Cybersecurity Tech Accord Submission to the Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

August 2022

The Cybersecurity Tech Accord welcomes the opportunity to provide input into the Third Session of the *Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*. As a non-ECOSOC accredited member of the multistakeholder community, we would like to thank the AHC for establishing such a robust and inclusive structure for multistakeholder participation in its work.

Since 2018, our coalition of over 150 technology companies has served as the voice of the tech industry on matters of peace and security online. Our signatories include small and medium-sized technology and cybersecurity enterprises, as well as global technology companies, allowing us to coordinate a range of input from private sector organizations across the globe. We represent those in the industry that can uniquely speak to the challenges posed by cybercrime and to how technology is expected to evolve in the coming years and the implications for crime online.

The Cybersecurity Tech Accord has carefully followed the work of the Committee and was glad to be able to engage with member states during the June 2022 intersessional, where several of our signatory companies addressed the floor on the topic of Technical Assistance. We have also partnered with the CyberPeace Institute to produce the Multistakeholder Manifesto on Cybercrime, highlighting key principles to guide the AHC negotiations. These principles include:

- protecting victims of cybercrime;
- combating cybercrime by promoting international cooperation;
- maintaining existing international legal obligations;
- focusing on accountability mechanisms;
- time-proofing any treaty requirements;
- preserving the global public internet;
- promoting transparency and stakeholder participation in negotiations;
- limiting the scope of any new cybercrime treat; and
- adopting a consensus-driven approach.

Our understanding is that the AHC's Third Substantial Session will be focused on (i) international cooperation, (ii) preventative measures, (iii) technical assistance and (iv) implementation measures. Against that background, the Cybersecurity Tech Accord encourages member states to take into consideration the following guidance.

I. *International* Cooperation provisions

Ensure lawful access to digital information

Any new treaty should establish unambiguous rules around government access to digital information, and only grant access under lawful processes and with appropriate safeguards. This must not include requirements for so called "back-doors" to be established by private industry or *any* other methods of granting access which would require the weakening of encryption. Such requirements would only serve to weaken security across the entire digital ecosystem, which relies on robust and trustworthy encryption.

Promote harmonized rules to support international cooperation

A new treaty should advance harmonized laws to fight cybercrime across member states and avoid rules that would conflict or make cooperation on cybercrime between states and the private sector difficult. Wherever possible, a new convention should promote existing solutions to enforce international cooperation between the judiciary and law enforcement under transparent oversight and with protections for human rights. It should also recognize that investigating and prosecuting cybercrimes necessitates increased cross-sector and international collaboration, as well as harmonization of frameworks. The Council of Europe's Convention on Cybercrime, for more than two decades and with today more than 60 signatory governments, in particular has proven indispensable in supporting industry cooperation with law enforcement. Therefore, any new treaty should seek to complement, as opposed to conflict with, this existing cybercrime convention to avoid damaging ongoing work to fight cybercrime.

II. Preventative Measures

Remain focused on cyber-dependent and significant cyber-enabled crime

Cybersecurity Tech Accord believes a treaty with a narrow scope that is agreed upon and implemented by all states could significantly aid efforts to combat cybercrime. With that in mind, we hope that states remain focused on criminalizing only substantive offences that are cyber-dependent and avoid focusing attention on instances where a computer was merely involved in the planning or execution of a crime. A treaty on cybercrime should remain focused on *cybercrimes* to prevent contradictions from re-criminalizing activity that is already covered in other international agreements and to avoid wading into restrictions on objectionable content that will be difficult to harmonize and which could threaten freedoms of expression. This is not to dismiss concerns around pressing topics like stopping violent extremism, which should continue to be pursued aggressively within other appropriate forums.

Remain focused on state requirements

A new treaty should be focused on state commitments and obligations, rather than on setting requirements and standards for industry or other actors. Measures focused on things like increasing resilience of critical infrastructure need to be adopted at the national level but not as part of a convention seeking to enhance law enforcement cooperation. The convention should therefore not seek to introduce industry regulation as part of this process and instead focus on public authorities and on empowering them to prosecute cybercrime effectively.

III. Technical Assistance

Ensure multistakeholder inclusion and tech-neutrality in capacity building

Combating cybercrime will require significant investment in capacity building, especially in emerging economies. We encourage member states to consider industry's inclusion in those efforts, especially when it comes to capacity building to support law enforcement agencies and other governmental bodies. Ensuring that industry is a partner in such efforts not only leverages expertise but also creates opportunities for synergies and burden-sharing between governments and the private sector and can avoid duplication of efforts. Member states should also consider using portals like https://cybilportal.org/ to track assistance efforts in order to minimize duplication. Capacity building must include all entities and not be limited only to public entities.

Finally, the convention should focus on technical assistance that is technology-neutral and affirm its provision to be on a voluntary basis only, rather than mandating any forms of technology transfers. Intellectual property rights of any leveraged products and services require appropriate protections to facilitate public-private cooperation in combatting ICT crimes.

Transparency and knowledge sharing: cybercrime trends

Given the nature of the internet, countries everywhere face shared threats online, though different governments are often privy to the actions of different criminal groups. These varying perspectives and differing levels of readiness mean that countries frequently have different understandings of major cybercrime trends. To promote a more informed and comprehensive understanding, a new convention should establish a transnational information sharing regime, focused on cybercrime trends in particular. The constructive and timely exchange of knowledge and information between relevant authorities and the industry is critical to successfully identifying threats and taking action to combat cybercrime.

IV. Implementation Mechanisms

Preserving and building on existing frameworks

We call on states to ensure that any new convention does not conflict with existing frameworks, laws, or agreements. A new cybercrime treaty cannot become an avenue for states to reduce their existing obligations under international law, especially as it relates to international human rights law. In that spirit, a new treaty should seek to add to or streamline, rather than replace, existing obligations. It should reinforce existing international legal obligations, including due diligence expectations to take action against known criminal actors operating within a government's borders.

Ensure industry is included in implementation

We hope that a new convention can provide effective tools for promoting international cooperation between the judiciary, law enforcement and private companies to combat transnational cybercrime. We therefore ask states to ensure meaningful multistakeholder consultation and involvement in the implementation of the agreement by considering the equities of industry, as well as researchers, technical experts, and scientific and research institutions in the process.