United Nations General Assembly

Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025

Informal Dialogue Between the Chair and Interested Stakeholders Statement by the Paris Peace Forum
Delivered by Jerome Barbier, Head of Outer Space, Digital and Economic Issues

11 July 2023

Thank you, Mr. Chairman, distinguished Delegates and dear participants,

[*My name is Jerome Barbier and I am speaking on behalf of the Paris Peace Forum, which welcomes the secretariat of the Paris Call for Trust and Security in Cyberspace. The Paris Call is one of the world's main multistakeholder platform to advance norms and principles to common norms and principles to defend accountability and human security in cyberspace, thanks to its community of over 1200 supporters from across the ecosystem.*]

Mr. Chairman, we would like to reiterate our appreciation for your sustained efforts to ensure the participation of all interested stakeholders in the work of this Open-Ended Working Group, including through today's informal dialogue. As you have offered stakeholders to share insights on how they could best contribute to the action-oriented proposals captured in the zero draft of the second annual progress report, allow me to first commend States for the progress made in the 3rd and 4th substantive session as well as during the intersession.

We first welcome the reference made, under the Existing and Potential Threats section, to the proliferation of commercially available ICT capabilities that can be used for malicious purposes as well as the uncontrolled growth of "access as a service" markets as mentioned in paragraph 11. As a major threat to international peace and security and to the global stability of cyberspace, addressing this worrying trend is a crucial step towards a comprehensive handling of this multi-layered issue.

While States retain the exclusive regulatory authority to address this phenomenon – and remain so far the main clients of such capacities on the primary market - the stakeholder community has been key to understanding the dynamics of this market and to paving the way for a global response. These include for example the work of the University of Toronto's Citizen Lab or journalistic investigations coordinated by Forbidden Stories, as well as the Principles to limit the threats posed by cyber mercenaries recently released by the Cybersecurity Tech Accord, offering Industry good practices on this matter. It is also crucial to seek better coordination of these efforts on this topic

especially as to articulate existing frameworks with necessary new norms where relevant, as well as the responsibility of all actors, whether public or private. In compliance with Principle 5 of the Call, the Paris Call community is currently pursuing this endeavor in a multistakeholder format and is at the disposal of the OEWG to contribute further to any discussion on these topics, which we believe to be a critical link in securing a stable and peaceful ICT environment.

Better international understanding of cyber threats is besides key to the work of the OEWG. We therefore welcome the proposal to introduce a voluntary glossary of national definitions of technical ICT terms, and we'd like to reaffirm that the stakeholder community is, again, in a position to help States develop their national doctrines and terminologies – as they are already doing it especially at a national level – as well as to support better convergence at the international level.

Better clarity and, where possible, convergence on the notion of "critical infrastructure" would especially contribute to the goal of the OEWG. While we recognize the right of each States to decide for themselves which infrastructures should be qualified as critical on their soil, in particular considering national security concerns, concrete and large-scale threats to populations posed by the disruption of certain infrastructures should be objectivized and made the subject of a more unambiguous agreement.

A first step, that we believe to be achievable for this second APR as it is aligned with many contributions made during the 3rd and 4th substantive session, could be to differentiate more clearly the diverse criticalities at stake – either considering *inter alia* disproportionate impacts on populations, damages to the public core of the internet, or national security reasons. The different categories of criticalities would indeed clarify the different sorts of regimes to look as, as well as enable better coordination with the stakeholder community to identify risks and threats, as well as levers to better secure CI and CII.

Here too, stakeholders have unique resources and expertise when it comes to protecting populations for disproportionate cyber harms, or to identify major threats to the public core of the internet - when it is understood that critical national security threats shall be dealt with trusted stakeholders only. The Paris Call community is also addressing this challenge and would be happy to share its initial conclusions with the OEWG, if relevant. The Paris Peace Forum remains at the disposal of delegations which would like to exchange further on these ideas ahead of the 5th substantive session.

Thank you, Mister Chair.