the OEWG, and touch on stakeholders' accountability and integrity, the benefits to cyber norms, or the need to avoid conflicts of interest. It would help limit the number of stakeholders the OEWG engages with and ensure that they are credible. Once a stakeholder has been accredited it is also important that the OEWG leverages its fullest potential; for instance, by extending invitations to attend public meetings, to give briefings or statements, to assist in the development of relevant ideas, or to propose policy projects. Further criteria could be introduced to allow certain stakeholders to become full observers of the OEWG. If the group succeeds in institutionalizing such a multi-stakeholder model it would also clearly serve the purpose of the UNGGE, which could follow these debates and infuse its own process with external ideas and opinions.

Convene Like-Minded Stakeholders into Larger Interest Groups

Groups or associations of stakeholders carry more weight to influence policy and are easier for intergovernmental organizations to interact with since they aggregate many different views into one voice. In global cyber governance, non-governmental stakeholders have a long tradition of interacting with the UN, but their approach is often diffuse and incoherent. Forming or using existing groups or associations could make their interaction with the UNGGE or the OEWG more efficient. These could then function in the same way that BIAC does inside the OECD or NIAG inside NATO. They also could be recognized, for instance, by establishing distinct communities for the private sector, academia, and civil society. Where such communities already exist, they need to be empowered to assist the UNGGE and the OEWG in their objectives. For the private sector one such stakeholder group could emerge based on the Cybersecurity Tech Accord[16] because the signatories include many of the global technology companies. The Paris Call for Trust and Security in Cyberspace[17] could offer another basis for like-minded stakeholders from business or civil society to come together.

> *"While the UNGGE has already clearly defined which external actors it wishes to engage with, the situation is less clear for the OEWG.*

Stakeholder associations and groups have already demonstrated their ability inside intergovernmental processes to focus goals, propose solutions, build consensus, and keep negotiations on track. In its secretariat capacity for the UNGGE and OEWG, the UN Office for Disarmament Affairs could coordinate with the both to open them up to such an approach.

[16] For more information, see Tech Accord.

[17] For more information, see "Paris Call for Trust and Security in Cyberspace", November 12, 2018.

Organize Independent Events that Gather UNGGE Member States and Stakeholders

Given the absence of a mandate for the UNGGE to engage with a broader set of stakeholders, members of the group need to think creatively about how to stay up-to-date with ideas and debates emerging from the private sector and civil society. Nothing prevents UNGGE members, for example, from holding consultations in their capitals with a variety of external stakeholders. Such initiatives already exist but a systematic approach is still missing. More frequent private meetings, roundtable discussions, or public events can easily be organized independently from the UN context. Such efforts would support the UNGGE's regional consultation process and infuse the group with regular ideas from business, academia, and NGOs on specific policy issues. It would also be an opportunity for members to inform stakeholders about the UNGGE, gain support for policies, and make the process more transparent.

All the intergovernmental organizations looked at for this study have endorsed small to large multi-stakeholder events as a tool to enrich their process, from the OECD's Annual Forum to the IAEA Nuclear Energy Innovation Global Forum to the regular NATO Engages conferences. With the Internet Global Forum (IGF) the UN created a venue to convene stakeholders to discuss the future of global cyber governance. Since its inception in 2006 the IGF has developed into a leading global platform to discuss public-policy issues related to key elements of Internet governance. But the IGF also has some shortfalls. It is heavily dependent upon the office of the United Nations secretary-general, which appoints its management in an opaque, top-down process. The wide variety of topics on the agenda makes it also harder to unite stakeholders around a shared interest. Moreover, the IGF rarely transforms the output of its discussions into policy recommendations. While the inclusive model of the IGF deserves to be sustained, another more focused platform would also benefit the global cyber governance discussion.

> “ *Members of the UNGGE need to think creatively about how to stay up-to-date with ideas and debates emerging from the private sector and civil society.*

It is therefore worth exploring if an independent NGO could create a larger annual event that brings together the 25 members of the UNGGE with a representative group of stakeholders for informal and interactive policy debates. Most important would be to use the outcome of such discussions and to publish actionable recommendations for the UNGGE's work program. Such a Track II diplomacy initiative offers an appealing option to convene the UNGGE and key stakeholders in a neutral environment, to manage disagreements, and to explore solutions without the requirements of formal negotiation.

Develop an 'Aarhus Convention for Cyberspace'

A root cause of insecurity in cyberspace is the widespread reluctance of governments to disclose their threat intelligence or technical information on cyber incidents, or to make available their information on the attribution of cyber incidents. This prevents the development of shared situational awareness or cyber-threat assessments among governments, and it paralyzes multi-stakeholder input for good cyberspace governance. However, mechanisms to increase transparency and information access on contentious policy issues have been developed in the past and could serve as a model for cyberspace.

The principles enshrined in the UN Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (also known as the Aarhus Convention) offer a good base to accomplish this.[18] The convention has substantially increased opportunities for citizens to access environmental information, and it has secured transparent and reliable regulation procedures. It has also enhanced an environmental governance network, introduced a relationship between civil society and governments, demonstrated the value of public participation in the decision-making process, and most importantly it has improved access to justice. The Aarhus Convention can be credited with leading a shift toward an environmentally responsible society. Not only in environmental affairs, but also in other sensitive topics such as chemical weapons, atomic energy, or medical epidemics several transparency principles of the Aarhus Convention are nowadays increasingly coming to the forefront; for instance, the public's right to administrative resources in case of violations or decision-makers taking advantage of public expertise.

In recent years there have been efforts to advance public-private cooperation for more transparency in cyberspace; for example, through the Global Commission on the Stability of Cyberspace and the Freedom Online Coalition's working group on "An Internet Free and Secure",[19] as well as important work done at the regional level, such as the Inter-American Committee against Terrorism's Cybersecurity Program. These efforts demonstrate there is more room for common ground on information transparency than the divisions within the UNGA's First Committee would suggest;[20] for instance, on issues like offensive cyber operations by non-state actors or norms on basic cyber hygiene. The OEWG and UNGGE would do well to build on these initiatives and engage outside actors, particularly civil society and the private sector, that have valuable expertise to offer. The principles of the Aarhus Convention could also help to develop the function of stakeholders as whistleblowers.

Engage the UN through Multi-stakeholder Dialogue in National and Regional Platforms

The United Nations is unique because it convenes the full spectrum of global views and interests. But there are other international platforms that could be used to achieve similar results among a smaller group of countries. These are interesting because they gather diverse key players, their structures are more flexible, they possess a credible level of expertise, they have more experience working with stakeholders, and they carry enough weight to negotiate on an equal footing with big countries like China or with influential institutions such as the UN or the G20. Ideas developed inside smaller platforms could then be more easily transferred to an institution like the UN. Such diplomatic sequencing creates options for stakeholders to be heard at the global level too.

> “ In recent years there have been efforts to advance public-private cooperation for more transparency in cyberspace.

In Europe, the EU probably offers the best opportunities because it has strategies on how to actively involve stakeholders in its policies. A good example is Cyber Direct, an EU-funded project designed by stakeholders.[21] Its aim is to inject ideas from the public, private, and academic sectors into EU and member state policies, and to use these ideas to create a dialogue between the EU and other big players in cyberspace such as Brazil, China, India, Japan, South Korea, and the United States. Furthermore, capitals of countries like Netherlands, Romania, Germany, France or Estonia constitute good locations for public debate and multi-stakeholder events since these countries are part of the UNGGE. EU member states increasingly coordinate their cyber policies at

[18] "The UNECE Convention on Access to Information, Public Participation in Decisionmaking and Access to Justice in Environmental Matters", United Nations Economic Commission for Europe, June 2019

[19] A multi-stakeholder working group for 15-20 selected individuals co-chaired by a government official and civil society representative.

[20] Deborah Brown, "UN General Assembly Adopts Record Number of Resolutions on Internet Governance and Policy: Mixed Outcomes for Human Rights Online", Association for Progressive Communications, January 10, 2019

[21] For more information, see "EU Cyber Direct".

the supranational level, enabling the EU to bring a united vision to the UN level, shaped in part by multi-stakeholder processes.

The OECD offers opportunities too because on many occasions it offers space for policy vetting and experimentation between member states and stakeholders. The organization's Water Governance Initiative is a good example of how to gather best practices from the public, private, and nonprofit sectors. What is more, the OECD/G20 Base Erosion and Profit Shifting Project is evidence that the organization carries enough influence to be treated on an equal footing with a global group like the G20. As a result, many guidelines and standards that were initiated at OECD level have gradually spilled over across the globe. As the OECD takes more interest in cyber governance, there are opportunities for stakeholders to engage with the organization in this field too.

> "*Ideas and opinions emerging from civil society and businesses have become unavoidable factors in agenda-setting.*

The OSCE is increasingly engaging in shaping cyber norms too. For instance, it achieved remarkable results in 2012[22] and in 2016[23] by having its members, including Russia, agree on measures to reduce the risk of tensions arising from ICT activities. At its 2017 Annual Security Review Conference, all participating states agreed that, in light of developments at the UNGGE, the OSCE's main focus should be on adopting more multi-stakeholder approaches.[24] Moreover, in May the OSCE released an internal paper on how to evaluate the role of international organizations—including itself—in the UNGGE. Given the OSCE's strong network of missions and offices that keep in touch with civil society, its practice of inviting experts to its council meetings, its regular events, and its "food-for-thought" papers that are distributed among its member states, there is a real opportunity for stakeholders to shape the organization's policies in cyberspace.

Conclusion

Policymaking is no longer the prerogative of governments. Ideas and opinions emerging from civil society and businesses have become unavoidable factors in agenda-setting. At the same time, current intergovernmental structures too often are ill-equipped to deal with this evolution. But there is a clear trend in international organizations toward open-governance models and including external stakeholders in decision-making. This change is most visible in smaller or regional organizations that can perhaps benefit from more flexible structures. At the UN level much work remains to be done, not least when it comes to involving third parties in global cyber governance or in the activities of the UNGGE and OEWG.

There is reason for optimism, though. Best practices from other domains offer lessons on how to make cyber governance more inclusive. Moreover, ideas on multi-stakeholder engagement are circulating among the members of the UNGGE and OEWG that perhaps realize that the methods of the past have not sufficiently delivered and that new forms of cooperation are needed. The suggestions presented in this paper can serve as a source of inspiration in this direction.

[22] "OSCE Permanent Council Decision No. 1039", OSCE, April 26, 2012

[23] "OSCE Permanent Council Decision No. 1202", OSCE, March 10, 2016

[24] "2017 Annual Security Review Conference, Chairperson's Report", OSCE, August 16, 2017

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org