Edoardo Ravaioli – Head of the Secretariat, Cybersecurity Tech Accord

Presentation for UN Disarmament Conference Thematic Event on the Centrality of International Cooperation and Capacity Building in building a safe and secure cyberspace

Thank you, Mr Chair,

Mr Chair, Excellencies, fellow Panellists,

On behalf of the Cybersecurity Tech Accord, I would like to thank Mr. Chair and the Secretariat for inviting us to this thematic discussion and for giving us this opportunity to participate in today's panel.

For those of you who are not familiar with our organization, the Cybersecurity Tech Accord is a coalition of global technology companies committed to protecting users and customers everywhere from evolving cyber threats. Since 2018, our coalition of over 150 technology companies has worked to serve as the voice of the technology industry on matters of peace and security online. Our partnership is based on four foundational principles: (1) protecting all of our users and customers everywhere; (2) opposing all cyberattacks on innocent citizens and enterprises from anywhere; (3) empowering users, and developers to strengthen cybersecurity protection; and (4) partnering with each other and likeminded stakeholders to enhance cybersecurity worldwide.

The breadth of our membership is one of our strongest assets, as our coalition represent micro-, small- and medium-sized technology and cybersecurity enterprises, as well as global technology companies. Our diverse Signatory base enables us to tap into insights from private sector organisations across the globe. We strongly believe that collaboration between customers, businesses and governments is necessary to address hybrid threats present on the internet.

Mr Chair, excellencies,

Over the past four years, we have engaged in and observed a range of both multilateral and multistakeholder cyber diplomacy forums – including at the United Nations (UN) OEWG and GGE, the Organization for Economic Co-operation and Development (OECD), the Global Forum on Cyber Expertise (GFCE), the Internet Governance Forum (IGF) and the Paris Call for Trust and Security in Cyberspace. We are actively following these discussions and adamantly believe in the value of industry and wider stakeholder input in these fora.

We would like to take this opportunity to renew our call that a multistakeholder approach is vital to addressing the growing and transnational challenges of ICT, to crack down on the malicious use of information and communication technologies (ICT) and to protect and empower users online. The private sector offers frontline experiences and cutting-edge technologies that are invaluable to developing effective long-term solutions.

When it comes to the industry and wider cybersecurity community's role in capacity building in the context of disarmament, our organization is able to provide three different types of capacity building: organizational, cyber awareness and technical capacity building. I would like to point to a couple of examples of the Cybersecurity Tech Accord's as well as some of our Signatories' capacity building initiatives.

(1) Firstly, we have guided governments in building their organizational capacity. In October 2021, the Cybersecurity Tech Accord published a guide to strengthen cyber diplomacy, titled: *Towards effective cyber diplomacy: A guide to best practices and capacity building* (link). The guide demystifies cyber diplomacy and provides a roadmap for countries developing their own cyber diplomacy capabilities. It was developed on the basis that international cybersecurity cannot move forward solely based on dialogues among a limited number of advanced cyber powers. We have compiled resources and recommendations from our engagements with first generation cyber diplomats around the world. The guide serves as a valuable and easy-to-use

guide for countries seeking to build or to mature their own cyber diplomacy capacities. In particular, the report can support governments working to engage in the global cyber dialogue with limited resources and those that have yet to develop a cyber diplomacy apparatus, including emerging and developing economies.

(2) We have also increased cybersecurity awareness, promoting an aware citizenry to make attacks less successful. In March 2020, we partnered with the UK's Foreign & Commonwealth Office (FCO) to release another policy capacity building report, *Cybersecurity Awareness in the Commonwealth of Nations* (link). The Report catalogues cybersecurity awareness-raising activities taking place across the 53 states that make up the Commonwealth of Nations, and stresses the importance of national efforts to develop cybersecurity awareness at all levels of a society, and provides industry guidance to support such efforts. Both white papers can be found on the Cybersecurity Tech Accord's website.

(3) Finally, our Signatories have established several technical capacity building initiatives, actively assisting governments and citizens across the world increase their cybersecurity knowledge, and effectively making it harder for malicious cyber actors to be successful. I would like to list a few examples of collaboration between stakeholders and governments, which shows the value of industry in this type of technical capacity building.

- Our signatory Salesforce is leading 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. That some of the most popular modules include Cyber Resilience, Cyber Hygiene, and Application Security points to how individuals are

prioritizing preparations for cyberattacks, how to prevent a cyberattack and how to build secure applications that can help them do business.

- Cisco, another of our Signatories, 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. The program is based on partnerships with over 9,600 schools, community colleges, universities, governments, NGOs, and other organizations, which implement the program across 170 countries. With these partnerships, Cisco has provided IT education to more than 15 million students over the course of 24 years and improving the lives and economic stability of communities worldwide, with a particular focus on developing and transitioning economies.
- In 2020, the Global Forum on Cyber Expertise and Microsoft partnered to increase cyber capacity building efforts in Africa, through the launch of a program focusing on unifying existing cyber capacity building efforts and strengthening the understanding of the cyber capacity needs of the continent. The partnership created the role of a "GFCE-Microsoft Africa Program Fellow" who specifically focuses on mapping, coordinating, and ultimately streamlining existing efforts in Africa.
- In the past, the Cybersecurity Tech Accord has also supported the 'Let's Talk Cyber' initiative a multistakeholder initiative between governments, civil society, and industry, helping raise the profile of ongoing multilateral discussions at the UN, and in particular the OEWG and Ad Hoc Committee on Cybercrime. The support from the governments of Australia and Canada in particular added immense value to the overall effort of this endeavour.

These are just some of the examples that point to how our initiative, industry and the wider multistakeholder community can contribute to the capacity-building at both the policy and technical levels to help support a peaceful and secure cyberspace.

One forum where cyber capacity building measures are crucial to discussions, is the OEWG. Recently, our organization was unfortunately vetoed from participating in the work of the OEWG. While we deeply regret this decision, we will continue to engage where we can and where our timely input can be constructive to discussions. We believe that states could strengthen coordination and cooperation between States and interested stakeholders, including businesses, non-governmental organisations and academia, as was outlined in Section F on Capacity Building of the Annual Progress Report adopted two weeks ago during the third substantive session of the OEWG on ICT Security.

Mr Chair, Excellencies, fellow Panelists,

We thank you, Mr. Chair and the Secretariat, and all of you distinguished delegates, once again for your time.

Response to statements
Thank you, Mr. Chair, for giving us the opportunity to provide additional remarks.

I echo Dr Macak's comment and want to thank you, all distinguished delegates, for your statements – on our side this has been a very educational session with regards to examples of state cyber capacity initiative.

We welcome the statements by the States that have stressed the importance of including the multistakeholder community, including industry, in international multilateral discussions on cybersecurity and especially in relation to capacity building. We also welcome statements of support on the PoA on cybersecurity as proposed by France and Egypt, and would like to point out that the Cybersecurity Tech Accord has been in support of this initiative since October 2021.

As the Conference on Disarmament continues to explore the role of the internet in conflict and comes to term with the need to increase capacity building across the globe, we renew our call that a multistakeholder approach is vital to addressing the growing and transnational challenges of ICT, and we stress that industry is able to provide both policy insights as well as concrete technical capacity building solutions for states.

With regards to the question made by the delegate from Brazil regarding cooperation between industry and governments on cybercrime, while I cannot speak for the entirety of industry, I can confidently say that there are well established frameworks between public sector organisations and technology companies in our Signatory base that allow and ensure this exchange of information regarding cybercrime. I would like to point your attention to a statement (link) that was delivered by Panasonic, the large Japanese multinational, and Balasys, a small cybersecurity firm from Hungary, during an intersessional stakeholder consultation to the AHC on Cybercrime, which highlighted industry's role in technical assistance with regards to cybercrime cooperation. I would be happy to share with you. Our organization is also drafting a statement for the upcoming substantive session of the AH committee on cybercrime, which I would be happy to share with you once finalized.

To conclude, as was mentioned by delegates and panelists today, we welcome the adoption of the OEWG Annual Progress Report. We also support the proposed next step calling on States to find a better understanding of the capacity building needs of developing states with the aim of narrowing the digital divide through tailored capacity-building efforts. Again, we call on states to include industry and the wider multistakeholder community in these efforts. Capacity building efforts are the most successful when they are responding to a real need. Taking into consideration the regional and local context, as well as different cultural approach technology is

crucial in identifying gaps in capacity, as the needs of member states greatly vary.

We thank you once again, Mr Chair for organizing this session, and thank you distinguished delegates for allowing us to speak during this important discussion.