Cybersecurity Tech Accord – Statement for the informal, intersessional meeting of the Open-Ended Working Group on security of and in the use of ICTs

(5-9 December 2022)

The Cybersecurity Tech Accord is honoured to be able to participate in the intersessional meeting of the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies. We are encouraged that we were able to do so despite challenges in obtaining accreditation for many non-governmental groups, including the Cybersecurity Tech Accord. We want to thank the Chair for making sure that this could happen.

As a coalition of 150+ technology companies committed to a safe and secure internet, we are well placed to provide input into these deliberations. Since its inception in 2018, the Cybersecurity Tech Accord has worked to draw attention to priority cybersecurity challenges, share best practices, and offer industry guidance – to serve as the voice of the technology industry when it comes to peace and security online.

The Cybersecurity Tech Accord is firmly committed to supporting inclusive and transparent dialogues that promote an open, free and secure online world. We have long advocated for permanent and more structured methods of multistakeholder inclusion in UN negotiations in particular and we welcome the passing of the resolution on the Program of Action (PoA) last month in furtherance of that objective. We know that protecting our online environment is not only in everyone's interest, but also our collective responsibility. We look forward to continuing to engage in these important dialogues in the future.

Regarding the thematic topics for the OEWG December intersessional meeting, the Cybersecurity Tech Accord submits the following:

Thematic Session: Points of Contact

The Cybersecurity Tech Accord believes that a proposed Points of Contact (PoC) directory represents a helpful tool for increasing the resilience and security of cyberspace. Having ready access to relevant points of contact has been critical to the community of defenders in the technology community for many years. For governments, such a resource would not only have the potential to improve incident response, but also represent a fundamental confidence building measure to create trust amongst member states.

While the First Draft Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 dated August 2022 referred to contacts at the technical, policy and diplomatic levels, it would be important not to duplicate existing PoC networks of Computer Emergency Response Teams (CERTs) as well as cooperative networks run by the cybersecurity technical community (e.g., FIRST.org). The OEWG should, whenever possible, seek to leverage these and other existing structures instead of recreating them. With that in mind, we would recommend prioritizing establishing diplomatic points of contact for cybersecurity issues. At the very least, a "points of contact" directory should have specificity around what kinds of roles and responsibilities the names included should reflect – to avoid having technical experts on a policy directory, or vice versa, for example.

The directory should also consider how to include relevant points of contact from outside government circles, where industry or other stakeholder expertise could provide added value. Once established, the directory should be maintained by a designated body (e.g., the UN Office of Disarmament Affairs) and made available to both participating states and stakeholders. States should be encouraged to notify changes in their national PoC's (for example no later than 30 days after the change has occurred), so that the directory stays up to date. Communication checks could be made, for example on a bi-annual or annual basis, to ensure the directory is current and functional.

Thematic Session: 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 First Draft Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 dated August 2022 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 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, particularly 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 via adopting "vulnerability equities processes." By providing greater transparency around how governments decide to handle a vulnerability – whether 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. Therefore, 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.

Moreover, it is important to note that there is a great number of information sharing initiatives that are already well established and functioning. Our members, as well as others across the private sector – not just the ICT industry – have partnered and worked together in these groups sometimes for over 20 years. Our members participate in several information sharing organizations, including Space ISAC, IT ISAC, Auto ISAC, FSI ISAC, and GSMA Telecommunications ISAC.

Thematic Session: Existing and Potential Threats

The Cybersecurity Tech Accord signatories wholeheartedly agree with the OEWG's first Annual Progress Reports 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. This is unsustainable.

At the same time, we do see, as indicated by the Chair's guiding questions, an increase in use of new technologies as part of offensive operations. Artificial intelligence (AI) is but one such example. We can say with growing confidence that AI will become one the 'tools of the trade' for powering and scaling cyberattacks. By leveraging basic automation, these attacks will create efficiencies and amplify their impact. In fact, many malware variants already use simple sets of logical rules to recognize and adapt to operating environments – such as checking for time zones – in order to avoid detection. AI can also be used to generate ultra-personalized phishing attacks, which are capable of duping even the most security-conscious users. A striking study from 2018 demonstrated how AI systems can learn from publicly available data – such as online profiles – and optimize the timing and content of messages with the goal of maximizing clickthrough rates.

To address these issues, states should ensure a regular dialogue with academia and industry, the two groups closest to cutting edge development and innovation in this space. This should span both threat briefings on the current state of affairs, as well as conversations around the potential mid-and long-term trends in this arena. Technology will continue to evolve so it is critical that the work of the OEWG endeavours to be forward thinking and not exclusively preoccupied with the threats of the day. This is why we were disappointed to see that the references to technological neutrality were dropped into the discussions section of the first draft text of the Progress Report.

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. 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 behaviour on the part of governments. We feel these dynamics could be more clearly stated in the OEWG Annual Progress Report.

Thematic Session: International Law

The Cybersecurity Tech Accord signatories appreciate that the OEWG Progress Report 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. Therefore, we not only recommend an even stronger recognition of international law's authority by the OEWG, particularly regarding international humanitarian law and human rights law, but also call for greater clarity regarding how this body of law applies to cyberspace.

This is why we also support the recommendation of the OEWG Progress Report encouraging 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."

We strongly encourage states to make use of discussions from academic institutions on how international law applies to cyberspace, such as Oxford University's research initiative on the applicability of international law in cyberspace. Furthermore, we encourage states to leverage international law as able following cyber incidents, for instance highlighting potential violations as part of public attribution statements. This will contribute to our collective understanding of how international law applies to cyberspace in specific situations.

Thematic Session: Capacity Building

The Cybersecurity Tech Accord signatories support the recommendations related to cybersecurity capacity building contained in the OEWG's First Progress Report, as well as the introduction of guiding principles and their focus across processes, partnerships and people. It is our understanding that many of the principles have already been incorporated into the leading cybersecurity capacity building initiatives, such as those driven by the ITU and OAS. These must be at the core of any new initiative that is spun up.

We also encourage the OEWG to include in the Capacity Building section's recommendations of the Final Report, a more explicit recognition of the importance of multistakeholder cooperation for successful cybersecurity capacity building efforts. A recognition of existing capacity building initiatives that operate outside the UN system, such as the Global Forum for Cyber Expertise (GFCE), would be important. Meaningful work to improve capacities and uphold a rules-based order in cyberspace will require cooperation across stakeholder groups. The GFCE has an important role to play in collecting and coordinating capacity building efforts – acting as a clearing house, effectively match making between donors and recipients. We call on the UN to drive greater awareness of this effort, rather than seeking to duplicate it.

We further encourage the UN to break cybersecurity capacity building out of its silo and ensure that it is fully integrated into broader development efforts. This could include, for example, identifying the criticality of cybersecurity to reaching the UN's Sustainable Development Goals (SDGs) and working to address any gaps that emerge.

Finally, there are a number of existing initiatives that have been driven by the private sector, independently and in partnership with governments, that are worth highlighting in this regard. For example, The Cybersecurity Tech Accord in 2020 published a report with the UK's Foreign Commonwealth and Development Office (FCDO) and the Commonwealth of Nations documenting the breadth of cybersecurity awareness campaigns across the member state organization and providing industry input on how to make such efforts successful. We also produced guidance last year on how governments can structure and effectively build-out their cyber diplomacy capacities.

Our signatory companies from across the technology industry are also leading capacity building efforts. To provide just a few examples: Cisco has launched the Cisco Networking Academy, a world-leading IT skills and career building program, which addresses the growing need for IT

talent by equipping students with IT career skills. Meanwhile, Salesforce leads The Cybersecurity Learning Hub initiative with partner support from The World Economic Forum and the Global Cyber Alliance. The Learning Hub was launched in 2019 to reduce the global cybersecurity workforce gap through training and upskilling by delivering free and globally accessible cybersecurity training. This platform aims to democratize access to cybersecurity career paths and has already trained over 80,000 individuals spread across all continents and over 480,000 completed learning modules.

Thematic Session: Regular Institutional Dialogue

Institutional dialogue should not only focus on regular dialogue between states, but also bring in other relevant voices. The importance of multistakeholder inclusion in discussions of peace and security in cyberspace should be self-evident by now, given the overlapping security responsibilities and constantly evolving nature of cyberspace. We therefore hope that any further discussions on these issues in the United Nations incorporates a mechanism for regular and meaningful dialogue with the multistakeholder community.

The Cybersecurity Tech Accord signatories welcome the recent passing of a UN resolution to establish a Programme of Action (PoA) to serve as a permanent standing body to address international cybersecurity. While not immediately clear from the resolution text, we hope that the PoA will include robust and meaningful multistakeholder participation, reflected by:

- Inclusion of the relevant multistakeholder community in the PoA's regular meetings;
- Consulting on proposals to take action with the multistakeholder community;
- Conferring through multiple channels with nongovernmental stakeholders, such as meetings or written responses to create multiple opportunities for outside groups to engage;
- Organizing inclusive side events and roundtables, in cooperation with states and the secretariat;
- Exploring opportunities for the ongoing exchange of information across stakeholders to address pressing challenges.

As conflict in cyberspace continues to escalate and evolve, in terms of both techniques and technologies, it is clear that iterative ad-hoc working groups at the UN have been insufficient in addressing these threats on their own. As a permanent body, the PoA has the potential to provide an enduring forum to leverage the tools available to strengthen and reinforce expectations for responsible state behaviour online. As such, we would suggest it be established outside the new OEWG framework rather than within in it, as indicated in the text of the First Draft Report.

Thematic Session: Rules, Norms and Principles of Responsible State Behaviour

Cyber norms have an important role to play in guiding responsible behaviour 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 rely on connected

devices, industry, which must prioritize cybersecurity across its operations, products and services, as well as governments. As the First 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 behaviour. 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 – particularly the 11 cyber norms recognized by the United Nations.

The 11 UN cyber norms create expectations for behaviour 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 behaviour (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 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 behaviour 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.

Thank you once again to the Chair of the OEWG for providing this opportunity to provide input and guidance. If you have further questions, please do not hesitate to reach out to our secretariat: info@cybertechaccord.org.