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

*28 February 2023*

Mr Chair

The Cybersecurity Tech Accord is honoured to participate in today’s informal dialogue and we would like to thank you for once again organizing an inclusive dialogue with industry, civil society, and other third parties. Unfortunately, once again, the Cybersecurity Tech Accord was one of the several nongovernmental organizations that received a veto on their accreditation request to take part in the next Formal meeting of the Open-Ended Working Group without a clear explanation as to why this has happened for the seventh time since the beginning of these discussions. We are encouraged by the decision of the Chair to continue to pursue regularized informal engagement with the multistakeholder community alongside the OEWG, such as today’s event.

We want to reiterate that as a community of more than 150 global technology firms committed to advancing cybersecurity and fostering trust online, we are well placed to participate in these discussions.

The Cybersecurity Tech Accord is deeply concerned about the increasing number of state-sponsored cyberattacks on the ICT supply chain in recent times. These are indiscriminate attacks that aim to disrupt individual citizens’ lives and livelihoods, and therefore they are contrary to responsible state behavior in cyberspace.

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.

Once again, Mr Chair, Katherine,

We thank you for your time.