

Multistakeholder participation at the UN

The need for greater inclusivity in the UN dialogues on cybersecurity

A study by Paris Call Working Group 3 on Advancing the UN negotiations with a strong multistakeholder approach

November 2021



Letter from the Cybersecurity Tech Accord

2021 marks the third anniversary of the Paris Call for Trust and Security in Cyberspace. The initiative, launched by French President Emmanuel Macron in November 2018, unites governments, industry, civil society, and academia on a shared path towards greater stability in cyberspace. The Paris Call's nine principles – from protecting individuals and infrastructure, to preventing the proliferation of malicious software – reflect responsibilities for all actors in the digital space that are committed to defending it against evolving cyber threats. To date, the Paris Call has attracted over 1,200 supporters, including over 75 national governments, demonstrating a growing recognition by the international community of the need to work together, across stakeholder groups, to protect cyberspace.

What sets the Paris Call apart from other agreements, in addition to its multistakeholder structure, is its ability to enable its growing community of supporters to engage with one another and work together to advance toward shared goals. In that spirit, in November 2020, the French Ministry for Europe and Foreign Affairs announced the creation of six working groups to advance international norms and to cooperate on concrete initiatives building on the Paris Call's principles. The six Paris Call working groups were tasked with 1) growing the community, 2) engaging emerging countries, 3) supporting the continuation of UN negotiations with a strong multistakeholder approach, 4) advancing international norms, 5) building a stability index, and 6) offering concrete tools to supporters.

For the past year, the Cybersecurity Tech Accord, a coalition of over 150 technology companies from around the world committed to peace and stability in cyberspace, has been chairing Working Group 3 (WG3) on "Advancing the UN negotiations with a strong multistakeholder approach." As a longtime supporter of the Paris Call, we were honored to have this opportunity to help further

unite the multistakeholder community in discussion around this important issue and to advance the work of the Paris Call overall. The online world increasingly intersects with all aspects of our lives, and it is important that all relevant stakeholders – from human rights organizations to those who operate the infrastructure of the internet – have the opportunity contribute to discussions on expectations and rules of the road in cyberspace. Indeed, only a multistakeholder approach, focused on improving global prosperity and security, can help us achieve an open, secure, stable, accessible and peaceful online world.

This study is the result of six months of engagement and discussions within WG3. It makes the case for enhanced collaboration across stakeholder groups and provides a set of recommendations on the ways to ensure greater inclusivity in the UN dialogues on cybersecurity. The study is addressed to policymakers and diplomats that will design the next generation of cyber diplomacy at the UN. This work would not have been possible without the input of the many entities that have participated in WG3, including the Global Forum on Cyber Expertise, the Global Commission on the Stability of Cyberspace, Global Partners Digital, the CyberPeace Institute, and ICT4Peace, each of which chaired one of our workshops; as well as companies such as Capgemini, DXC Technology, Microsoft and NEC; and states including France, Australia, and Canada, to name just a few. Above all, this work would not have happened without the impetus and leadership of the French Ministry for Europe and Foreign Affairs, which has made advancing cybersecurity in an inclusive manner a top priority. We hope the findings of this working group will help guide the efforts of policymakers in designing the next generation of cybersecurity dialogues and generate further discussion around how we can work together to advance peace and security in cyberspace.

Table of Contents

Glossary	4
1. Introduction	6
2. Multistakeholder Participation at the UN: A Long Tradition	9
3. Internet Governance and the Role of Non-State Actors: Promoting Progress	10
4. Multistakeholder Participation in the UN Cybersecurity Dialogues: Valuable Partnerships	12
5. UN Multistakeholder Participation Processes: A Successful UN Norm	15
5.1 United Nations Program of Action on Small Arms and Light Weapons (UN PoA SALW) - (Direct Participation).....	15
5.2 Open-Ended UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS) - (Direct Participation).....	16
5.3 Internet Governance Forum - (Multistakeholder Consultative Session).....	17
5.4 Open-Ended Working Group on Ageing – (Direct Participation).....	18
5.5 Ad-hoc Open-Ended Working Group “Towards a Global Pact for the Environment” - (Direct Participation).....	19
5.6 United Nations Development Programme Civil Society Advisory Committee - (Advisory Body)	20
5.7 United Nations Women Organization Civil Society Advisory Groups - (Advisory Body).....	21
5.8 United Nations High Level Meeting on HIV/AIDS – (Multistakeholder Consultative Session)	22
5.9 ECOSOC Partnership Forum – (Multistakeholder Consultative Session)	23
Analysis of Case Studies	24
6. Recommendations for Meaningful Multistakeholder Participation in the UN Cybersecurity Dialogues	25
7. Conclusions	28
Further Research.....	29
Bibliography	30
Annex – WG3 Participants	34

Glossary

This section provides common definitions of the key terms and concepts mentioned throughout this study:

cyberspace: the digital space made of network infrastructure (such as servers and cables), devices (like computers and smartphones), software (both human-machine and machine-to-machine interfaces) and data carried over the network.¹

cyberconflict: actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and techniques, that can include damaging, destroying, disabling, or usurping an adversary's computer systems ('cyberattack') or by obtaining information that the adversary would prefer to keep secret ('cyber espionage' or 'cyber exploitation').²

cyber diplomacy: the use of diplomatic tools and initiatives to pursue a state's national interest in cyberspace, such as establishing and fostering dialogue between state and non-state actors, developing global norms and standards of appropriate behavior in cyberspace, and pursuing policies to reduce cyber-related threats and prevent conflicts.³

multistakeholderism: a form of global governance that brings together all relevant stakeholders in discussion when addressing policy challenges or goals. Such stakeholders might include governments, international institutions, industry, civil society, academia, technical experts, and others. Multistakeholderism is seen as a departure from a traditional form of multilateralism, where nation states exclusively participate in international policy debates in dialogue with other nation states. Multistakeholderism can also be understood as a way to enhance or better inform multilateral processes by ensuring that other relevant entities can inform dialogues among states based on their expertise and perspectives in particular subject areas.⁴

norms for responsible state behavior in cyberspace: 11 voluntary, non-binding norms for the responsible behavior of states in cyberspace aimed at promoting an open, secure, stable, accessible and peaceful information and communications technology (ICT) environment. The norms were first agreed upon by the UN General Assembly's First Committee Group of Governmental Experts (UN GGE) on information security in 2015, and endorsed by all countries in UN General Assembly Resolution 70/237 as part of the UN Framework of Responsible State Behaviour in Cyberspace.⁵

Paris Call for Trust and Security in Cyberspace: a non-binding declaration launched in 2018 during the Internet Governance Forum held at United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Paris Peace Forum. The agreement calls for states, the private sector, and organizations in civil society to

¹Paris Call for Trust and Security in Cyberspace, "Paris Call for Trust and Security in Cyberspace — Paris Call" (pariscall.international) <https://pariscall.international/en/>.

²Herbert Lin, "Cyber Conflict and International Humanitarian Law" (2012) 94 International Review of the Red Cross 515 <https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf>.

³Mark Bryan F. Manantan, "Defining Cyber Diplomacy" (Australian Institute of International Affairs - May 19, 2021) <https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/>.

⁴Digital Peace Now, "Multistakeholderism: What Is It and Why Does It Matter to International Peace and Stability Online?" (Digital Peace - July 17, 2020) <https://digitalpeacenow.org/multistakeholderism-what-is-it-and-why-does-it-matter-to-international-peace-and-stability-online/#:~:text=Multistakeholderism%20Defined>.

⁵Sheetal Kumar, Deborah Brown and Anriette Esterhuysen, "Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms" https://www.gp-digital.org/wp-content/uploads/2019/12/unpacking_gge_cyber-norms.pdf.

work together to promote peace and security in cyberspace, fight disinformation and address new threats that put citizens and infrastructure in danger. The Paris Call is based around a set of nine principles to secure cyberspace. It has been endorsed by 79 states, 35 public authorities and local governments, 391 organizations and members of civil society, as well as 706 companies and private sector entities as of November 2021.⁶

UN First Committee: one of the six committees of the United Nations General Assembly, the First Committee deals with disarmament, global challenges, and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime. It considers all disarmament and international security matters within the scope of the United Nations Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; and promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.⁷

UN GGE: United Nations Group of Governmental Experts; a type of UN process that has been the primary avenue for dialogue between states about the international legal regulation of cyberspace and expectations for responsible behavior. Six successive GGEs on information and communications technology in the context of international security, each established by a resolution of the United Nations General Assembly, have taken place from 2004 to 2021, and their reports have consolidated a “framework for responsible state behavior in cyberspace” representing the current basis of the normative framework applicable to states’ use of ICTs. The GGEs have always been open to a limited number of states, initially 15 rising to 25 as of 2019.⁸

UN OEWG: United Nations Open-Ended Working Group; a type of process present in the UN typically considered the most open, as the name suggests, allowing all UN member and observer states, intergovernmental organizations, and non-governmental organizations with the UN Economic and Social Council (ECOSOC) consultative status and some others to attend public meetings of the Working Group. In 2018, the UN OEWG on Developments in the Field of ICTs in the context of International Security was established in parallel with the UN GGE by the Russian Federation. Starting its work in June 2019, the UN OEWG gathered close to 100 member states who worked on continuing to develop the rules, norms and principles of responsible state behavior, discuss implementation and ways to establish institutional dialogue on cybersecurity. The work of the UN OEWG concluded in March 2021 with the publication of its final report. In December 2020, the OEWG was renewed for 2021-2025.⁹

PoA: the Programme of Action on advancing responsible State behaviour in cyberspace; a proposal supported by over 50 states to establish a permanent, inclusive, consensus-based and action-oriented international instrument to advance responsible behavior in the use of ICTs in the context of international security. To that end, the PoA proposal aims at supporting states’ capacities to implement agreed upon commitments, fostering exchanges of good practices and promoting constructive dialogue and engagement with non-governmental stakeholders.¹⁰

⁶Paris Call for Trust and Security in Cyberspace, “Paris Call for Trust and Security in Cyberspace — Paris Call” (pariscall.international) <https://pariscall.international/en/>.

⁷United Nations, “UN General Assembly - First Committee - Disarmament and International Security” (Un.org2020) <https://www.un.org/en/ga/first/>.

⁸Anders Henriksen, “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace” (2019) 5 Journal of Cybersecurity. <https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865>.

⁹Anrijana Gavrilovic, “A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers” (DiploMarch 18, 2021) <https://www.diplomacy.edu/blog/new-landmark-global-cybersecurity-negotiations-un-cyber-oewg-numbers>.

¹⁰France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States, “The Future of Discussions

1. Introduction

Rising tensions in cyberspace, where cyberattacks by both cybercriminals and state actors have been increasing in frequency and sophistication for over a decade, have driven cybersecurity to become a matter of grave concern for the international community across all stakeholder groups. Sophisticated cyberattacks impacting businesses, critical infrastructure, and key societal services have become a regular occurrence, and finding solutions to address these threats has risen to the top of the global political agenda. Since its inception in 2018, the *Paris Call for Trust and Security in Cyberspace*¹¹ has provided a platform for engagement and dialogue on advancing the security and stability of cyberspace, creating an unprecedented forum for multistakeholder dialogue on this issue. Over 1,200 entities, including governments, businesses, and international civil society organizations, have now endorsed the Paris Call's nine principles, which emphasize protecting individuals, organizations, and infrastructure from attacks, as well as preventing the proliferation of malicious software. For some time now, escalating cyberattacks have demonstrated the need for a more inclusive and holistic approach to peace and securi-

ty online, one that promotes responsible behavior alongside capacity building, and which leverages expertise from across stakeholder groups to find solutions.

In 2021, the Paris Call engaged its supporters by establishing six Working Groups *“to strengthen the Paris Call community and to implement tangibly the principles structuring it.”*¹² This study was developed in the context of Paris Call Working Group 3 (WG3), which has been tasked with *“Advancing the UN negotiations with a Strong Multistakeholder Approach.”* Over the past 20 years, United Nations (UN) discussions on cybersecurity have taken place within the UN First Committee that is responsible for disarmament, nonproliferation, arms control, and international security issues, and with limited involvement from non-governmental stakeholders. This has raised questions regarding the sustainability and efficacy of such an approach in a domain as complex as cyberspace, where overlapping roles and responsibilities are shared across stakeholder groups, especially when it comes to cybersecurity.

On ICTs and Cyberspace at the UN” (2020) <<https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf>>.

¹¹Paris Call for Trust and Security in Cyberspace, “Paris Call for Trust and Security in Cyberspace — Paris Call” (pariscall.international) <https://pariscall.international/en/>.

¹²Ministère de l'Europe et des Affaires étrangères, “Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace” (France Diplomacy - Ministry for Europe and Foreign Affairs) <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->

The multistakeholder model has always been central to internet governance outside the security space. Moreover, *multistakeholderism*, defined as a form of global governance bringing together relevant stakeholders in policy discussions, is not a foreign concept in the context of the UN dialogues. The issue of multistakeholder participation in discussions pertaining to the global political agenda has been debated since the inception of the UN as an organization. In fact, examples of UN discussions that have gradually opened-up to non-governmental stakeholder participation abound, and while the matters of the UN First Committee's competence have often been more exclusive to states, there have been successful efforts to involve relevant organizations in debates around international security issues.¹³ The 2021 report by the UN Secretary-General, "*Our Common Agenda*," is a testament to reinvigorated attention to multistakeholderism at the UN. The report stresses the importance of ensuring stronger involvement from all relevant stakeholders to identify and agree on the global commons or public goods that may require renewed commitments from the international community as well as policy reform.¹⁴

Chaired throughout 2021 by the Cybersecurity Tech Accord,¹⁵ a coalition of over 150 technology companies committed to advancing the stability of cyberspace, WG3 has facilitated an inclusive and far-reaching discussion within the Paris Call community on how to support multistakeholder participation in future cybersecurity dialogues at the UN. Following a kick-off meeting in March 2021, WG3 held three thematically organized workshops between May and September in which over 80 participants, including representatives from governments, academia, industry and civil society organizations from around the world, dis-

cussed the importance of making UN cybersecurity dialogues more inclusive and proposed concrete approaches for doing so.

○ The first workshop,¹⁶ held in May and titled "*Examples of multistakeholder governance and applicability to the discussions on cyber*," reflected on the lessons learned from previous multistakeholder initiatives at the UN and beyond, including one that led to the development of the International Code of Conduct for Private Security Service Providers (ICoC). Participants also discussed the challenges impeding progress toward making the UN cybersecurity negotiations more inclusive and solutions oriented.

○ The second workshop,¹⁷ held in June, was organized as part of the 10th edition of the RightsCon conference, the world's leading summit on human rights in the digital age. Titled "*Playing by the Rules: Working together to rein in nation-state cyberattacks*," the event featured a panel of experts who examined the evolving threats posed by state-sponsored cyberattacks on businesses and society, as well as the government's role in addressing this pressing issue, including by implementing international norms and facilitating greater dialogue within the multistakeholder community.

○ The third workshop, held in September and titled "*The proposal for a Programme of Action and the way forward for multistakeholder dialogue on cyber*," offered participants an opportunity to hear from Henri Verdier, French Ambassador for Digital Affairs, about a proposal supported by over 50 UN member states, to advance more concrete and action-oriented cooperation on cybersecurity at the UN

¹³Section 5 of this study includes further details on multistakeholder participation in the context of First Committee processes including in the context of the United Nations Program of Action on Small Arms and Light Weapons (UN PoA SALW) and Open-Ended UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).

¹⁴United Nations, "Our Common Agenda. Report of the Secretary-General" https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf.

¹⁵Cybersecurity Tech Accord, "About the Cybersecurity Tech Accord" (Cybersecurity Tech Accord) <https://cybertechaccord.org/about/>.

¹⁶Cybersecurity Tech Accord, "Discussions on Cyberspace Security Need to Be More Inclusive, Says Paris Call Working Group" (Cybersecurity Tech Accord - August 4, 2021) <https://cybertechaccord.org/discussions-on-cyberspace-security-need-to-be-more-inclusive-says-paris-call-working-group/>.

¹⁷Cybersecurity Tech Accord, "Cybersecurity Tech Accord Discusses Threat Posed by State-Sponsored Cyberattacks and the Importance of Cooperation during RightsCon 2021" (Cybersecurity Tech Accord - July 13, 2021) <https://cybertechaccord.org/cybersecurity-tech-accord-discusses-threat-posed-by-state-sponsored-cyberattacks-and-the-importance-of-cooperation-during-rightscon-2021/>.

and discuss a way forward, including plans to bring this proposal to the attention of the new OEWG later in the year.

This study seeks to capture the key takeaways from these workshops, as well as the results of a desk review of relevant literature and multiple rounds of open consultation with the participants of WG3 over six months. The study is addressed to policymakers and diplomats that will design the next generation of cyber diplomacy at the UN. It considers the history of multistakeholder partic-

ipation at the UN, explores and assesses recent multistakeholder inclusion processes in relation to ICT discussions, taking stock of their successes and shortcomings, and provides examples of other multistakeholder processes within the UN framework in order to analyze and assess their feasibility in the context of ICT discussions. Finally, this report draws conclusions based on this input, identifying recommendations for meaningful multistakeholder participation in future UN discussions on cybersecurity in the context of international security.

Additional multistakeholder efforts

The study is part of a broader effort to discuss the ways to ensure greater multistakeholder participation in the UN dialogues on cybersecurity. A brief published in October 2021 by civil society representatives from Association of Progressive Communications, Global Partners Digital, Women's International League of Peace and a Consultant to the OSCE Office for Democratic Institutions and Human Rights, entitled "Promoting stakeholder engagement at the Open-Ended Working Group on ICTs," touches upon similar issues and provides examples of good practices and lessons learned from civil society engagement in a range of UN and non-UN forums. We encourage readers of this study to consult this brief as well for additional insightful considerations on these issues.¹⁸

¹⁸Association for Progressive Communications, "Promoting stakeholder engagement at the Open-Ended Working Group on ICTs" <https://www.apc.org/en/pubs/promoting-stakeholder-engagement-open-ended-working-group-icts>.

2. Multistakeholder Participation at the UN: A Long Tradition

The basis for the participation of non-state actors in the UN resides in its Charter, the foundational treaty signed in 1945 by 50 of the 51 original UN member states. Article 71 of the UN Charter states that the United Nations Economic and Social Council (ECOSOC) “*may make suitable arrangements for consultation with non-governmental organizations which are concerned with matters within its competence.*” ECOSOC resolution 1296, passed in 1968, defined the criteria and rights associated with this consultative status, stressing that these arrangements would “*provide an important means of furthering the purposes and principles of the United Nations.*” Overall, the resolution recognized the importance of securing expert information or advice from organizations with special competence in certain subjects, and of ensuring that important elements of public opinion would be represented.¹⁹ This approach to multistakeholder inclusion at the UN has led to the proliferation of inclusive arrangements with increasing involvement of non-governmental stakeholders in several UN processes.

In the 1990s, the UN seemed to recognize that existing models for multistakeholder inclusion needed to be expanded and built upon on various issues to ensure impactful outcomes for the world. The 1992 UN Conference on Environment and Development (UNCED) catalyzed greater participation of non-governmental stakeholders: over 1,400 NGOs were welcomed into the offi-

cial intergovernmental process to help governments and international organizations work and deliberate on sustainable development. Following UNCED, momentum for greater multistakeholder involvement continued to build, especially around subsequent world conferences on other global issues. However, as demands for accreditation began to produce more and more conflicts between NGOs and States, as well as within the NGO community, it quickly became clear that the rules governing ECOSOC consultative status were poorly designed to facilitate participation in the follow-ups to these conferences and to allow non-governmental stakeholders to engage in a more structured way in the context of permanent UN organizations.²⁰

During the 1990s, the debate about how to reform UN relations with business and society continued, and there were several attempts to introduce coherence in the rules governing the participation of non-governmental organizations in international conferences convened by the United Nations and elsewhere.²¹ ECOSOC Resolution 1996/31 revised the criteria for NGO accreditation to consultative status.²² The resolution stressed the need for greater transparency with “*wide and timely dissemination of information on meetings*” as well as “*provision of access and transparent, simple and streamlined procedures for the attendance of non-governmental organizations in United Nations meetings.*”

¹⁹United Nations Economic and Social Council, “ECOSOC Resolution 1296 (XLIV)” <https://archive.globalpolicy.org/component/content/article/177-un/31832.html>.

²⁰Chadwick Alger, “The Emerging Roles of NGOs in the UN System: From Article 71 to a People’s Millennium Assembly” (2002) 8 *Global Governance: A Review of Multilateralism and International Organizations* 93 https://www.jstor.org/stable/27800329?seq=4#metadata_info_tab_contents.

²¹United Nations Economic and Social Council, “1993/80 Review of the Arrangements for Consultation with Non-Governmental Organizations” <http://www.un-documents.net/1993-80.htm>.

²²United Nations Economic and Social Council, “1996/31 Consultative Relationship between the United Nations and Non-Governmental Organizations” <https://www.un.org/ecosoc/sites/www.un.org.ecosoc/files/documents/2020/resolution-1996-31.pdf>.

The 2002 Monterrey Conference on Financing for Development, the World Summit on Sustainable Development in Johannesburg (2002), and the World Summit on the Information Society in Geneva and Tunis (2003, 2005) set new precedents in the history of multistakeholder inclusion at the UN with private sector and civil society actors systematically included right from the start in the shaping of international diplomacy.

Today, the UN 2030 Agenda emphasizes the importance of multistakeholder partnerships for

achieving the 17 UN Sustainable Development Goals (SDGs). In fact, SDG 17 includes a specific target for national governments to promote multistakeholder collaboration between state and non-state actors. While these models cannot be a substitute for government responsibilities in the 21st century, they are instrumental in identifying and implementing outcomes where successful implementation of international commitments requires cooperation and coordination with non-governmental partners.

3. Internet Governance and the Role of Non-State Actors: Promoting Progress

The extent of participation to welcome from industry, civil society and academia in UN dialogues is a subject of debate in the international community. While the need to include these voices in international diplomacy and discussions around modern issues is widely recognized, there remains no consensus around the modalities and influence that these stakeholder groups should have. In recent years, considerations regarding greater inclusivity have also been raised in the context of the UN discussions on international ICT security. This desire for greater inclusion is understandable given the complex nature of cyberspace and the division of roles and responsibilities among different stakeholders, including states, academia, civil society and the private sector which owns and operates the majority of the global internet infrastructure today.

Increasingly, governments have looked to the ICT industry to prevent, detect, respond to, and re-

cover from cyberattacks, as well as to identify and expose the perpetrators. In recent years, beyond supplying this technical expertise, the technology industry has become more active in offering support concerning international cybersecurity norms development and implementation. This growing engagement from the private sector in the global political arena stemmed from the recognition that as cyberspace has emerged as a new domain of conflict, technical tools will not be sufficient to address evolving cyber threats that undermine a domain that is largely privately owned. Normative instruments and political commitments by states are essential to a more stable and secure cyberspace, as they are in other domains of human activity. This is one of the conclusions of a recent study by the Cybersecurity Tech Accord in partnership with the Economist Intelligence Unit analyzing the evolving threat of state-sponsored cyberattacks.²³ Survey results showed that businesses see political coop-

²³Cybersecurity Tech Accord and The Economist Intelligence Unit, "Securing a Shifting Landscape: Corporate Perceptions of Nation-State Cyber-Threats" (2021) <https://cybertechaccord.org/uploads/prod/2021/02/eiu-cybersecurity-tech-accord-report.pdf>.

eration as one of the main solutions to increasing numbers of state-led and sponsored cyberattacks.

In addition to the private sector, civil society has emerged as another important actor seeking engagement and legitimacy in ICT security discussions. As more and more of our daily lives intersect with the digital world, the security and stability of the internet are increasingly essential to modern society, making the involvement of civil society organizations particularly important as rights defenders in a new domain. Civil society groups have been fundamental in driving recognition of the need to include human rights considerations in the global cybersecurity agenda. They have also raised governments' awareness of evolving threats in cyberspace, such as the rise in cyberattacks against healthcare facilities during the COVID-19 pandemic, shedding light on the impact of these attacks and helping to identify possible solutions.

Finally, the valuable role of academia and NGOs in these dialogues should not be underestimated. Academia plays a key role in facilitating and developing studies and technical research that can help the UN and individual states progress their approaches to ICT governance. For example, legal scholars and other academics play a critical role in developing our understanding of how international law applies to state behavior cyberspace. In 2020 and 2021, legal experts from across the globe, in a collaborative effort known as the "*Oxford Process*,"²⁴ released four statements aimed at providing states with guidance on international law protections against cyber operations targeting the healthcare sector, on safeguarding vaccine re-

search, on protecting electoral processes and on the application of international law to ICT-related operation and activities. While the road to clarifying how other key concepts of international law apply to cyber operations is still long, similar efforts have been helping states navigate this relatively new field with greater confidence and certainty, and helping to build international consensus.

It would be difficult to deny the value that these stakeholders – industry, civil society and academia – can add to the discussions on cyber governance. In line with the point already recognized in the 1968 ECOSOC Resolution 1296 defining the criteria and rights associated with third-party consultative status, they have the needed capacities and resources to provide expert information and advice to governments on these issues. In fact, the need to identify mechanisms for greater multistakeholder engagement has been widely acknowledged, including in the conclusions of the recent UN cybersecurity dialogues – UN GGE and OEWG - discussed in the next section. Despite this recognition, however, progress on greater multistakeholder inclusion has been limited. From the discussions, it has emerged that the view held by several member states is that an appropriate balance needs to be found between multistakeholder inclusion and the central role of states in negotiations dealing with matters pertaining to international security. In the meantime, the multistakeholder community has taken every opportunity to provide states with meaningful contributions, and the hope is that more effective mechanisms will be established to make this process smoother and more robust.

²⁴Oxford Institute for Ethics, Law and Armed Conflict, "The Oxford Process on International Law Protections in Cyberspace" (www.elac.ox.ac.uk/the-oxford-process-on-international-law-protections-in-cyberspace/).

4. Multistakeholder Participation in UN Cybersecurity Dialogues: Valuable Partnerships

While it might be difficult to identify a specific event that ushered in the era of cyberconflict, governments have been using cyber capabilities for offensive operations against other states to advance their political interests for over two decades. Countries such as the United States, China, Israel, Russia and the United Kingdom have been the first to invest in and deploy offensive cyber capabilities.²⁵ However, research shows that over one-quarter of United Nations member states possess such cyber capabilities, and the number of states able to conduct cyber operations in or through foreign infrastructure is growing.²⁶ According to the Council on Foreign Relations, 33 states have already utilized international cyber operations with the intent to advance their strategic interests in or through foreign ICT infrastructure since 2005.²⁷ Despite the covert nature of these attacks, they can have devastating consequences, especially when targeting critical infrastructure or ICT supply chains such as in the hack against software company SolarWinds in 2020.²⁸ Malicious state-sponsored cyber operations are not only concerning due to their potential disruption of critical infrastructure, business operations and key societal services, but also for their escalatory potential and the risk that hostilities might extend to the kinetic domain. Thus, ensuring the safety and

stability of cyberspace has emerged as a key security challenge for the international community.

The first attempts to codify the impacts and developments of ICT on international security and military affairs in UN discussions began in 2004 with the establishment by the United Nations General Assembly (UNGA) of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE). The GGE was tasked with exploring ways to strengthen peace and security in cyberspace through confidence-building measures and by developing norms and standards for responsible state behavior in this new domain. A total of now six GGEs with similar mandates have been convened since 2004, the most recent of which was the GGE 2019-2021. Several of these GGE bodies produced seminal reports that set precedent and expectations for responsible state behavior online. The 2012-2013 GGE concluded by setting an important milestone: the adoption of a consensus report affirming the applicability of international law to cyberspace for the first time.²⁹ Meanwhile, the 2014-2015 GGE report, adopted by the UN General Assembly Resolution A/RES/70/237,³⁰ reaffirmed the consensus around international law and its applicability to cyberspace, and also intro-

²⁵Keith Breene, "Who Are the Cyberwar Superpowers?" (World Economic Forum) May 4, 2016. <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>.

²⁶United Nations Institute for Disarmament Research, "International Cyber Operations: National Doctrines and Capabilities" (2021) <https://unidir.org/sites/default/files/2021-05/International%20Cyber%20Operations%20Series%20-%20Paper%201.pdf>

²⁷Council on Foreign Relations, "Cyber Operations Tracker" (2020) <https://www.cfr.org/cyber-operations/>

²⁸Reuters, "SolarWinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President" Reuters (February 15, 2021) <https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R>.

²⁹United Nations General Assembly, "Report on the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security" (2011) <https://undocs.org/A/RES/66/24>.

³⁰United Nations General Assembly, "Resolution adopted by the General Assembly on 23 December 2015" (2015) <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf>.

duced 11 voluntary norms for responsible state behavior in this new domain.³¹

The importance of the respective GGEs in advancing political discussions on international ICT security is undeniable; however, the non-inclusive format and approach of these deliberations have made it difficult for stakeholders including industry, civil society and academia to provide valuable input and expertise as a routine part of the process. Since they began, the GGE dialogues have been exclusive to a limited number of UN member states (originally 15, and rising to 25 as of 2019) and have not included mechanisms for direct engagement with the multistakeholder community, with the exception of the regional consultations organized in advance of the sessions of the 2019-2021 GGE, which allowed for some measure of engagement with other stakeholders such as NGOs.³² This approach is in sharp contrast with the UN's long history of multistakeholder participation in other dialogues and with the tradition of a multistakeholder model in internet governance.

In May 2021, the 2019-2021 GGE adopted its final consensus report. The report's selection signaled optimism regarding future efforts by states to identify how international law applies to cyberspace and detailed how states can uphold expectations for responsible behavior online. The report also recognizes the importance of input from and participation of relevant non-governmental stakeholders, including the private sector, academia and civil society. However, it remains largely silent regarding their involvement in future UN cyber negotiations.³³

The GGE has not been the only UN venue dedicated to discussions on international ICT security. In 2018, the UN General Assembly established the Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security, a parallel and more inclusive track to the GGE. Not only did the OEWG open the discussions to all UN member states, but in December 2019 it also held the first informal multistakeholder consultation in the history of these dialogues.³⁴ 113 non-state organizations registered to participate in the meeting, including private companies, NGOs and universities from all regions of the world, a testament to the multistakeholder community's great interest in and commitment to contributing to the evolution of these discussions.³⁵ The December 2019 meeting also demonstrated the value of non-governmental stakeholder participation, as it was widely noted among member states following the event how their participation enriched the discussions. It also afforded all participants an opportunity to discuss their ongoing work and ways to further collaborations across stakeholder groups, including states.

The OEWG final report, published in March 2021 and reaffirming the conclusions of previous GGE reports, including the applicability of international law to cyberspace and the framework of 11 norms for responsible state behavior in this domain, recognizes the value of this multistakeholder exchange.³⁶ The report states that "the broad engagement of non-governmental stakeholders [in these dialogues] has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure

³¹United Nations General Assembly, "Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security" (2015) https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

³²United Nations, "Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (2019) <https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf>

³³GGE on Advancing responsible State behaviour in cyberspace in the context of international security, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (2021) https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

³⁴Resolution "A/RES/73/27" which set up the OEWG, "with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent" specifically stresses that "while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations."

³⁵Council on Foreign Relations, "From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity" (Council of Foreign Relations Blog - January 27, 2020) <https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity>.

³⁶Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), "Final Substantive Report" (2021) <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

an open, secure, stable, accessible and peaceful ICT environment.”³⁷ Further, the report recognizes “the importance of regular intergovernmental dialogue and of identifying appropriate mechanisms for engagement with other stakeholder groups in future processes.”

Unfortunately, the December 2019 consultative session proved to be an isolated event, and the OEWG failed to facilitate greater and more consistent multistakeholder inclusion for the remainder of its deliberations. After convening the 2019 consultative session, the OEWG closed its doors to non-ECOSOC accredited NGOs and private organizations. Multistakeholder discussions were held separately on the initiative of academia, the private sector and civil society groups.³⁸ Several UN member states took part in the unofficial side events, including the Swiss delegation and the OEWG Chair, and the Australian delegation consistently and proactively sought out multistakeholder input on their own.³⁹ However, no official processes or mechanisms were established to allow non-governmental stakeholders to provide input to the negotiations within the OEWG, except through the provision of written comments. At the same time, the conclusions of the OEWG final report are encouraging, and the recognition of the value of multistakeholder inclusion should inform future UN dialogues on peace and security in cyberspace. In December 2020, a second OEWG was adopted to run until 2025. Its mandate began in June 2021, and it plans to advance the dialogue on international ICT security with regular reporting to the UNGA. The new OEWG 2021-2025 has a unique opportunity to build on the conclusions of the March 2021 report and to ensure greater multistakeholder participation in its proceedings.

2021 has been a watershed year for the UN dialogues on cybersecurity, given the adoption of consensus reports by the UN GGE and the OEWG and greater recognition by UN member states of the importance of jointly addressing evolving threats in cyberspace. During its 76th session, held in September 2021, the UNGA separately adopted the 2021 UN GGE and the OEWG final reports and approved the OEWG’s work plan for 2021 through 2025. Upcoming developments are expected to be equally significant. In the coming months, UN member states will consider a proposal known as Programme of Action (PoA) on advancing responsible State behaviour in cyberspace, which was supported by over 50 states and hopes to end the parallel tracks of the GGE and OEWG to advance more concrete and action-oriented cooperation on cybersecurity at the UN through a new standing body.⁴⁰ The PoA would aim to establish a permanent, inclusive, consensus-based and pragmatic international instrument to advance responsible state behavior in cyberspace in alignment with the norms and rules recognized in earlier GGE and OEWG reports. Its objective is also to promote constructive dialogue and engagement with other stakeholders, such as the private sector, academia and civil society.

Regardless of the chosen approach – ending parallel tracks to establish a permanent platform or continuing with two separate working groups – ensuring UN dialogues on cybersecurity are more inclusive of non-governmental stakeholders’ voices will be crucial to future progress in turning the tide against escalating conflict online. The private sector, NGOs, academia and civil society are all important contributors to ensuring an inclusive, safe and secure ICT environment.

³⁷Ibid.

³⁸The *Let’s Talk Cyber* event series was launched in December 2020 by a group of stakeholders including the Canadian government, Global Partners Digital, Microsoft, Research ICT Africa and Women’s International League for Peace and Freedom with the objective of bringing together state and non-state actors to discuss the progress of the discussions at the OEWG.

³⁹In November 2019, the Australian Department of Foreign Affairs and Trade (DFAT) launched a Public Consultation on Responsible state behaviour in cyberspace in the context of international security at the United Nations <https://www.internationalcybertech.gov.au/public-consultation-responsible-state-behaviour-in-cyberspace>.

⁴⁰France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States, “The Future of Discussions on ICTs and Cyberspace at the UN” (2020) <<https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf>>.

5. UN Multistakeholder Participation Processes: A Successful UN Norm

As previously mentioned, the UN has a long history of multistakeholder inclusion dating back to its origins. Non-governmental actors have played an active role in several UN dialogues and have contributed to the development of global policies and positions on some of the most pressing issues of our time. This section explores some of the most notable examples of multistakeholder participation at the UN and considers the lessons learned from these experiences to formulate a series of recommendations for meaningful multistakeholder participation in the UN dialogues on cybersecurity moving forward. The examples have been grouped in three categories that describe the modality of participation for non-state actors of each example. These include:

- **Direct participation** – modalities that foresee the direct involvement of multistakeholder actors in international negotiations and agreements, either written or oral;
- **Multistakeholder consultative session** – regularly scheduled sessions organized purposely to engage the multistakeholder community in international conversations; and
- **Advisory bodies** – modalities which actively seek the input of relevant experts from the multistakeholder community to establish priorities and drive the overall direction of the work.

5.1 United Nations Program of Action on Small Arms and Light Weapons (UN PoA SALW) - (Direct Participation)

In July 2001, the United Nations adopted by consensus the Program of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA SALW). This UN Program of Action established the first globally recognized framework for activities to counter the illicit trade in small arms and light weapons and to control its negative consequences.⁴¹ It was adopted by UN states in an effort to improve national small arms laws, import and export controls, and stockpile management, as well as to engage in cooperation and assistance at the global level.⁴² In its establishing treaty, the PoA recognized: “the important contribution of civil society, including non-governmental organizations and industry in, inter alia, assisting Governments to prevent, combat and eradicate the illicit trade in small arms and light weapons in all its aspects.”⁴³

At the local, regional and international levels, civil society plays a key role in advocating for disarmament and arms control. A good example of the influence of the multistakeholder community and its active participation in international discussions about disarmament, can be observed in the Biennial Meeting of States to Consider the Implementation of the Programme of Action to Prevent,

⁴¹United Nations Regional Centre for Peace and Disarmament in Asia and the Pacific, “Programme of Action – the United Nations Programme of Action on Small Arms and Light Weapons” (UNRCPD) <<https://unrcpd.org/conventional-weapons/poa/>.

⁴²United Nations Disarmament, Programme of Action on small arms and its International Tracing Instrument. <https://www.un.org/disarmament/convarms/salw/programme-of-action/>

⁴³United Nations, “Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects,” 21 July 2001 [https://undocs.org/en/A/CONF.192/15\(SUPP\)](https://undocs.org/en/A/CONF.192/15(SUPP))

Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (BMS).

Accreditation and Participation: Rule 63 of the Protocol's Rules of Procedure clearly lays out the rules for third-party participation: relevant non-governmental organizations with ECOSOC consultative status must inform the President of the Conference, who will, in turn, provide the Conference with a list of these organizations on a no-objection basis. Organizations may attend the Conference except for sessions defined as closed and may address the Conference during one meeting specifically allocated for this purpose. Finally, accredited non-governmental organizations are provided, upon request, with documents related to the Conference, and they may, at their own expense, provide material to the delegations, outside the conference room, in the area of the Conference.⁴⁴

Impact of the COVID-19 Pandemic: While in its establishing rules and in previous years, participation from civil society in the work of the Biennial Meeting of State was foreseen and encouraged, multistakeholder participation was not prioritized in the BMS7, which took place in July 2021. Most of the preparatory meetings were informal and held in a closed format, for instance, and significant portions of the BMS7 were also held in closed format and not webcasted.

Coordination: Civil society participation in the Seventh Biennial meeting (BMS7) was coordinated by the International Action Network on Small Arms (IANSA), an international NGO that aims to reduce gun violence and promote local, national, regional and global measures to strengthen human security.⁴⁵ IANSA provided all information to interested non-governmental organizations on participation in the conference, including contact points and ways to sign up for the sessions.⁴⁶

The modalities for third-party participation in the discussions of the UN PoA SALW provide NGOs and civil society a clear path for participation in the PoA's conferences. While the COVID-19 pandemic made in-person participation at meetings practically impossible, in earlier years of UN PoA implementation the driving role of civil society behind the instrument's creation was better reflected in the participation of civil society at its biennial and other meetings.

5.2 Open-Ended UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS) - (Direct Participation)

Another example of multistakeholder participation in the UN's First Committee structure can be observed in the open-ended UN Group of Governmental Experts (GGE) process underway within the Convention on Certain Conventional Weapons (CCW). The GGE was established in 2016 to assess questions related to emerging technologies in lethal autonomous weapons systems. The creation of this Group reflects international recognition that incorporating emerging technologies such as artificial intelligence (AI) and robotics into military capabilities must be assessed by the international community regarding their potential impact on peace and stability and implications for the applicability of international humanitarian law. At the recommendation of the 2019 GGE on LAWS, 11 guiding principles were adopted by the 2019 Meeting of the High Contracting Parties to the CCW. The first principle affirms that international humanitarian law continues to apply fully to all weapons systems, including LAWS.

Taking a multistakeholder approach, the Group encourages non-governmental actors to submit contributions that would be fed into its work. In fact, throughout the years the GGE has been meeting, it has been possible for civil society to send in written submissions or reactions. GGE meetings also allow for civil society to deliver in-

⁴⁴United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, "Provisional Rules of Procedure of the Conference" (2001) <https://undocs.org/A/CONF.192/L.1>.

⁴⁵International Action Network on Small Arms, "What We Do" (IANSA) <https://iansa.org/what-we-do/>.

⁴⁶International Action Network on Small Arms, "Seventh Biennial Meeting of States on the United Nations Programme of Action on Small Arms (BMS7)" (IANSA – April 10, 2021) <https://iansa.org/seventh-biennial-meeting-of-states-on-the-united-nations-programme-of-action-on-small-arms/>.

terventions at any point during the discussion on any topic, providing all stakeholders equal footing in the discussions while states remain the ultimate decision-makers. For instance, international organizations and civil society groups were invited to provide comments on the 11 guiding principles adopted by the GGE.⁴⁷ Additionally, the GGE encourages the participation of representatives and experts specialized or interested in issues pertaining to lethal autonomous weapon systems and other forms of military AI, through holding side events to its sessions, such as the UNIDIR side event to the 2020 GGE on predictability and understandability in military AI.

The highly technical nature of the debate surrounding potential policy, legal, and ethical challenges posed by emerging technologies in the area of lethal autonomous weapons systems often demands expert clarification. Therefore, involving researchers and experts in the workings of the GGE to inform boundaries of acceptability on autonomous weapon systems can be considered a best practice of multistakeholder inclusion.

5.3 Internet Governance Forum - (Multistakeholder Consultative Session)

The Internet Governance Forum (IGF) is an annual multistakeholder UN event that aims to facilitate policy dialogue on internet governance issues with a focus on addressing risks and challenges, exchanging information and sharing best practices. One of the outcomes of the World Summit on the Information Society (WSIS-II) held in 2005 was an agreement that the process of internet governance involves many stakeholders in a variety of roles. As a result, the WSIS-II requested the UN Secretary-General to convene an Internet Governance Forum as a multilateral, multistakeholder, democratic and transparent platform for discussions on internet governance issues. A key part of the mandate of the IGF, as set out by the Tunis

Agenda, is to “discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet,” and to “facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.”⁴⁸

From its inception, the IGF was designed to be a multistakeholder forum. This is clearly reflected in its process: it is set up as a year-long open and inclusive process that consists of annual meetings and intersessional activities.⁴⁹ IGF meetings are coordinated by the Multistakeholder Advisory Group (MAG) and the IGF Secretariat. The Multistakeholder Advisory Group is comprised of 40 members from governments, the private sector, civil society, academic and technical communities, from all five UN regional groups (Africa, Asia-Pacific, Eastern Europe, Group of Latin America and Caribbean Countries – or GRULAC, Western European and Other Group – or WEOG). The process typically involves calls for issues to determine the main meeting topics, calls for workshop proposals, and several rounds of open consultations. Participants in the Forum represent governments, intergovernmental organizations, the private sector, the technical community, academia, and civil society, and participation is open and free of charge to anyone interested, both in its annual meetings and intersessional activities.

In a sign of the growing importance of multistakeholder governance on matters pertaining to the digital sphere, the UN Secretary-General’s “Roadmap for Digital Cooperation,” issued in 2020, stressed the need for the IGF to start delivering tangible results.⁵⁰ The Roadmap included ideas for making the Forum more responsive and relevant to current digital issues, including creating a strategic and empowered multistakeholder high-level body and having a more focused agenda.

⁴⁷Reaching Critical Will – Women’s International League for Peace and Freedom, “Statements from the 2020 CCW Group of Governmental Experts on Lethal Autonomous Weapon Systems” (reachingcriticalwill.org – September 21, 2020) <https://reachingcriticalwill.org/disarmament-fora/ccw/2020/laws/statements>.

⁴⁸Internet Governance Forum, “About the IGF” <https://www.intgovforum.org/multilingual/tags/about>.

⁴⁹Internet Governance Forum, “About the Internet Governance Forum” https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4099/481.

⁵⁰United Nations, “Report of the Secretary-general. Roadmap for Digital Cooperation,” (2020) https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

So far, the IGF has successfully fostered dialogue on global trends and risks, inspiring decision-makers and providing an outlet for developing countries in particular to engage in debates surrounding internet governance. It has enabled representatives from emerging economies especially to build knowledge and acquire skills to enhance their participation in existing internet governance institutions.⁵¹ The Forum's Dynamic Coalitions are another example of how the IGF's efforts have found success. These coalitions discuss community connectivity, core internet values, gender and internet governance and much more.⁵²

One of the main challenges for the IGF so far has been translating the discussions and their outcomes into policy recommendations and cutting-edge opinions that are of importance and of influence beyond the Forum. Based on the priorities identified by the above-mentioned Roadmap, making the IGF more directly impactful will likely continue to be high on the UN agenda. In the context of the UN cybersecurity dialogues, the IGF could be used to help bridge the gap between the state-centered processes such as the GGE and the OEWG and the need for a more open forum able to make the results of discussions more influential and legitimate.

5.4 Open-Ended Working Group on Ageing - (Direct Participation)

The Open-ended Working Group on Ageing for the purpose of strengthening the protection of the human rights of older persons was established by the UN General Assembly Resolution 65/182 in 2010. The Working Group's aim is "to consider the existing international framework of the human rights of older persons and identify possible gaps and how best to address them, including considering, as appropriate, the feasibility of further instruments and measures."⁵³ Between 2010 and 2021, the Working Group has held 11 annual ses-

sions, each consisting of multiple meetings finalized with the adoption of a draft report.

A prime example of a UN Working Group with a strong multistakeholder approach, its sessions are attended by a variety of relevant stakeholders, such as representatives of UN member states, organizations of the UN system and intergovernmental organizations, as well as accredited national human rights institutions (NHRIs) and non-governmental organizations (NGOs). Multistakeholder participation is facilitated by clear modalities:

○ **Accreditation.** Besides the participation of NGOs with ECOSOC status, other relevant NGOs may apply to the secretariat for accreditation. Accreditation to the OEWG need only be done once and applies for all sessions, and new NGOs are approved under the first agenda item of each annual meeting by all participants. The OEWG has also agreed that accredited "Category A status" National Human Rights Institutions (NHRIs) can take part in the OEWG.⁵⁴ The UN Focal Point on Ageing is tasked with answering queries on NGOs participation as needed.

○ **Input to the sessions.** Each year during the inter-sessional period, the Chair of the Open-ended Working Group on Ageing invites: (i) Members of the Working Group, (ii) Member States and Observer States, (iii) National Human Rights Institutions accredited with an "A" status (fully compliant with the Paris Principles, relating to the status of national institutions for the promotion and protection of human rights), (iv) non-governmental organizations with ECOSOC Status, (v) previously accredited organizations to the Open-ended Working Group on Ageing, as well as (vi) United Nations Funds, Programmes, Specialized Agencies and other UN Entities, to provide inputs on the focus areas of the session by referring to a series

⁵¹Internet Governance Forum "About the Internet Governance Forum." https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4099/481

⁵²Internet Governance Forum "About IGF FAQs" <https://www.intgovforum.org/multilingual/content/about-igf-faqs>

⁵³United Nations Department of Economic and Social Affairs, "United Nations Open-Ended Working Group on Strengthening the Protection of the Human Rights of Older Persons" (social.un.org) <https://social.un.org/ageing-working-group/>.

⁵⁴Global Partners Digital, "NGO Participation in Multilateral and Multistakeholder Forums: Good Practice Examples" (2020) https://www.gp-digital.org/wp-content/uploads/2020/06/ngo-participationgoodpractice_gpd.pdf

of guiding questions. The focus areas are selected based on two questionnaires prepared by OHCHR and the Department of Economic and Social Affairs. For the eleventh session, held in 2021, these areas were “Right to Work and Access to the Labour Market” and “Access to Justice” in the context of older persons.⁵⁵ Based on the contributions received, the bureau of the working group, through OHCHR and the Department of Economic and Social Affairs, prepares an analytical discussion paper to guide each interactive discussion on the focus areas, making a summary of the contributions and highlighting areas of common ground and trends identified in the responses to the questionnaires.

Continuous multistakeholder dialogue. There are several variations to the program according to the relevant issues identified each year; however, the emphasis on a multistakeholder approach is consistently at the forefront of the Group’s work. For instance, in the tenth session of the Working Group, held in 2019, each debate was preceded by a panel discussion featuring presentations by a variety of stakeholders providing insights from different perspectives, such as the human rights treaty body system, current international human rights law, national and regional experiences, the specific human rights mandates and the national human rights institutions. Additionally, each panel was followed by an interactive discussion involving all stakeholders, guided by the discussion papers prepared by OHCHR and the Department of Economic and Social Affairs, which summarized the main trends and areas of common ground to emerge from the input received prior.

The level of transparency in the process and openness of the Group, where relevant NGOs besides those with ECOSOC status can apply for accreditation, as well as the possibility for NGOs to provide input at different stages of the discussion and decision-making process, ensure a larger and more constructive pool of potential voices in the

discussions, allowing for a wide array of interests and perspectives to be taken into consideration. While the OEWG Group on aging concerns itself with a very different thematic area from that of cyberspace, and sets out to address very different challenges, the general principles described above, such as transparency and openness, will remain just as relevant in setting up any multistakeholder initiative on cybersecurity.

5.5 Ad-hoc Open-Ended Working Group “Towards a Global Pact for the Environment” - (Direct Participation)

The Global Pact for the Environment was launched in 2017 to establish a legally binding international instrument under the UN that synthesizes the principles outlined in various agreements to solidify the environmental rule of law around the world and to achieve the 2030 Agenda for Sustainable Development, including the Stockholm Declaration, the World Charter for Nature, the Rio Declaration, the IUCN World Declaration on the Environmental Rule of Law, and other instruments.⁵⁶ Resolution 72/277 “Towards a Global Pact for the Environment” of May 2018 created an Ad-Hoc Open Ended Working Group (AHWG) to discuss options to address gaps in international environmental law and related instruments and present its recommendations to the General Assembly during the first semester of 2019.⁵⁷

The Working Group embraces a multistakeholder approach, opening up participation to accredited NGOs working in sustainable development. Some modalities which are important to highlight include:

Accreditation/requirements for participation.

ECOSOC accredited NGOs were allowed to attend sessions of the ad-hoc OEWG as observers. Additionally, other NGOs accredited to relevant conferences and summits were allowed to attend these: the United Nations Conference on Environment and Development; the World Summit on Sustainable De-

⁵⁵United Nations Department of Economic and Social Affairs, “United Nations Open-Ended Working Group on Strengthening the Protection of the Human Rights of Older Persons” (social.un.org) <<https://social.un.org/ageing-working-group/eleventhsession.shtml>>.

⁵⁶United Nations General Assembly, “Report of the Secretary-General – Gaps in International Environmental Law and Environment-Related Instruments: Towards a Global Pact for the Environment” (2018) <https://wedocs.unep.org/bitstream/handle/20.500.11822/27070/SGGaps.pdf?sequence=3&isAllowed=y>.

velopment; the United Nations Conference on Sustainable Development, and the United Nations summit for the adoption of the post-2015 development agenda.⁵⁸

Input to the sessions. NGOs were permitted to speak after delegate statements during the “informal dialogue” portion of the sessions. At this point, NGOs delivered joint statements and spoke individually. Accredited NGOs could attend the formal meetings of the group, receive copies of the official documents, and make their materials available to delegates. NGOs were active participants, particularly in the second and third substantive meetings, which took place in March and May 2019, respectively. On these occasions, NGOs met with states and regional groupings, and collaborated on joint statements.

Despite the slow progress of its proceedings, the Working Group “Towards a Global Pact for the Environment” represents a valuable example of multistakeholder participation. The Working Group allows potential civil society beneficiaries of the Global Pact on the Environment the opportunity to get involved throughout the decision-making process and have a say on matters that would concern them directly. For instance, the Group invites environmental protection NGOs, which could be empowered by any new legal guarantees enshrined in the Pact when asserting environmental rights in a court of law, to provide their input to the discussions. Just as important, the Working Group establishes clear avenues for NGOs to obtain accreditation and take part in the working sessions, permitting them to offer their expertise at every stage of the process. Drawing a parallel to the field of cybersecurity, one lesson to be drawn from the workings of this group would be the importance of involving, for instance, entities representing the victims of cybersecurity attacks, including private sector and civil society groups, in any multistakeholder dialogue on the matter.

5.6 United Nations Development Programme Civil Society Advisory Committee - (Advisory Body)

More structured mechanisms for multistakeholder participation in UN dialogues and policymaking can be observed in discussions on human rights and development. In May 2000, the United Nations Development Programme (UNDP), which promotes technical and investment cooperation among nations, established the UN Civil Society Advisory Committee (CSAC), an institutional mechanism for dialogue between civil society leaders and UNDP senior management. The establishment of CSAC systematized the consultation process between the UNDP and civil society actors and strengthened the overall civic engagement dimension of the UNDP’s policies and programs by providing independent prospective and critical analyses of the organization’s work.⁵⁹ Among its modalities, we can observe:

- **Composition.** CSAC members include global leaders, who are authoritative voices in UNDP thematic areas of focus such as governance, human rights, poverty reduction, conflict prevention and peacebuilding, environment and gender. The geographic provenience and gender of members is considered at selection.
- **CSAC input and involvement.** The CSAC’s specific objectives include providing substantive inputs, developing UNDP strategies and policies, advising the UNDP on different aspects of its work to promote civic engagement, supporting UNDP outreach and partnership development efforts, and joining hands with UNDP Advocacy efforts on matters of shared concern. Beyond their consultative role, members contribute to UNDP activities as event speakers, organizers of joint member events, or developing messaging on emerging issues.
- **Meetings.** The CSAC meets annually at the UN Headquarters in New York and is supported by a secretariat based in the Inclusive Political

⁵⁷Ibid.

⁵⁸Global Partners Digital, “NGO Participation in Multilateral and Multistakeholder Forums: Good Practice Examples” (2020) https://www.gp-digital.org/wp-content/uploads/2020/06/ngo-participationgoodpractice_gpd.pdf.

⁵⁹United Nations Development Programme, “UNDP’s Civil Society Advisory Committee Operating Framework” (2016) <https://www.undp.org/sites/g/files/zskgke326/files/2021-04/CSAC%20Operating%20Framework.pdf>.

Processes Team of UNDP's Governance and Peacebuilding Cluster. Among other tasks, the secretariat facilitates communication between UNDP's senior management and the Committee's Co-Chairs, and drafts the Annual Meeting agenda, final report and monitoring of recommendations.⁶⁰

In 2015, CSAC's structure was examined, and in 2016, the UNDP published a CSAC operating framework which included six considerations and lessons learned⁶¹:

- The committee members' substantive expertise must be fully leveraged to ensure CSAC's success.
- Adequate space and time must be allocated for in-depth discussion and engagement on issues.
- As follow-ups shape the quality of the interaction between UNDP and the Committee, a strong mechanism to track organizational progress on CSAC recommendations will be critical.
- CSAC's reach should be enhanced by expanding opportunities for interaction with regionally focused parts of UNDP (i.e., Regional Bureau and Regional Hubs).
- CSAC engagement should be expanded beyond Annual Meetings.
- Appropriately combining the engagement of the entire Committee on cross-functional strategic matters while leveraging the thematic expertise and experience of selected members on more focused initiatives.

These takeaways offer valuable insights into ensuring meaningful multistakeholder participation in the executive decision-making level of UN processes. The recommendation of establishing a mechanism to track decisions and proposals made by the stakeholder groups is of particular

importance. In the case of the UNDP, a secretariat facilitates the mechanism, which directly assists the CSAC in its advisory role supporting the UNDP's Executive Managers. Such a structure ensures that recommendations made by third parties are taken into consideration and acted upon by the UNDP.

5.7 United Nations Women Organization Civil Society Advisory Groups - (Advisory Body)

Similar to the modality of the UNDP's CSAC, we can observe another structured way to include multistakeholder voices in UN policymaking through the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women). Since its establishment in 2010, UN Women has been active in empowering local voices across the globe on issues of political participation, economic empowerment, ending violence against women, and peace and security. The organization features a strong multistakeholder dimension, which has led to the establishment of Civil Society Advisory Groups (CSAG) to act as consultative bodies for regular dialogue on policy issues, and on the programming of normative, intergovernmental and operational activities.

The Global Advisory Group was established in 2012 by former UN Women's Executive Director Michelle Bachelet as a consultative forum and platform for regular dialogue with civil society. The Global CSAG enables the Executive Director to consult with its 25 members, including leading feminists and gender equality advocates. Civil Society Advisory Groups are established at the national and regional level based on local priorities and practices, under the broad guideline of "creating a just, balanced and effective body," where different groups maintain contact through a web-based platform. CSAGs are an institutional mechanism for regular dialogue, between UN Women and leaders from the gender equality movement, on key gender equality issues and priorities at national, regional and global levels.⁶² As of 2021, 38 CSAGs are active across the globe, ranging from

⁶⁰United Nations Development Programme, "UNDP's Civil Society Advisory Committee (CSAC) Procedure" <https://www.ohchr.org/Documents/AboutUs/CivilSociety/Procedures/UN/UnitedNationsDevelopmentProgramme.pdf>.

⁶¹United Nations Development Programme, "UNDP's Civil Society Advisory Committee Operating Framework" (2016) <https://www.undp.org/sites/g/files/zskgke326/files/2021-04/CSAC%20Operating%20Framework.pdf>.

⁶²UN Women, "Civil Society Advisory Groups - CSAG Strategy" (2015) <https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2016/civil-society-advisory-groups-strategy-en.pdf?la=en&vs=2147>.

regional groups like the Western and Central Africa CSAG or the Arab States CSAG, to national entities in Malawi or Paraguay. The following principles apply to setting up the groups:

Participation: The advisory groups need reputable individuals committed to the UN's core values, preferably with strong credentials as gender, development and/or human rights advocates. Participants should possess expertise in one or more of UN Women's priority areas and represent diverse developmental and human rights perspectives and should be drawn from gender equality networks, women's and grassroots organizations, development and social policy think tanks and academia.

Conflicts of Interest: Members take part in advisory groups in their personal capacities for a fixed period on a renewable basis, and their membership is rotational. CSAG participants may belong to organizations that are implementing partners of UN Women. However, the goal must be to avoid any conflicts of interest. Hence, the CSAGs should not have any oversight, monitoring or decision-making role in UN Women programming activities.

The UN Women Civil Society Advisory Groups identify areas in which each civil society stakeholder can contribute and integrates these voices into the multistakeholder framework according to their subject matter expertise. Additionally, to ensure that civil society actors with technical expertise can contribute efficiently, UN Women enables a structured participation process by organizing several civil society advisory groups with a narrower focus. The establishment of these groups strengthens leaders' voices from grassroots institutions, rural and community-based groups, and indigenous organizations, scholars, activists and male advocates for gender equality and women's rights. To successfully draw lessons from the workings of this group, any multistakeholder initiative on cybersecurity would do well to determine the expertise of each relevant group (private compa-

nies, governments etc.) to efficiently involve them in the discussion.

5.8 United Nations High Level Meeting on HIV/AIDS - (Multistakeholder Consultative Session)

Recognizing the need to address the persisting global health challenge represented by AIDS, the UN General Assembly adopted in 2021 resolution 75/260⁶³, through which a high-level meeting (HLM) on human immunodeficiency virus (HIV) and acquired immunodeficiency syndrome (AIDS) was convened. A United Nations High-Level Meeting (UN HLM) is convened by the UNGA as a forum for UN member states to discuss and work together on a wide array of international issues covered by the UN Charter, such as development, peace and security, international law, etc. Agreement to hold a dedicated UN HLM on a specialized topic is taken in exceptional circumstances through a UN resolution, to reach an agreement on cooperation measures and solutions on important global issues among Heads of State and governments.⁶⁴ The HLM on HIV/AIDS facilitated a comprehensive review of the progress made on the commitments in the 2016 Political Declaration towards ending the AIDS epidemic by 2030. Further, participants examined how the social, economic and political response contributes to progress on the 2030 Agenda for Sustainable Development and the global health goal. The meeting provided recommendations to guide and monitor the HIV/AIDS response beyond 2021, including new concrete commitments to accelerate action and promote renewed commitment and engagement from leaders, countries, communities and partners to accelerate and implement a comprehensive universal and integrated response to HIV/AIDS.

To prepare for the HLM, an interactive multistakeholder hearing took place with support from the Joint United Nations Programme on HIV/AIDS. Several groups participated, including those living with, at risk of or affected by HIV, including key populations, representatives of member states and observers of the General Assembly, parlia-

⁶³United Nations General Assembly, "Resolution Adopted by the General Assembly on Implementation of the Declaration of Commitment on HIV/AIDS and the Political Declarations on HIV/AIDS" <https://undocs.org/en/A/RES/75/260>.

⁶⁴UHC30, "UN HLM FAQs" (UHC2030) <https://www.uhc2030.org/un-hlm-2019/un-hlm-faqs/>.

mentarians, representatives of local governments, and civil society organizations, including non-governmental organizations in consultative status with the Economic and Social Council, philanthropic foundations, academia, medical associations, and the private sector.

The interactive hearing provided all relevant stakeholders with an opportunity to contribute through these interactive panel discussions. During the group discussions, civil society representatives and other stakeholders shared their views and experiences from their work on the ground, including lessons learned, obstacles, gaps, challenges and opportunities, which actively informed the negotiations of the HLM declaration.

5.9 ECOSOC Partnership Forum - (Multistakeholder Consultative Session)

The UN's Economic and Social Council's (ECOSOC) Partnership Forum is an annual event that provides a policy space for member states, non-governmental stakeholders and the UN development system to discuss the role of partnership in driving sustainable development across the globe. The 2030 Agenda for Sustainable Development identified partnerships as an essential tool to achieve the UN's Sustainable Development Goals (SDGs). The Partnership Forum is organized by ECOSOC to showcase how inclusive multistakeholder partnerships and partnership platforms can help achieve these goals. The event is a two-hour session, opened by a keynote to set the stage for the discussions, followed by a substantive interactive dialogue session where member states and other stakeholders can contribute by making statements. The discussion is followed by a closing statement.

The 20th ECOSOC Partnership Forum was held online in May 2021, after a hiatus due to the COVID-19 pandemic. Titled "Partnerships as Game Changer for a Sustainable Recovery from COVID-19," the meeting focused on discussing the critical role of multistakeholder partnerships in achieving the UN's Sustainable Development Goals following the outbreak of the COVID-19 pandemic, as well as their role in helping societies rebuild. This year, participants discussed how multistakeholder partnerships could support COVID-19 recovery, particularly to reverse the increase in extreme poverty and enhance social

protection. Further, they discussed ways the scientific and technological communities can help accelerate systemic change, promoting equal access and the right to development for all.

The 2021 session was attended by participants including representatives of member states, UN system entities, relevant inter-governmental organizations, multilateral development banks, NGOs, the private sector, think-tanks and scientific communities, philanthropic organizations, local governments, parliaments, academia and other stakeholders. Overall, the discussion highlighted that:

- Key determinants for successful multistakeholder partnerships lie in the capability of partners to add value and advance collective objectives.
- Multistakeholder partnerships should enhance accountability and transparency through effective data collection and management at all levels.
- To build data-driven and results-focused multistakeholder partnerships, collaborators should agree on monitoring and evaluation frameworks.
- The UN has a critical role to play in facilitating the shift towards more measurable, comparable and transparent frameworks and means of environmental, social, and corporate governance factors (ESG) at the global level.
- As the alignment of interests among partners within public-private partnerships (PPPs) is often challenging, given the interests of the public and private sectors may diverge between purpose and profit, all actors involved should agree upon concrete ways to share the risks and benefits of PPPs fairly.
- In order to meet the challenges facing the world today, multistakeholder partners should come together to invoke broader and more inclusive coalitions.
- Participants stressed the critical role that multistakeholder partnerships can play in mobilizing not only finance, but also science, technology and innovation in support of sustainable recovery and development.

ECOSOC's yearly Partnership Forum is not only a very productive way to include multistakeholder voices in the UN work towards achieving the 2030 Sustainable Development Goals, but the event itself also acts as a forum promoting multistakeholderism overall. Multistakeholder partnerships are praised for "clearly making a positive impact

on sustainable recovery and development and should be considered a key instrument for building back better, faster and fairer." Perhaps most important is the first point: the importance of including partners capable of adding value and advancing collective objectives.

Analysis of Case Studies

The above section took nine different modalities for multistakeholder participation in UN governance and policymaking into consideration. The first two examples: the UN PoA on Small Arms and Light Weapons (5.1) and the Open-Ended UN GGE on Lethal Autonomous Weapons Systems (5.2), highlighted UN fora where the participation of the multistakeholder community is recognized and considered necessary due to the nature of the First Committee's work on disarmament. The technical expertise required to address disarmament at the global level ensures that civil society, academia and the private sector are directly included in the participation of these discussions. Example 5.3 provides an overview of the IGF, an ICT-specific multistakeholder forum where states, industry and civil society can discuss internet governance and where the input of non-state actors is encouraged, as they are recognized as key players in the wider ecosystem of the internet. These examples were in the First Committee processes or directly related to internet governance, but other UN processes provide food for thought on the ways to ensure greater multistakeholder inclusion than has been the case in UN cybersecurity dialogues.

The UN Working Group on Ageing (5.4) and the Open-Ended Working Group Towards a Global Pact for the Environment (5.5), represent structured direct participation forums where a wide range of voices, from accredited to non-accredited NGOs, civil society groups and other third-party stakeholders, can feed into UN discussions at major UN Conferences. This modality allows interested groups to sit at the table with representatives of UN members, exchange ideas and provide input on influential UN decisions. Examples 5.6 and 5.7: the Civil Society Advisory Groups from UN Women and the UNDP, present a different, but still structured way in which grassroots groups and civil society organizations can feed into the work of the UN in a consultative way. The boards advising the leadership of UN Women and the UNDP are very influential in their advocacy, and while the members of the advisory boards act as independent consultants and not on behalf of their own interest groups, these structures can steer the management of large UN Bodies, influencing the direction and focus of their work. The final two examples: UN High-Level Meeting on HIV (5.8) and the yearly ECOSOC Partnership Forum (5.9), represent another great model of multistakeholderism in action.

While none of these models provides a definitive template for multistakeholder participation in UN processes, each offers a useful example of how third-party actors can be included in conversations in fields ranging from healthcare to the environment in a way that enriches discussions and benefits all parties involved.

6. Recommendations for Meaningful Multistakeholder Participation in the UN Cybersecurity Dialogues

The history of multistakeholder inclusion in political discussions on critical issues demonstrates that involving different stakeholders in cybersecurity dialogues is both viable and vital given the value, perspectives and expertise industry, civil society and academia bring to bear. The experience gained in other UN formats also shows that meaningful multistakeholder participation requires consistent effort by all actors to communicate and exchange information as well as clear mechanisms for input and participation. The invaluable input provided by non-governmental organizations and industry, as well as other stakeholders in the format of the WG3 sessions held throughout 2021, and the evidence that emerged from this research, helped us identify seven principles for meaningful multistakeholder participation in UN cybersecurity dialogues. Overall, it is critical that a new process for multistakeholder participation in the UN negotiations on cybersecurity is designed to confirm that such participation is: i) well-structured, to ensure that it is helpful and constructive; ii) regular, to reflect the evolving nature of cyberspace and the cyber threat landscape, and iii) systematic, rather than ad hoc. Specifically, it will be important to:

1. Establish an inclusive accreditation process.

So far, participation in some of the OEWG meetings has been restricted to NGOs with ECOSOC status. This means that numerous stakeholders in fields ranging from the private sector to civil society and academia with relevant experience have been consistently denied access to the discussions. It is pivotal to establish a flexible accreditation system that ensures participation of all relevant entities that can contribute valuable input and expertise to UN member states on these

matters. A system allowing non-governmental organizations to voice their interest in participating in the discussions on an ongoing and systematic basis would ensure that all views and interests are represented.

2. Promote a regular, interactive dialogue.

It is key to engage stakeholders throughout a process in a systematic way in order to have meaningful engagement and develop trust and a cooperative dynamic among all participants. This is particularly important considering cybersecurity is a rapidly evolving area, where pockets of expertise can emerge rapidly in response to dynamic events. The fast evolution of the threat environment and of the technological solutions to address these challenges calls for close cooperation to ensure that the discussions reflect the reality of the security environment. One-off exchanges, such as the consultative session that the OEWG organized in December 2019, are helpful to gain insight into different stakeholders' perspectives and to gather high-level input on the main areas of work. However, they are not sufficient on their own to explore complex matters such as those related to international obligations for states in cyberspace, or to allow for the development of coherent positions on these matters. Regular, interactive dialogues allow for more fruitful discussions and can better promote progress.

3. Ensure timely sharing of information.

Transparency needs to be at the center of all UN discussions on cybersecurity. Timely sharing of documents, agendas, and information is the baseline on which effective multistakeholder cooperation can be built as it ensures that stakeholders are informed and can meaningfully participate.

Such sharing of information can be facilitated by the deployment of online tools. The United Nations Office for Disarmament Affairs (UNODA) has made full use of technological means as part of the previous OEWG, and this should be looked at as a good practice to replicate in upcoming UN dialogues on cybersecurity and other topics. We hope that UNODA builds on those efforts, enhances its existing platform, and continues to publish information around the ongoing process, as soon as possible. The types of information that can be made public should include (though not be limited to):

- Meeting agendas,
- Official documents produced by the secretariat,
- Official communication to states,
- Individual submissions by states or non-governmental actors to the ongoing dialogue, and
- Contact details of the secretariat.

4. Establish mechanisms for stakeholders to provide input and support entities to help process that input.

In addition to ensuring that relevant discussion documentation is shared with the multistakeholder community, and that meaningful access is given to deliberations, it is important to set up mechanisms to allow representatives of non-governmental organizations to provide input, in-person and in writing, to meetings and working documents. The 2018-2021 OEWG on cybersecurity has worked toward ensuring that happened. Submissions by non-governmental entities were published to the UNODA website and the secretariat regularly informed state representatives of this input. Such a system could be improved upon by ensuring there is clarity regarding the documents that are open for consultation and the deadlines to provide input. To ensure transparency, the modalities used by stakeholders to participate should be agreed upon in advance. In addition, given the

many varied contributions offered, both verbal and written, a synthesis of the statements before producing a final report could be useful for identifying areas where states and other stakeholders agree, not only on positions but also in terms of what and how additional research and work needs to be done. This could help provide insights into alternative paths forward and promote progress. Entities such as the UN Institute for Disarmament Research or independent NGOs could be asked to take on various tasks like these.

5. Hold hybrid or virtual meetings/consultations in addition to in-person ones.

While in-person meetings can be more fruitful in establishing relationships, negotiating details, and building consensus, virtual meetings also have their benefits. They can be more inclusive of non-governmental organizations that do not have representation in, or the budget to travel to, New York. For live events, it is important that all formal meetings are live-streamed, recorded, and published on the relevant UNODA website and that virtual meetings are organized to ensure the participation of a broader group of stakeholders than in-person meetings would allow. As far as virtual or hybrid meetings are concerned, stakeholders should be offered the necessary technical support and information, such as the links to participate remotely.⁶⁵ In addition, for live online events, virtual break-out groups can be used to help establish the relationships that are typically developed from in-person meetings

6. Explore different models and leverage relevant venues for multistakeholder participation.

In addition to the systematic inclusion of multistakeholder representatives, states should deepen that relationship by considering other models that could increase the exchange of views between and among the different stakeholder groups. The models that could be considered include:

- Organization of formal side events, such as intersessional discussions, with the modalities for participation agreed upon in advance;

⁶⁵Women's International League for Peace & Freedom, "Locked Out During Lockdown, An Analysis of the UN System During COVID-19." (2020) <https://www.wilpf.org/wp-content/uploads/2020/09/un-system-analysis-covid-1.pdf>.

- Regular engagement of groups of stakeholders, such as with the private sector through, for example, the Private Sector Forum/UN Global Compact,⁶⁶ the SDG Business Forum,⁶⁷ or other entities, perhaps even newly developed ones, if required, and with other established multistakeholder forums;
- Creation of “leadership dialogues,” bringing together relevant ministers, and leaders of business and civil society for interactive discussions and an exchange of views on priorities, best practices, challenges, etc., modeled on the work done by the UN Environment Assembly;⁶⁸
- Organization of a dedicated summit on the topic, possibly modeled on the Climate Action Summit.⁶⁹

7. Beyond the UN discussions: Foster multistakeholder engagement to drive implementation of international agreements.

While it is critical to focus on multistakeholder participation during UN negotiations to agree on the rules and norms of responsible behavior in cyberspace, transparency and inclusion of different perspectives will be equally important in discus-

sions about their application and in the implementation process itself. Regional organizations will also be key to this process and help states identify common areas of work and mutual support, so it will be important for these organizations to foster multistakeholder inclusion in discussions at the regional level. At the international level, initiatives such as the Paris Call for Trust and Security in Cyberspace have so far been pivotal in fostering dialogue about principles for peace and stability in cyberspace and on the ways to translate these principles into concrete actions. It will be important to leverage the Paris Call community and take advantage of the synergies and cooperative structures that have emerged among the Paris Call supporters in past years, including through working groups such as WG3. With sufficient support, these communities can help develop and support action agendas for enhanced peace and security in an expanded, more robust, and inclusive cyberspace.

The participation of non-governmental actors in the UN negotiations on cybersecurity would greatly benefit from such a structured approach as clearer modalities for their inclusion would help make the dialogues both more efficient and effective.

⁶⁶United Nations Secretary-General, “Secretary-General’s Video Remarks to the Private Sector Forum | United Nations Secretary-General” (www.un.org/September 21, 2020) <https://www.un.org/sg/en/content/sg/statement/2020-09-21/secretary-generals-video-remarks-the-private-sector-forum>.

⁶⁷SDG Business Forum, “Home” (SDG Business Forum 2020) <https://www.sdgbusinessforum.org/>.

⁶⁸United Nations Environmental Programme, “Private Sector Engagement at the 2019 UN Environment Assembly” <https://wedocs.unep.org/bitstream/handle/20.500.11822/29499/Private%20Sector%20Engagement%20at%20the%202019%20Assembly.pdf?sequence=1&isAllowed=y>.

⁶⁹United Nations, “Climate Action” (United Nations) <https://www.un.org/en/climatechange>.

7. Conclusions

This study is the product of informal consultations between governments, industry, civil society and academia on how to advance multistakeholder participation in the UN dialogues on cybersecurity. Its publication comes at a time when the need to clarify states' obligations in cyberspace is more pressing than ever, with tensions between states in this new domain escalating at an unprecedented rate. It is critical for the international community to advance discussions on how to ensure an open, secure, stable and rights-respecting online environment.

As section 4 explored, thus far the UN dialogues on cybersecurity have been largely exclusively open to states, and often a limited number of states. While attempts to codify international cybersecurity frameworks have been steadily intensifying since the early 2000s, multistakeholder inclusion in cybersecurity discussions has been noticeably absent. With the exception of the consultative session as part of the 2019-2021 OEWG, and the regional consultations held as part of the 2019-2021 GGE process, the voices of non-governmental actors including industry, civil society and academia have been largely absent in official processes. Such an approach is in sharp contrast with the UN's long history of multistakeholder participation in other dialogues, as illustrated in section 5, and, more generally, with the tradition of a multistakeholder model in internet governance.

The UN's long history of inclusion of third parties in its decision-making processes is rooted in its understanding that the involvement of all relevant voices in global policymaking is key to achieving change and progress and ensuring the legitimacy of global agreements. Processes in the UN's First Committee, like the United Nations Program of Action on Small Arms and Light Weapons (UN PoA SALW) and the Open-Ended UN Group of Governmental Experts on Lethal Autonomous Weapons, show that involving local civil society groups as well as researchers and experts on highly technical issues can bring positive outcomes in

the field of peace and security. In the health space, the Open-Ended Working Group on Ageing is an example of transparent and open third-party participation: the ability of both ECOSOC and non-ECOSOC status organizations to participate in the Working Group provides for a wide array of interests and perspectives to be taken into consideration and to produce better outcomes. The more structured, consultative roles of the Civil Society Advisory Groups, both at the United Nations Development Programme and United Nations Women Organization, provide these organizations with meaningful, transparent and conflict-free multistakeholder participation in the executive decision-making level of UN processes. Finally, multistakeholder fora like the Internet Governance Forum, United Nations High Level Meeting on HIV/AIDS, and the ECOSOC Partnership Forum, are useful examples of engaging the wider multistakeholder community in international discussions.

Establishing clear modalities for industry, civil society and academia participation in UN cyber dialogues is essential to ensuring relevance to the evolving threat environment and the success of future negotiations. Section 6 highlights seven recommendations to ensure more inclusive and efficient participation from the multistakeholder community in these discussions:

1. Establish an inclusive accreditation process.
2. Promote a regular, interactive dialogue.
3. Ensure timely sharing of information.
4. Establish mechanisms for stakeholders to provide input and support entities to help process that input.
5. Hold virtual meetings and consultations in addition to in-person ones.
6. Explore different models of and leverage relevant venues for multistakeholder participation.

7. Beyond the UN discussions, foster multistakeholder engagement to drive implementation of international agreements

As calls from the multistakeholder community to be involved in governance at the international level grow louder, one thing is becoming clear: the growing field of multistakeholderism deserves

more attention from policymakers and international organizations because of its potential to ensure greater representation in discussions impacting our societies. Progress toward an expanded, inclusive cyberspace that is peaceful and secure can only be achieved by engaging not only states but also the range of critically affected stakeholders.

Further Research

The study does not provide an answer to all questions concerning multistakeholder inclusion in UN cybersecurity dialogues. More questions remain, including to what extent non-governmental stakeholders' views were integrated into the OEWG and UNGGE final reports. In addition, it would be worthwhile to understand whether and to what extent the outcomes of these processes would have been different if multistakeholder voices were included more regularly and consistently. With those and other questions in mind, we hope that this report will serve not only as a valuable reference point in structuring upcoming dialogues at the UN, but also open the door to further research to strengthen the impact of cooperative multistakeholder models to promote a free, open and secure online world for all.

Bibliography

1. Alger C, "The Emerging Roles of NGOs in the UN System: From Article 71 to a People's Millennium Assembly" (2002) 8 *Global Governance: A Review of Multilateralism and International Organizations* 93 <https://www.jstor.org/stable/27800329?seq=4#metadata_info_tab_contents>
2. Breene K, "Who Are the Cyberwar Superpowers?" (World Economic Forum May 4, 2016) <<https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>>
3. Buxton N, "Multistakeholderism: A Critical Look" (Transnational Institute September 10, 2019) <<https://www.tni.org/en/publication/multistakeholderism-a-critical-look>>
4. Council on Foreign Relations, "From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity" (Council of Foreign Relations Blog January 27, 2020) <<https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity>>
5. Cybersecurity Tech Accord, "Cybersecurity Tech Accord Discusses Threat Posed by State-Sponsored Cyberattacks and the Importance of Cooperation during RightsCon 2021" (Cybersecurity Tech Accord July 13, 2021) <<https://cybertechaccord.org/cybersecurity-tech-accord-discusses-threat-posed-by-state-sponsored-cyberattacks-and-the-importance-of-cooperation-during-rightscon-2021/>>
6. —, "Discussions on Cyberspace Security Need to Be More Inclusive, Says Paris Call Working Group" (Cybersecurity Tech Accord August 4, 2021) <<https://cybertechaccord.org/discussions-on-cyberspace-security-need-to-be-more-inclusive-says-paris-call-working-group/>>
7. —, "About the Cybersecurity Tech Accord" (Cybersecurity Tech Accord) <<https://cybertechaccord.org/about/>>
8. Cybersecurity Tech Accord and The Economist Intelligence Unit, "Securing a Shifting Landscape: Corporate Perceptions of Nation-State Cyber-Threats" (2021) <<https://cybertechaccord.org/uploads/prod/2021/02/eiu-cybersecurity-tech-accord-report.pdf>>
9. Digital Peace Now, "Multistakeholderism: What Is It and Why Does It Matter to International Peace and Stability Online?" (Digital Peace July 17, 2020) <<https://digitalpeacenow.org/multistakeholderism-what-is-it-and-why-does-it-matter-to-international-peace-and-stability-online/>> accessed August 26, 2021
10. —, "Multistakeholderism: What Is It and Why Does It Matter to International Peace and Stability Online?" (Digital Peace July 17, 2020) <<https://digitalpeacenow.org/multistakeholderism-what-is-it-and-why-does-it-matter-to-international-peace-and-stability-online/#:~:text=Multistakeholderism%20Defined>> accessed September 15, 2021
11. France Diplomacy - Ministry for Europe and Foreign Affairs, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace" (France Diplomacy - Ministry for Europe and Foreign Affairs) <<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>>
12. France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States, "The Future of Dis-

- cussions on ICTs and Cyberspace at the UN" (2020) <<https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf>>
13. Gavrilovic A, "A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers" (DiploMarch 18, 2021) <<https://www.diplomacy.edu/blog/new-landmark-global-cybersecurity-negotiations-un-cyber-oewg-numbers>> accessed September 15, 2021
 14. GGE on Advancing responsible State behaviour in cyberspace in the context of international security, "Report of the GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (2021) <<https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>>
 15. Global Partners Digital, "NGO Participation in Multilateral and Multistakeholder Forums: Good Practice Examples" (2020) <https://www.gp-digital.org/wp-content/uploads/2020/06/ngo-participationgoodpractice_gpd.pdf>
 16. Henriksen A, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace" (2019) 5 *Journal of Cybersecurity* <<https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865>> accessed November 8, 2020
 17. International Action Network on Small Arms, "Seventh Biennial Meeting of States on the United Nations Programme of Action on Small Arms (BMS7)" (IANSA April 10, 2021) <<https://iansa.org/seventh-biennial-meeting-of-states-on-the-united-nations-programme-of-action-on-small-arms/>>
 18. —, "What We Do" (IANSA) <<https://iansa.org/what-we-do/>> accessed August 27, 2021
 19. Kumar S, Brown D and Esterhuysen A, "Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms" (December 2019) <https://www.gp-digital.org/wp-content/uploads/2019/12/unpacking_gge_cyber-norms.pdf>
 20. Lin H, "Cyber Conflict and International Humanitarian Law" (2012) 94 *International Review of the Red Cross* 515 <<https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf>> accessed July 7, 2020
 21. Manantan MBF, "Defining Cyber Diplomacy" (Australian Institute of International Affairs May 19, 2021) <<https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/>> accessed September 15, 2021
 22. Maurer T, "A Dose of Realism: The Contestation and Politics of Cyber Norms" (2019) 12 *Hague Journal on the Rule of Law*
 23. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), "Final Substantive Report" (2021) <<https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>>
 24. Oxford Institute for Ethics, Law and Armed Conflict, "The Oxford Process on International Law Protections in Cyberspace" (www.elac.ox.ac.uk) <<https://www.elac.ox.ac.uk/the-oxford-process-on-international-law-protections-in-cyberspace/#/>>
 25. Paris Call for Trust and Security in Cyberspace, "Paris Call for Trust and Security in Cyberspace — Paris Call" (pariscall.international) <<https://pariscall.international/en/>>
 26. Reaching Critical Will - Women's International League for Peace and Freedom, "Statements from the 2020 CCW Group of Governmental Experts on Lethal Autonomous Weapon Systems" (reachingcriticalwill.org September 21, 2020) <<https://reachingcriticalwill.org/disarmament-fora/ccw/2020/laws/statements>>
 27. Reuters, "SolarWinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President" Reuters (February 15, 2021) <<https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R>>
 28. SDG Business Forum, "Home" (SDG Business Forum 2020) <<https://www.sdgbusinessforum.org/>>

29. UHC30, "UN HLM FAQs" (UHC2030) <<https://www.uhc2030.org/un-hlm-2019/un-hlm-faqs/>> accessed September 15, 2021
30. UN Women, "Civil Society Advisory Groups - CSAG Strategy" (2015) <<https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2016/civil-society-advisory-groups-strategy-en.pdf?la=en&vs=2147>>
31. United Nations, "General Assembly Approves List of Civil Society Participants for June Hiv/Aids Special Session | Meetings Coverage and Press Releases" (www.un.org February 26, 2001) <<https://www.un.org/press/en/2001/ga9857.doc.htm>> accessed September 15, 2021
32. —, "UN General Assembly - First Committee - Disarmament and International Security" (Un.org2020) <<https://www.un.org/en/ga/first/>>
33. —, "Climate Action" (United Nations) <<https://www.un.org/en/climatechange>> accessed September 15, 2021
34. United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, "Provisional Rules of Procedure of the Conference" (2001) <<https://undocs.org/A/CONF.192/L.1>>
35. United Nations Congress on Crime Prevention and Criminal Justice, "Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation" <https://www.unodc.org/documents/congress/Declaration/V1504151_English.pdf>
36. United Nations Department of Economic and Social Affairs, "United Nations Open-Ended Working Group on Strengthening the Protection of the Human Rights of Older Persons" (social.un.org) <<https://social.un.org/ageing-working-group/>> accessed August 24, 2021
37. —, "United Nations Open-Ended Working Group on Strengthening the Protection of the Human Rights of Older Persons" (social.un.org) <<https://social.un.org/ageing-working-group/eleventhsession.shtml>>
38. United Nations Development Programme, "UNDP's Civil Society Advisory Committee Operating Framework" (2016) <<https://www.undp.org/sites/g/files/zskgke326/files/2021-04/CSAC%20Operating%20Framework.pdf>>
39. —, "UNDP's Civil Society Advisory Committee (CSAC) Procedure" <<https://www.ohchr.org/Documents/AboutUs/CivilSociety/Procedures/UN/UnitedNationsDevelopmentProgramme.pdf>>
40. United Nations Economic and Social Council, "ECOSOC Resolution 1296 (XLIV)" <<https://archive.globalpolicy.org/component/content/article/177-un/31832.html>>
41. —, "1993/80 Review of the Arrangements for Consultation with Non-Governmental Organizations" <<http://www.un-documents.net/1993-80.htm>>
42. —, "1996/31 Consultative Relationship between the United Nations and Non-Governmental Organizations" <<https://www.un.org/ecosoc/sites/www.un.org.ecosoc/files/documents/2020/resolution-1996-31.pdf>>
43. United Nations Environmental Programme, "Private Sector Engagement at the 2019 UN Environment Assembly" <<https://wedocs.unep.org/bitstream/handle/20.500.11822/29499/Private%20Sector%20Engagement%20at%20the%202019%20Assembly.pdf?sequence=1&isAllowed=y>>
44. United Nations General Assembly, "Report on the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security" (2011) <<https://undocs.org/A/RES/66/24>>
45. —, "Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security" (2015) <https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>

46. —, "Towards a Global Pact for the Environment" (2018) <https://wedocs.unep.org/bitstream/handle/20.500.11822/25982/UNGARES_72_277.pdf?sequence=1&isAllowed=y>
47. —, "Report of the Secretary-General - Gaps in International Environmental Law and Environment-Related Instruments: Towards a Global Pact for the Environment" (2018) <<https://wedocs.unep.org/bitstream/handle/20.500.11822/27070/SGGaps.pdf?sequence=3&isAllowed=y>>
48. —, "Resolution Adopted by the General Assembly on Implementation of the Declaration of Commitment on HIV/AIDS and the Political Declarations on HIV/AIDS" <<https://undocs.org/en/A/RES/75/260>> accessed September 15, 2021
49. United Nations Office on Drugs and Crime, "Toolkit on Stakeholder Engagement - Implementing the United Nations Convention against Transnational Organized Crime (UNTOC)" (2020) <<https://www.unodc.org/documents/NGO/SE4U/UNODC-SE4U-Toolkit-Interactive-WEB.pdf>> accessed September 15, 2021
50. United Nations Regional Centre for Peace and Disarmament in Asia and the Pacific, "Programme of Action - the United Nations Programme of Action on Small Arms and Light Weapons" (UNRCPD) <<https://unrcpd.org/conventional-weapons/poa/>>
51. United Nations Secretary General, "Secretary-General's Video Remarks to the Private Sector Forum | United Nations Secretary-General" (www.un.org September 21, 2020) <<https://www.un.org/sg/en/content/sg/statement/2020-09-21/secretary-generals-video-remarks-the-private-sector-forum>> accessed September 15, 2021
52. Wall Street Journal and others, "Cataloging the World's Cyberforces" (The Wall Street Journal December 28, 2015) <<http://graphics.wsj.com/world-catalogue-cyberwar-tools/>> accessed September 16, 2021
53. United Nations Convention Against Transnational Organized Crime and the Protocols Thereto 2000

Annex – WG3 Participants

1. Asia Society Policy Institute
2. Asociación Colombiana de Ingenieros de Sistemas
3. Association for Progressive Communications (APC)
4. Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT)
5. Broadband India Forum
6. Capgemini
7. Chatham House
8. Community Development Initiative
9. Consortium d'Appui aux Actions pour la Promotion et le Développement de l'Afrique (CAAPDA)
10. Cornerstone IT, Inc.
11. Cyber Defence Center of Portugal
12. Cyber Security Agency of Singapore
13. Defence Force of Zambia
14. Department for Digital, Culture, Media & Sport (DCMS), UK government
15. Dynamic Coalition on Internet Standards, Security and Safety (DC-ISSS)
16. DXC Technology
17. European Dialogue on Internet Governance (EuroDIG)
18. Global Affairs Canada
19. Global Commission on the Stability of Cyberspace (GCSC)
20. Global Cyber Alliance
21. Global Cyber Security Capacity Centre (GCSCC)
22. Global Forum on Cyber Expertise (GCSC)
23. Global Partners Digital
24. Globant
25. Independent Media Council, Ukraine
26. Institute for Peace Research and Security Policy
27. Institute for Security and Safety (ISS), Brandenburg University of Applied Sciences
28. International Chamber of Commerce (ICC) UK
29. Internet Society
30. Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
31. Kaspersky
32. Lumen
33. Microsoft
34. Ministry of External Relations of Cameroon
35. Ministry of Foreign Affairs of Estonia
36. Ministry of Foreign Affairs of Mexico
37. Ministry of Foreign Affairs of Russia
38. Ministry of Transport and Communications of Botswana
39. Mission of Colombia to the OAS
40. NEC Corporation
41. Observer Research Foundation (ORF) America
42. onShore Security
43. Organization of American States (OAS)
44. Panasonic
45. Permanent Mission of Australia to the United Nations
46. Permanent Mission of Lebanon to the United Nations
47. Permanent Mission of the Republic of Slovenia to United Nations

48. Professional Options LLC
 49. Raiffeisen Switzerland
 50. Rajartnam School of International Studies (RSiS)
 51. Safe PC Cloud
 52. School of International Service (SIS)
 53. Stanford Global Digital Policy Incubator (GDPI)
 54. Stimson Center
 55. Strong Connexions
 56. Tehran University
 57. The CyberPeace Institute
 58. The Fletcher School, Tufts University
 59. The Hague Center for Strategic Studies (HCSS)
 60. The Organization for Security and Co-operation in Europe (OSCE)
 61. OSCE Office for Democratic Institutions and Human Rights
 62. University of Bath
 63. University of KwaZulu-Natal
 64. University of Montenegro
 65. United Nations University Institute in Macau
 66. Validy Net Inc
 67. Wallencore, Inc.
 68. Yes We Hack
 69. Zambia Police Service
-

