Cybersecurity Tech Accord Statement – Informal Dialogue with the Chair of the Open-Ended Working Group

17 May 2024

Mr. Chair,

The Cybersecurity Tech Accord is pleased to participate in today's session and we would like to thank you for once again organizing an inclusive dialogue with stakeholders, particularly given that we understand that the government of Singapore itself had to pay for the arrangements for these five days, which is above and beyond the call of duty but for which we are really grateful. We also welcome your efforts to try and foster a compromise on what the future mechanism could be for continuing the critical dialogue on cyber policy in the peace and security field.

With respect to that subject, we think it is useful to illustrate our main point about the current proposal with an example from our personal experience. We have requested accreditation to the 8th Session of the OEWG in July, though since we have been vetoed seven times in a row, we are not very hopeful.

The Cybersecurity Tech Accord, representing more than 150 companies globally in international cybersecurity policy, has long advocated for greater multistakeholder participation in UN cyber processes. We have provided input into the OEWG since 2019, however, we continue to believe that modalities that allow any single state to veto individual stakeholders is not fit for purpose, and thank others for making the same point.

The draft is nearly silent on how to include non-state actors in the work of the proposed mechanism. Page 4 simply reads that: "*Other interested parties, including businesses, non-governmental organizations and academia* ***could*** *contribute to any future regular institutional dialogue,* ***as appropriate.***"

In our view, the success of the PoA, or any other permanent mechanism, will depend on its ability to facilitate multistakeholder inclusion in building and maintaining a rules-based order online. The internet, and the technology and services that use it, are largely privately owned and operated. Fundamental building blocks of the Internet are also overseen by multistakeholder processes. This unique nature of the digital domain requires cooperation across stakeholder groups to set meaningful expectations and then implement and uphold them.

To this end, we propose that any successor mechanism to the OEWG should ensure the modalities for the Ad-Hoc Committee on cybercrime, which have proven to be successful and valuable, are the minimum starting place for stakeholder participation.

On the scope of a permanent mechanism, this should include:

- **capacity building** to support effectively implementing UN norms globally;
- **monitoring progress and building consensus,** cataloguing how states take action and implement norms but also for states to understand the opinions of other states to build consensus; and
- **updating and setting new norms,** recognizing that the current 11 UN norms are not exhaustive, the PoA should facilitate adoption of new norms to address emerging and unforeseen cyber threats, including, as we highlighted in December 2023 and February 2024, new norms on protection of ICT supply chain security.

Excellency, distinguished delegates, we thank you for your attention, and wish everyone a good weekend and a safe return home for those not based here.

Annex from Statement in February 2023

Our signatory companies have observed a growing trend of state-sponsored cyberattacks that particularly target the IT sector. The motivation behind these attacks is clear: threat actors aim to compromise an IT vendor in order to gain access to its clients' systems. These attacks have significant humanitarian, social, and economic consequences, disrupting essential services for the well-functioning of our societies, such as education, healthcare, and financial services. More than the practical consequences on our everyday lives, these attacks have the potential to harm our societies, undermining the trust and confidence of citizens.

During our last intervention in December 2023, the Cybersecurity Tech Accord and our signatories called for a new voluntary international norm to be established by the United Nations OEWG in order to address this challenge. This new norm would complement the existing 11 UN norms for responsible state behavior in cyberspace; while it would not be a legal requirement, it would constitute a new, strong commitment by states to tackle this issue.
Already existing UN norms state that "States should take reasonable steps to ensure the integrity of the supply chain…", however the context we find ourselves in has clearly shown that this has not been understood as a prohibition on attacks against the supply chain. And while states should, together with the private sector, work to improve security in the ICT supply chain due to its significance, that same significance should also oblige states to not target the ICT supply chain with cyberattacks.

A new norm would send a strong signal about responsible behavior, encouraging states to more carefully consider collateral damage and discourage attacks that put others needlessly at risk. Setting such an expectation would allow other states to take steps to promote accountability, including by adopting transparency measures regarding targeting decisions and calling out when the norm is violated in public attribution statements. This would help foster a culture of responsibility and restraint among states and other actors in cyberspace and contribute to the development and observance of a rules-based order that respects the sovereignty, rights, and interests of all parties. Our signatories believe it is imperative that the United Nations take actions to protect the supply chain in accordance with this guidance.
We would like to restate the industry's commitment to support the application of existing norms in cyberspace. One of the ways in which the Cybersecurity Tech Accord is upholding this commitment is by sharing key information with governments about the cybersecurity threat landscape, such as important threats, major trends observed with respect to these threats, threat actors and attack techniques, as well as relevant mitigation measures. This is what we hope to achieve with our Threat Intelligence Newsletter aimed at the cyber diplomatic community, which the Tech Accord releases quarterly. We encourage cyber diplomats and all other interested stakeholders to join the distribution list of our threat intelligence newsletter if you would like to gain access to these resources from our signatory companies.