United Nations General Assembly

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

Seventh Substantive Session

Statement by the Paris Peace Forum
Delivered by Jerome Barbier, Head of Outer Space, Digital and Economic Issues

6 March 2024

Thank you, Mr. Chair, distinguished delegates,

Mr. Chair, allow me to first reiterate our appreciation for your sustained efforts to ensure the participation of all interested stakeholders in the work of this Open-Ended Working Group, during and outside of the substantive session. We would like to focus our intervention on the commercial proliferation of cyber intrusive and disruptive cyber capabilities, and possible useful steps that States could undertake in the short term.

Many delegations have acknowledged the worrying proliferation of intrusive and disruptive cyber capabilities on both underground and semi-regulated commercial markets where they can be mobilized by malicious actors to conduct unlawful actions that may threaten international peace and security. Such trend is empowering a growing threat landscape, both by increasing the number of threat actors across the Globe and by complexifying the modalities of cyberattacks.

On this important matter, the Paris Peace Forum wishes to commend the 25 States that united last month with members of the stakeholder community to launch the Pall Mall process to tackle proliferation and irresponsible use of commercial cyber intrusion capabilities. Such initiatives help drawing common understandings among participating States and can, in due course, inform the work of the OEWG by providing additional guidance for the implementation of the international framework of responsible State behavior.

In the framework of the OEWG and in line with your guiding questions, Mr. Chair, for the agenda item related to rules, norms, and principles, we would like to encourage States to share national positions on what they consider being a responsible use of commercially available intrusive and disruptive cyber tools, as well as to hackers available for hire. Such information would play a major

role in strengthening cooperation to ensure the integrity of the supply chain and preventing the use of harmful hidden functions. From an international peace and security perspective, it would further clarify national doctrines in the recourse to cyber proxies, limit risks of misunderstandings, and contribute to avoiding unwanted escalation.

I will finally mention that in line with principle 5 of the Paris Call for Trust and Security in Cyberspace, the Paris Peace Forum will reconvene the Paris Call working group on cyber mercenary and its network of expert stakeholders to focus on concrete use cases of responsible recourse to such technologies and services as to inform States efforts in this regard, in close cooperation with relevant intergovernmental processes and initiatives.

I thank you Mr. Chair.