Cybersecurity Tech Accord Statement - Virtual, informal consultative discussion with the Chair of the Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies 2021-2025

16 December 2021

To begin, I would like to thank the Chair on behalf of the Cybersecurity Tech Accord for the opportunity to participate in this consultation on the margins of the Open-Ended Working Group, and also the member states for their time and attention today. The Cybersecurity Tech Accord is a coalition of more than 150 global technology firms committed to foundational principles to advance trust and security in the online ecosystem.

Since the launch of the Cybersecurity Tech Accord in 2018, we have closely followed and provided contributions and recommendations as able to the UN negotiations around norms for responsible state behaviour in cyberspace and were encouraged by the adoption of both the OEWG and UNGGE consensus reports earlier this year. Given the shared and overlapping responsibilities which exist in cyberspace, especially when it comes to the technology industry, these deliberations on peace and security online must include the input and perspectives of a multistakeholder community.

To this end, over the past year the Cybersecurity Tech Accord has chaired a multistakeholder working group, as part of the Paris Call for Trust and Security in Cyberspace, on how to advance and facilitate the participation of nongovernmental organizations in UN dialogues on cybersecurity. Following a series of workshops and independent research, we published the working group’s findings in a new report – entitled, “Multistakeholder participation at the UN: The need for greater inclusivity in the UN dialogues on cybersecurity” – available now on the Paris Call website, which details how multistakeholder contributions have been instrumental in previous UN processes, including in the First Committee, and for advancing the UN agenda since its founding.

Adopting an inclusive process in the context of these dialogues will therefore not only improve outcomes by leveraging the multistakeholder model of internet governance, it would also be in keeping with the UN’s longstanding tradition of multistakeholder participation in similar dialogues. And given the escalating nature of conflict in cyberspace, it is important that the current OEWG lives up to its mandate to build on the expectations set previously – including the 11 norms for responsible state behavior in cyberspace and the recognition of international law online, including international humanitarian law – to now promote implementation and enforcement, as well as new expectations to respond to a constantly changing threat environment online.

We would like to share the following specific recommendations for this process going forward:

• Norms have been fundamental in helping clarify the limits of state behaviour in cyberspace. In addition to the existing 11 UN norms for responsible state behavior, we would encourage the
OEWG to specifically recognize cyberattacks against the ICT supply chain as off-limits and, in light of the concerning developments during the covid-19 pandemic, specifically prohibit cyberattacks against healthcare as well.

- Moreover, capacity-building efforts should include building and strengthening the diplomatic muscles necessary for states to engage in discussions on international cybersecurity. While it is commendable that the OEWG is open to the participation of all member states, without this kind of support many states will still be less prepared to engage in these deliberations than others. We recently published industry guidance on effective cyber diplomacy in a new whitepaper report and encourage states to reflect on the need to step up efforts in this space. The whitepaper is available on our website.

- Finally, the report of the most recent UN Group of Governmental Experts in particular has called on member states to clarify and publish statements on how they understand their obligations under international law apply online. These kinds of public statements can reduce confusion and highlight areas of agreement and disagreement, in order to begin to build consensus around what is required of governments by law in cyberspace, and to advance a rules-based order online.

We hope this consultative session will be followed by many more opportunities to provide feedback to this body as deliberations move forward. To that end, the Cybersecurity Tech Accord recently joined in supporting the multistakeholder letter to the Chair that was shared last week highlighting the need for these dialogues at the UN to include industry, civil society and academia more systematically throughout.

Thank you.

Annalaura Gallo
Head of Secretariat
Cybersecurity Tech Accord