Cybersecurity Tech Accord response to the UN-OEWG's *Substantive Report [FIRST DRAFT]*

The Cybersecurity Tech Accord signatories appreciate the multiple opportunities provided by the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) to provide input throughout its deliberations. Through live consultation events and invitations for written contributions, the OEWG has demonstrated the importance, interest and feasibility for multistakeholder inclusion in discussions of peace and security in cyberspace. In particular, we would like to recognize the efforts of Ambassador Jürg Lauber who, as Chair of the OEWG, has helped to welcome much of this multistakeholder inclusion.

Over the past two years, the OEWG has helped mature a model of multistakeholder participation in cyber diplomacy. From the initial requests for input, to the multistakeholder convening at the United Nations (UN) Headquarters in New York in 2019, to the recent rounds of "Let's Talk Cyber" events – multistakeholder consultation and engagement in these processes has become increasingly normalized. Despite this progress, however, more still needs to be done moving forward to facilitate more regular inclusion of multistakeholder voices in these dialogues and to plan for such inclusion from the outset such that it is not an ad-hoc process of identifying opportunities. Given the unique and overlapping equities in the digital domain, and the ever-evolving nature of technology itself, such inclusion will be essential in establishing and maintaining a rules-based order in cyberspace.

The Cybersecurity Tech Accord, a coalition of more than 150 global technology companies seeking to provide the industry's voice on peace and security challenges in cyberspace, has participated throughout this process via written statements as well as during successive rounds of live consultations. The following sections of this document provide our input on the recommendations included in the *Substantive Report [FIRST DRAFT]* produced by the OEWG. However, beyond any specific recommendations of the report, we hope the true legacy of this working group will be in demonstrating the need and potential for greater multistakeholder inclusion in discussions of peace and security in cyberspace moving forward, at the UN and beyond – that this will prove to be a stepping-stone for more robust engagement across stakeholder groups moving forward.

I. Existing and potential threats

The Cybersecurity Tech Accord signatories wholeheartedly agree with the report's assertion that "Harmful ICT incidents are increasing in frequency, precision and sophistication, and are constantly evolving and diversifying." The urgency of the challenge is difficult to overstate. The dramatic escalation in the numbers of sophisticated cyber incidents each year is well known and tracked by organizations like the Center for Strategic and International Studies, and has harmed countless innocent victims who are often unintentionally targeted.

A recent survey report published by the Economist Intelligence Unit and sponsored by the Cybersecurity Tech Accord – *Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats* – highlights how increasing numbers of nation-state attacks in particular is impacting the mindsets of organizations around the world. The report's findings, after surveying hundreds of business leaders, are unambiguous – executives from across industries and regions feel increasingly threatened by nation-state cyberattacks against their organizations, and only expect these trends to continue in the absence of action. This is unsustainable.

More than any one threat vector or method of attack, the increasing conflict and tension between governments online is threatening the stability of our shared online environment, and undermining the potential benefits of digital transformation in economies around the world. This is why we were disappointed to see that the references to technological neutrality were dropped into the discussions section of the text. Technology will continue to evolve, and it is critical that the work of the OEWG applies across the spectrum of online activity, including to those methods that are yet to be invented.

Even more critically, as the digital divide continues to close in the coming years, we need to address escalating nation-state activity that puts all who rely on ICT systems at risk. While every organization has cybersecurity responsibilities that should be encouraged and empowered, the expectation cannot realistically be that every organization will be capable of withstanding a nation-state attack on their ICT systems. There needs to be a larger shift in thinking to discourage reckless behavior on the part of governments. We feel these dynamics could be more clearly stated in the report.

Especially concerning have been attacks which target vulnerable organizations at critical times – this includes the attacks on hospitals and other healthcare infrastructure in the past year, which have threatened and compromised essential services amid a pandemic. And sophisticated attacks do not just threaten vulnerable organizations, the recent SolarWinds hack has highlighted how no organization should feel immune from a sufficiently resourced and determined adversary. It also demonstrated how brazenly advanced threat actors are willing to undermine confidence in essential processes and the public core of the internet in carrying out an attack. Fundamentally, this section of the report should communicate that threats online have only been escalating in ways that the international system, to date, has been unable to properly address.

II. International law

The Cybersecurity Tech Accord signatories appreciate that the Zero Draft affirms that international law is "applicable and essential" to maintaining peace and security in cyberspace. Unfortunately, this simple recognition of international law has thus far been insufficient in reducing escalating threats and conflict online. We therefore not only recommend an even stronger commitment, in particular to international humanitarian law and human rights law in the text, but also call for greater clarity regarding *how* this body of law applies to cyberspace. This is why we also support the recommendation that encourages Member States to "inform the Secretary-General of their national views and practices on how international law applies to their use of ICTs in the context of international security."

The First Draft says in the section on cyber threats, "*…any use of ICTs by States in a manner inconsistent with their obligations under international law undermines international peace and security, trust and stability between States*". This sentiment would seem to make it imperative that States respectively work to clarify in precise terms how they understand their own obligations under international law – delineating which actions they understand to be permissible and which are not. Not only would such an exchange of views provide transparency and highlight areas of agreement, it would also promote discussion around areas of disagreement and help reveal gaps in the international legal framework that should be addressed.

III. Rules, norms and principles for responsible State behavior

Cyber norms have an important role to play in guiding responsible behavior in a new domain of human activity. Participating in and reaping the benefits of digital transformation brings with it new responsibilities for all actors – including consumers who increasingly use connected devices, industry that needs to be prioritizing cybersecurity across its operations, products and services, as well as governments. As the draft report indicates, norms should not conflict with or replace international law, but they are essential in cyberspace to clarify what the expectations should be for responsible behavior. To this end, the Cybersecurity Tech Accord signatories support the recommendation that states should voluntarily survey their national efforts to implement international cyber norms and share relevant guidance on norms implementation – in particular as it relates to the 11 cyber norms recognized by the United Nations.

The UN cyber norms create expectations and states should think affirmatively about how they are implementing each of them to promote peace and stability in cyberspace. This includes norms which describe actions states *should* take, as well as norms describing actions states *should not* take. In the case of the former (ex. "states should take appropriate measures to protect their critical infrastructure") – states should identify what steps they have or will take to carry out these expectations. When it comes to norms which restrict behavior (ex. "states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure") states should similarly make clear what guardrails are to be put in place in order to uphold that commitment. For additional guidance on norms implementation, we recommend reviewing the Cybersecurity Tech Accord's submission to Australia's consultation on responsible state behavior in cyberspace.

While supporting the recommendation that states work together to implement the 11 UN cyber norms, the Cybersecurity Tech Accord also recognizes the important role a broader multistakeholder community needs to play in these efforts. To this end, external forums, like the *Paris Call for Trust and Security in Cyberspace* should be recognized in this report as instrumental in helping to implement and reinforce norms, as they can pull together the necessary multistakeholder coalitions to do so. This includes through the new Paris Call Working Groups, which were recently announced by the French government to advance the Paris Call principles. The Cybersecurity Tech Accord is co-chairing one such working group on advancing the inclusion of multistakeholder voices in international deliberations, and we would encourage all stakeholders, including governments, to join and contribute (more on this in Sec VI).

Finally, given the hardships endured over the past year as a result of the COVID-19 pandemic, and the unique impact of cyberattacks on hospitals during such times, we feel the OEWG would make a meaningful contribution to the UN's mission to advance peace and security, as well as human rights, in cyberspace by expressly recognizing in its report that attacks on healthcare should be prohibited. This could be included as an independent norm, or as an elaboration of the norm against attacks targeting critical infrastructure, but certainly these unique circumstances of the time that are impacting peace and security in cyberspace are what the OEWG is meant to be addressing.

IV. Confidence Building Measures

Fundamentally, improving confidence between parties in cyberspace means improving communication to create trust. With that in mind, the Cybersecurity Tech Accord agrees with the report's finding that the OEWG, especially given its more inclusive nature, has served as a confidence building measure in and of itself. Moreover, we support the recommendation that all States identify a government point of contact for issues of peace and security in cyberspace in order to facilitate greater communication and coordination between governments moving forward.

In addition, the Cybersecurity Tech Accord signatories encourage the OEWG final report to include a recommendation that governments, in particular advanced cyber powers, endeavour to be more transparent about their cyber policies and practices overall to improve confidence. This is especially important as it pertains to vulnerability handling. By providing greater transparency around how governments decideto handle a vulnerability – to retain it to be exploited or to disclose it to a vendor to be fixed - States will be less inclined to assume worst intentions.

For our part, companies across the technology industry also need to take greater responsibility for expeditiously and effectively addressing vulnerabilities in their products and services as soon as they are reported. This is why the Cybersecurity Tech Accord has encouraged all of its signatories to adopt coordinated vulnerability disclosure policies and to publish them. More than 100 of these policies are currently available for review on our website, to serve as an example across the industry and to signal to governments that we are prepared to be a responsible partner following vulnerability disclosure to protect civilians everywhere.

V. Capacity building

The Cybersecurity Tech Accord signatories support the recommendations related to capacity building contained in the OEWG's First Draft, and in particular the introduction of guiding principles and their focus across processes, partnerships and people.

However, we would encourage the OEWG to include a more explicit recognition in the section's recommendations of the importance of multistakeholder cooperation for successful cybersecurity capacity building efforts. In particular, a recognition of existing capacity building initiatives that operate outside the UN system, such as the Global Forum for Cyber Expertise, would be important. It is clear that any work to improve capacities and uphold a rules-based order in cyberspace will require cooperation across stakeholder groups.

VI. Regular Institutional Dialogue

As discussed in the introduction, the OEWG has already demonstrated the feasibility and importance of multistakeholder inclusion in discussions of peace and security in cyberspace. There seems to be widespread recognition that the OEWG has benefited from this necessary outside expertise and input, given the overlapping responsibilities and constantly evolving nature of cyberspace. We hope that any further discussion in the United Nations incorporates a mechanism for regular dialogue with the multistakeholder community.

To this end, the Cybersecurity Tech Accord signatories welcome the proposal made for establishing a Programme of Action, which seems to indicate that a development of a regular dialogue on this topic not just amongst States, but the multistakeholder community, would be possible. As conflict in cyberspace continues to escalate and evolve both in terms of techniques and technology, it is clear that iterative ad-hoc working groups at the UN have, on their own, been insufficient in turning the tide against these trends. The Programme of Action has the potential to provide an enduring forum to leverage the tools available to strengthen and reinforce expectations for responsible behavior online. As such we would advocate for its adoption, however outside the new OEWG framework rather than within in it, as indicated in the text of the First Draft.

In 2021, the Cybersecurity Tech Accord will be co-Chairing Paris Call Working Group #3 – *Promoting a multi-stakeholder approach in UN cyber negotiations.* In that capacity, we look forward to working with a broad coalition to advance solutions that ensure States working to address international security issues online are always able to benefit from guidance provided by a multistakeholder expert community.

Thank you once again to the organizers of the OEWG for providing this opportunity to provide input and guidance on the draft report from the Cybersecurity Tech Accord. If you have further questions, please do not hesitate to reach out to our secretariat: info@cybertechaccord.org.