THIRD SUBSTANTIVE SESSION OF THE UNITED NATIONS' OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Written contribution from the Paris Peace Forum

POLICY BRIEF | JULY 2022

PARIS PEACE FORUM de PARIS sur la PAIX

THIRD SUBSTANTIVE SESSION OF THE UNITED NATIONS' OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Written contribution from the Paris Peace Forum

Innovation in information and communication technologies (ICTs) have brought major opportunities for innovation, economic progress, cultural development, and access to information around the Globe. But with the rapid development of cyberspace, new, evolving threats to both public and private actors have emerged with critical risks for our collective security on- and offline. Normative uncertainty concerning the rights and responsibility of States is further complicating initiatives to cope with these emerging risks.

Following the rapid development of ICTs, successful negotiations have been conducted at the United Nations since 2004 towards a common understanding of responsible State behavior in cyberspace in the context of international security. Discussions in the framework of the 2021-2025 Open-Ended Working Group (OEWG) on security of and in the use of ICTs will be even more crucial to ensure the stability of cyberspace as it comes at a time of rising tensions in cyberspace. Proliferation of malicious activities and risks of extreme militarization of cyberspace should be a wake-up call for all States to ensure our collective security online, as they did in the physical world in the framework of the United Nations over the last 70 years.

The Paris Peace Forum has been working closely with stakeholders across the ICT value chain and beyond the industry to support these efforts and to improve the

stability of cyberspace in the framework of the Paris Call for Trust and Security in Cyberspace. Since 2018, the Paris Call has been gathering more than 1200 actors, including 80 Governments, 700 companies and 350 organizations from the civil society around 9 core principles to protect the open, free, and secure internet and to ensure better collaboration among all actors, whether public or private, to make cyberspace more secure and stable.

Close cooperation between public, private and non-profit actor is indeed not only key to defining relevant and adequate norms to secure cyberspace, but also to the actual implementation of most principles, rules or standards which can be agreed upon by States. The expertise of companies, civil society organization and academia is essential to inform Governments in how best to promote international security in cyberspace, but also to foster public scrutiny necessary to reward responsible behavior and deter malicious activities.

The Paris Peace Forum commends participating States to the OEWG on security of and in the use of information and communications technologies to have welcomed contributions from stakeholders to support their work during this third substantive session. Further extension of stakeholders' participation can only improve the precision and range of information received by States and thus be profitable to the substance of intergovernmental talks and agreements.

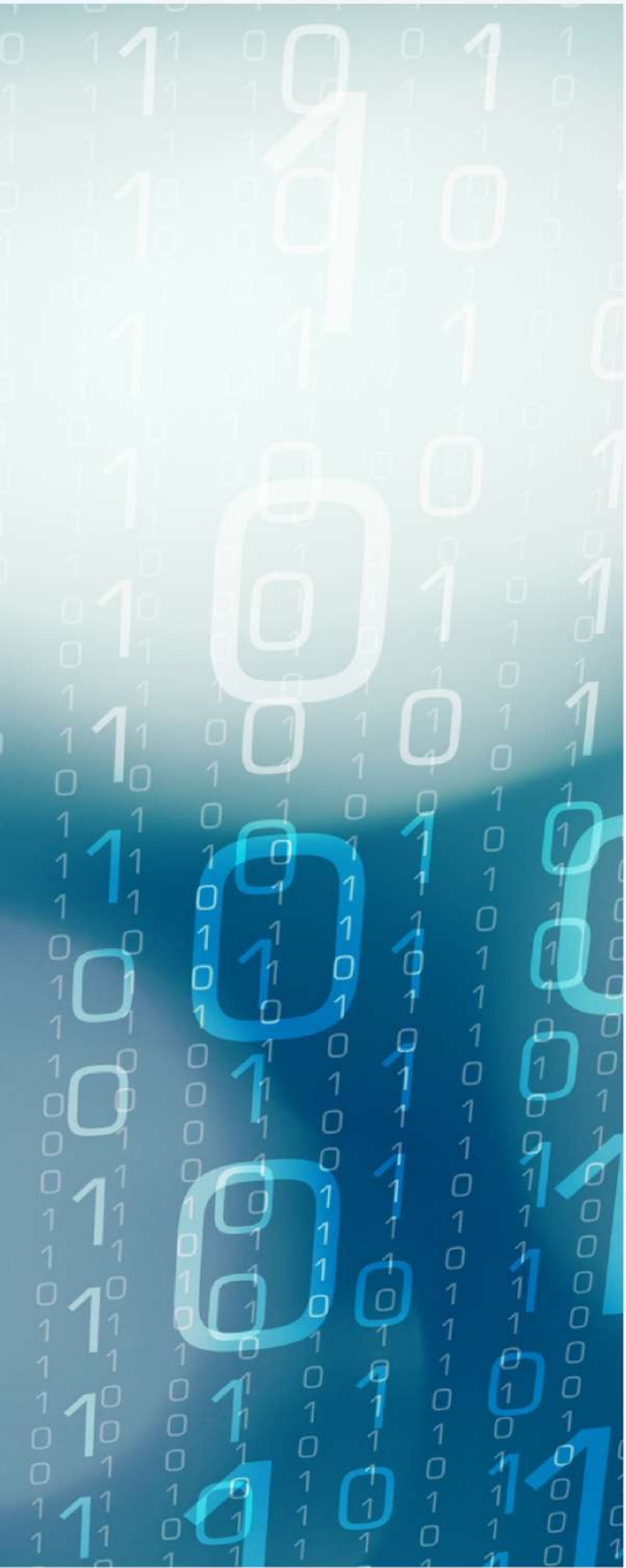
In the framework of this third substantive session and as proposed by the Chair in its letter of 22 June 2022, the Paris Peace Forum is happy and honored to draw upon successful deliverables of the Paris Call community to present some inputs on how stakeholders can contribute to the implementation of the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG.

I – INCREASING TRANSPARENCY AND INFORMING INTERGOVERNMENTAL DISCUSSIONS ON SECURING ICTS

Non-State actors' expertise and instrumental role in maintaining a free, open, secure, and stable cyberspace should encourage States to welcome their inputs and feedbacks as often as relevant. They are not only a valuable asset to inform intergovernmental discussions on securing ICTs, but also key to operationalize rules and standards in a transparent and cooperative manner.

Under the co-lead of the CyberPeace Institute, the GEODE Research Center and the Hague Center for Security Studies, the Paris Call community has for instance been developing a proposal for a methodology to measure cyberstability. Building on existing technical, industrial, and academic consensus, the proposed methodology aims at providing both the technical and the international community with a comprehensive tool to apprehend cyberstability as a prerequisite for trust and security in cyberspace.

This proposal has been presented to the OECD for discussion in the legitimate intergovernmental committee to develop a cyberstability index. This deliverable is both proving the strength of multistakeholder collaboration to develop innovative norms and tools to secure cyberspace and the willingness of stakeholders to cooperate with States in a constructive manner.



With regard to the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report as amended in the revised version:

- Stakeholders could efficiently contribute to identifying technical and cooperative measures to address existing and potential threats with regard to security in the use of ICTs as mentioned in §7(b), especially subpoints ii, iii, iv, v, viii, ix, and x. Contributions could either be made by national consultations by request of each State or through a dedicated procedure in the framework of the OEWG.

- Information exchanges on best practices and cooperation mentioned in §8(c) could also be applied to stakeholders by including them through dual-track approaches within intergovernmental channels, when relevant for international security.

- Transparency measures mentioned in §10(b) could also be applied to stakeholders when relevant to international security, especially concerning information sharing and lessons learnt.

II – CONTRIBUTING TO INTERNATIONAL NORM-SETTING ON SECURING ICTS

Creation, modification, and specification of international law are the exclusive prerogative of States as enshrined in international custom and the Charter of the United Nations. Stakeholders can although fruitfully contribute to norm-setting processes by raising awareness on current and emerging governance issues that would require further agreement between States to ensure our collective security. Stakeholders has for instance played an instrumental role in the making of international humanitarian law, to the point that some stakeholders are sometimes given a particular role to identify and disseminate international law in specific areas (e.g. the International Red Cross Committee).

Two reports published in the framework of the Paris Call emphasized how an extended practice of multistakeholderism can help adopting international norms related to the 9 principles of the Paris Call, and more specifically how it can contribute to cyber discussions at the United Nations.

A first report established under the co-lead of Microsoft, F-Secure and the Center for Cyber Security and International Relations Studies has emphasized concrete, action-oriented recommendations to develop international norms around the 9 core Paris Call principles to secure cyberspace by including inputs and contributions from all relevant actors across the value chain and beyond the industry.

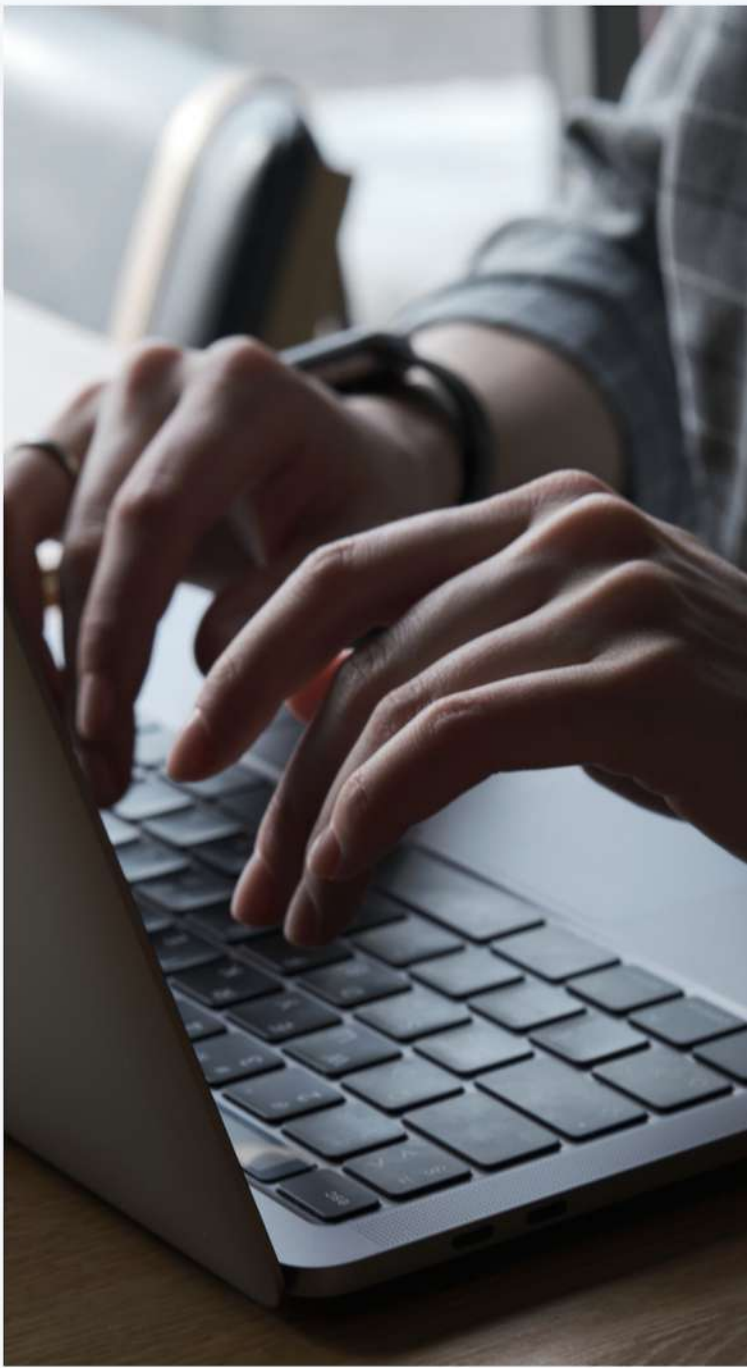
A second report established under the co-lead of the Cybersecurity Tech Accord and AccessCyber.org highlighted several successful experiences of extended inclusion of stakeholders in UN discussions and made concrete recommendations on the way States could draw upon these experiences to follow a multistakeholder approach in their work to secure cyberspace.

With regard to the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report as amended in the revised version:

- Stakeholders could efficiently contribute to developing additional guidance or checklists on norms implementation as mentioned in §8(a). Contribution could either be made by national consultations by request of each State or through a dedicated procedure in the framework of the OEWG.

- Should the OEWG convene discussions on specific topics related to international law as mentioned in §9(a), the inclusion of stakeholders will especially be relevant for discussions related to principles of international humanitarian law as for any discussion involving concrete impacts on individuals and non-state actors' rights and obligations.

- Voluntary contributions by Sates on how international law is applied in the use of ICTs mentioned in §9(b) could also be requested from stakeholders. Although the development of international law remains the exclusive prerogative of States, such contributions could be regarded as subsidiary means to inform States' work in specifying the applicability of international law in cyberspace, building on existing practice in international law to accept non-state actors' contributions as subsidiary means for the determination of rules of law – as for instance enshrined in the statute of the ICJ (art. 38, 1-d).



III – FOSTERING GREATER COLLABORATION AMONG ALL ACTORS AND BETTER INTEROPERABILITY WORLDWIDE

As securing cyberspace and ensuring its stability will require close cooperation among all actors worldwide, extended stakeholders' involvement is key in designing an efficient security architecture in cyberspace. Non-state actors further play an instrumental role in fostering better interoperability between existing practices, standards and frameworks.

A report published in the framework of the Paris Call for instance highlighted a path towards a comprehensive approach to securing the ICT supply chain by thinking at the scale of the whole ecosystem. Established under the co-lead of the Cigref and Kaspersky, the report provides operational recommendations for stakeholders to collaborate on grey zones of the current international framework.

With regard to the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report as amended in the revised version:

- Should the OEWG agree to establish a global, inter-governmental, points of contact directory on ICTs at the United Nations as mentioned in §10(a), additional steps could be taken to extend such initiative to stakeholders when relevant to international security. Inclusion of stakeholders POCs could be realized either at national level or by including a consultative, multistakeholder committee in the possible points of contact directory.

- As recognized in the proposed next steps, stakeholders could contribute to developing efficient and innovative confidence building measures as mentioned in §10(e), especially on issues involving public-private partnerships or active participation of non-state actors.

Contact

Jérôme Barbier

Head of Outer Space, Digital & Economic Issues

Policy Department | Paris Peace Forum

jerome.barbier@parispeaceforum.org

Pablo Rice

Cyberspace Governance Policy Officer

Policy Department | Paris Peace Forum

pablo.rice@parispeaceforum.org