# Cybersecurity Tech Accord submission to the UN High Level Panel on Digital Cooperation

Digital technology powers every aspect of business, society and our individual lives: from improving education and healthcare to advancing agriculture, from creating jobs to enhancing environmental sustainability. It keeps us informed, connected, entertained and inspired; opening the doors to an ever-bigger world of opportunity. The creation of the UN Secretary-General's High-Level Panel on Digital Cooperation ("the Panel") earlier this year marked an important moment, as it recognized the criticality of technology to the realization of the 2030 Agenda for Sustainable Development. It also reflected the understanding that digital technologies cut uniquely across international boundaries, sectors, and societies, and that a new form of governance is needed to reap its benefits, one that relies on cooperation amongst governments, the private sector, technical community, civil society, and other groups. The Cybersecurity Tech Accord signatories therefore wholeheartedly welcome this timely, important, but also ambitious project.

While the scope of the High Level Panel's mandate is quite broad, including a wide range of issues related to furthering cooperation in the digital space, our submission will be limited to the core commitment that brings more than 60 global companies together under the Cybersecurity Tech Accord - a commitment to protect and empower civilians online and to improve the security, stability and resilience of cyberspace. We hope that our responses help provide a technology industry perspective, highlighting the lessons of both small players and large multinationals, and serve as a starting point for further collaboration on these dynamic challenges moving forward.

## I. VALUES & PRINCIPLES

A. **What are the key values that individuals, organizations, and countries should support, protect, foster, or prioritize when working together to address digital issues?**

The Cybersecurity Tech Accord is first and foremost a commitment by its signatory companies to abide by four foundational cybersecurity principles, which were developed to reflect the values which we hope will eventually come to underscore the work of the entire technology industry. As mentioned above, the focus of the group is on cybersecurity, but we were nevertheless encouraged to learn that a similar approach is a priority for the Panel as it begins to undertake its mandate.

We hope that the Panel can learn from the principles we have adopted and encourage to adopt them in their own operations and approaches. The Cybersecurity Tech Accord principles are:

**Protect all users and customers everywhere.**

- The 68 Cybersecurity Tech Accord signatories understand we need to earn the trust our users and customers put in the technology we create and to protect those who rely on it and on us. We don't just design, develop and deliver software, hardware and services – we enable and empower people, enterprises and governments to imagine more, reach further, and push the boundaries of possibility. Prioritizing, security, privacy, integrity and reliability of our products and services is therefore critical. While security will never be perfect, we will collectively work to reduce the likelihood, frequency, and severity of vulnerabilities.
- We will strive to protect all our users and customers from cyberattacks, whether they are individuals, organizations, or governments. Online threats will evolve and so too will our efforts to mitigate them. Nevertheless, our focus on protecting our users and customers will remain and we will do so irrespective of the technical acumen, culture, or location of the people using our technology. Moreover, the motives of the attacker, whether criminal or geopolitical, will not deter our companies from this commitment.

**Oppose attacks on innocent civilians and enterprises from anywhere.**

- We invest significant resources in protecting the design, development, and delivery of the software, hardware, and services we deliver. However, each day we face increasing and evolving threats born from a community of sophisticated cybercriminals, as well as from a growing number of countries developing offensive capabilities. With this in mind we will fight hard to actively protect against efforts to tamper with or exploit our products and services.
- We support governments in their law enforcement and national security efforts. Indeed, many of our products and services are used to help governments protect themselves, their citizens, and their economies. Similarly, we will continue to work with law enforcement in responding to lawful requests for data. But, we do not and will not support governments that seek to use our products to attack our customers. Such activities undermine trust in the very foundations of cyberspace.

**Empower users and customers better protect themselves**

- Cybersecurity is not something you buy. It is something we all do, on an individual and company level. Cybersecurity risk management is a continuous process that benefits from partnerships and shared learnings. To that end we will provide our users, customers, and the wider developer ecosystem with information and tools that will enable them to protect themselves against cyberthreats.
- Digital transformation is occurring all around us. The dramatic changes in operations it brings must be met with a re-focus on risk management. This is true no matter where in the world you are and as a result cybersecurity capacity building challenges need to be addressed globally. We recognize our stewardship roles in cyberspace and commit to strengthen this critical element of technology adoption.

**Partner to advance cybersecurity**

- Cybersecurity has been recognized as a shared problem for over twenty years. The industry, experts and policy community have built organizations, launched initiatives, and funded projects to address it. The Cybersecurity Tech Accord signatories recognize these important efforts and participate in many of them, but we understand that more is needed. We came together to articulate our values and commitment to working together to protect customers and users by advancing security, privacy, integrity and reliability across the ecosystem. The Cybersecurity Tech Accord is the first step on that journey.
- Partnership lies at the heart of the Tech Accord. Together we can establish formal and informal partnerships across the industry, civil society, and security researchers, identifying solutions to emerging challenges. However, fostering the next generation of meaningful cybersecurity improvements will not be easy. We need to recognize that there will be setbacks and sobering moments of learning as we drive forward in our efforts to advance capabilities for identifying, preventing, detecting, responding to, and recovering from cyberattacks.

Development of core values and principles is essential for binding together the similarly-minded and simultaneously diverse coalitions of actors that are necessary to achieve real change in this space, whether we look at cybersecurity only, or the digital realm as a whole. In addition, they will over time be able to guide the efforts of the Panel itself, ensuring that any future work remains aligned with the thinking that led to its establishment.

**B. What principles should guide stakeholders as they cooperate with each-other to address issues brought about by digital technology?**

The Cybersecurity Tech Accord signatories convene around four principles, as mentioned above and which we would encourage Panel to adopt as well, but we have found that as important as the principles themselves was the process for establishing them. Our principles were not the product of a single entity determining what reflected the interests and values of the industry, but instead the result of a many months-long consultative process that sought input and feedback from every corner of the technology industry. In seeking to establish a “big-tent” set of principles which would reflect the diversity of the technology industry – chip manufacturers, software developers, cloud service providers, social media

companies, etc – those voices needed to be included in the discussions of the principles themselves. While slower, this deliberate process allowed us to agree upon principles that resonated with the entire industry and pull together the largest-ever industry coalition committed to common cybersecurity principles. This process can hopefully provide a helpful roadmap for the High Level Panel as it seeks input on its own set of principles here, in what we hope is the beginning of more multistakeholder collaboration on identifying values and principles for the Panel.

While the aims of the Panel may not focus on individuals it regards as "users" or "customers," there are likely important parallels between the principles of the Cybersecurity Tech Accord and those being developed by the Panel. For starters, the High Level Panel could recognize the role of the technology industry as being fundamentally opposed to the development and use of malicious cyberweapons through the corruption of peaceful technologies. Moreover, the Panel's work should recognize that we have a collective responsibility across sectors to protect innocent civilians from the impact of cyberattacks, in particular those engineered by nation states, and especially when the impacted populations have limited resources or come from least developed countries. The Panel should also endeavor to include in its principles a commitment to promoting cybersecurity awareness more broadly – as more and more nations come online, all internet users will need to accept some responsibility for safeguarding a secure online environment and be supported in doing so.

Beyond the principles of the Cybersecurity Tech Accord, the Panel should look to the recently announced Paris Call for Trust and Security in Cyberspace for guidance in developing principles related to cybersecurity. The Paris Call is a multistakeholder agreement on principles and a commitment to working together on cybersecurity challenges that has been signed by 55 governments, over 250 industry organizations and 100 civil society groups. It reflects the same multistakeholder approach that should underscore the work of the Panel and reaffirms commitments to previously identified norms in forums like the UN, G20 and G7, while pushing forward with new principles that focus on protecting the core of internet, as well as democratic processes, from cyberattack. Included in the Paris Call is the recognition of the application of international law in cyberspace, and the following specific commitments:

- Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;
- Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;
- Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;
- Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial
- sector;
- Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;
- Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;
- Support efforts to strengthen an advanced cyber hygiene for all actors;
- Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;
- Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

**C. How can these values and principles be better embedded into existing private and/or public activities in the digital space?**

Whatever form discussions on either implementation of existing commitments or development of new initiatives related to cybersecurity take, they should embrace the following three principles: a) leverage an inclusive approach that includes diverse geographical representation; b) ensure multi-stakeholder participation; and c) be open and transparent to increase trust.

Cyber-threats know no borders, nationality, size or wealth. Any discussion of principles, norms, values related to cybersecurity must replicate such diversity. To be effective, any agreement on cybersecurity must be understood and accepted by all countries, irrespective of the size of their economy, their geographic location, or ICT infrastructure. Furthermore, any discussions need to be open and transparent to ensure trust in the online environment is rebuild and retained. Public trust in governments behaving responsibility in cyberspace has been profoundly damaged in recent years. An increase in offensive online activity, in particular if coupled with information operations, could harm it irreparably. In addition, attacks by governments pose a particular problem for the private sector, since a government can utilize a range of tactics and capabilities that non-government cybercriminals normally will not. For example, governments are more likely to taint a supply chain, intercept communications, engage in surreptitious physical searches, and/or affirmatively embed spies into private sector organizations of interest. Additionally, deterrents to cyber-attacks are less applicable to government agents pursuing government missions.

Finally, the ecosystem of potential stakeholders in the development of cybersecurity initiatives needs to be diverse in other ways. The Cybersecurity Tech Accord sees the ICT industry, civil society, and academia as being necessarily involved alongside governments in this process. Not only might governments avoid focusing on certain issue to ensure their national security options are not impacted and should therefore be held accountable by other stakeholders, they might not always understand the technological implications of the decisions they make, resulting in agreements that do not achieve their objectives or are counterproductive. The recent discussions around revision to the Wassenaar Agreement are an unfortunate example.

## II. METHODS & MECHANISMS:

### A. How do the stakeholders you are familiar with address their social, economic, and legal issues related to digital technologies? How effective or successful are these mechanisms for digital cooperation? What are their gaps, weaknesses, or constraints? How can these be addressed?

Often, challenges relating to security have been the express province of governments, however, in the case of cybersecurity, such a model has proven to be inadequate to the nature and scale of the challenge at hand. For one, cybersecurity frequently requires a broader discussion on balancing security with other rights. Secondly, when it comes to development of rules and regulations, the industry knows the technology it produces best and has traditionally worked to develop the most effective standards for it. Finally, the cross-border nature of cybersecurity means that individual countries cannot effectively address the challenges they face and a focus on international agreements is critical.

Therefore, for initiatives to be effective, the cybersecurity initiative development should include a broader set of stakeholders, from private sector and civil society. Their various perspectives and expertise would add value to the process and the eventual outcome of any new conversations. In order to maximize security in cyberspace, organizations across all sectors should cooperate to ensure mutual protection from attacks by states, criminal groups, and terrorist organizations. As a result, as long as the systems and structures in place to facilitate either the domestic or international dialogue on security issues are reserved to government actors, meaningful progress on cybersecurity challenges may remain elusive.

### B. Who are the forgotten stakeholders in these mechanisms? How can we strengthen the voices of women, the youth, small enterprises, small island states and others who are often missing?

To ensure that existing cybersecurity tools and technologies are adopted as broadly as possible, we need to build programs to bring women, the LGBTQ community, minorities, youth, small enterprises, island states, and others into the fold. The tools that allow us to do so can include education, training,

and sponsorships across the industry. Furthermore, a commitment to rural broadband access and information literacy are cornerstones for a safe and stable future.

**C. What new or innovative mechanisms might be devised for multi-stakeholder cooperation in the digital space? How can stakeholders cooperate more effectively in the digital realm, including how can marginalized stakeholders be included?**

As the world proceeds through this period of digital transformation, with more nations and peoples coming online each year, and digitally-enabled connectivity redefining and expanding the ways in which companies conduct business and governments deliver services, it is important that all stakeholders take stock of both shared and respective responsibilities across sectors to contribute to greater security online. While earlier challenges have required a "whole of government" approach, cybersecurity challenges truly require a "whole of society" approach as the owners, operators and users of technology extend across and bleed between the public and private sectors, as well as civil society.

The Cybersecurity Tech Accord has tried to lead by example in this space. Our signatories reflect the diversity of the industry and bring together both small business and large multinationals. We are particularly proud that more than half of our signatories is outside the United States, an unusual composition in many industry groupings and something we have intentionally sought to bring about.

Moreover, the focus on multi-stakeholder cooperation with global representation is core to our work to increase cybersecurity capacity in emerging economies and utilizing modern tools, such as webinars to reach groups that would otherwise struggle to get access to the latest technological trends, as well as of our desire to reach out across sectors to identify partnership opportunities beyond the private sector to address dynamic challenges. To promote a shared understanding of cybersecurity challenges across sectors, the group recently released a set of draft definitions for cybersecurity concepts for comment from the public – the goal of which is to drive common understanding through more normative language.

The Cybersecurity Tech Accord has also been working with civil society organizations, such as the Global Forum on Cyber Expertise (GFCE) and the Cyber Threat Alliance (see below), to create new cybersecurity resources and host events to highlight pressing issues that require a cooperative approach. Finally, the Cybersecurity Tech Accord has been quick to take advantage of opportunities to join with governments in collaborative efforts as well, including joining with over 50 governments in signing the recent Paris Call for Trust and Security and cyberspace and endorsing its principles in a blog post (see above).

## III. ILLUSTRATIVE ACTION AREAS

**A. What are the challenges faced by stakeholders (e.g. individuals, Governments, the private sector, civil society, international organizations, the technical and academic communities) in these areas?**

When it comes to cybersecurity, the core challenge is the one that the Panel is trying to address – the lack of trust and cooperation across the different stakeholder group hinders our progress in this space. More than any other issue in the digital world, cybersecurity is cross-cutting: it affects all aspects of the online environment, and every individual and organization. However, these are all affected differently, respond differently, and are motivated by different incentives, even though they are frequently connected through a mesh of the same products and services, and affected by the same risks. As a result, it is frequently forgotten that cybersecurity is at a fundamental level a shared responsibility that requires cooperation and understanding of the different stakeholders involved.

Another critical issues, one that touches both on security and the need for capacity building, is the vast skills gap we face in cybersecurity across the world. Not only do we face a gap in talent, very few initiatives exist that focus on ensuring that the lessons that have been learnt in the past two decades the hard way in the developed world and translated to emerging economies. The Cybersecurity Tech Accord signatories recognize that the industry has a role to play in closing the digital divide and

protecting new users of technology who are just coming online. In that spirit, the group has partnered with Global Forum on Cybersecurity Expertise (GFCE) in launching a free webinar series in which signatory companies provide trainings and highlight best practices related to their respective areas of expertise in cybersecurity. The content is available through our website and the series will run through the spring, with new webinars added each month that are provide useful information for all users of technology but are tailored to the needs of those in emerging economies.

As cyberattacks are inherently borderless crimes and collective challenges, governments should also recognize that they too have a vested interest in promoting improved cybersecurity across the digital divide, and that poor cybersecurity practices anywhere can quickly become a liability everywhere. To that end, the High Level Panel could play an important role in encouraging governments to partner with one another, as well as with civil society and private industry on further capacity building efforts to better everyone from "weak links" in an increasingly networked world, and to refrain from undermining it through offensive operations.

**B. What are successful examples of cooperation among stakeholders in these areas? Where is further cooperation needed?**

While the Cybersecurity Tech Accord is a fairly new initiative, and primarily focused on exchange of information amongst one core group of stakeholders – the technology industry- it has quickly emerged as one of the most quoted examples of how by brining a set of stakeholders together, you can effect meaningful change. Whether it is a commitment to coordinated vulnerability disclosure, raising awareness of best practices in cybersecurity, or calling on governments to do more when it comes to vulnerability handling, the group has in six short months drove numerous substantive initiatives aimed at increasing the security of the online environment as a whole.

Moreover, the Cybersecurity Tech Accord signatories have recognized that we do not have all the answers and have therefore supported innovative new solutions put forward by civil society organizations. For example, the Cybersecurity Tech Accord has endorsed the Domain-based Message Authentication, Reporting & Conformance (DMARC) initiative, as well as the Internet Society's Mutual Agreed Norms for Routing Security (MANRS). DMARC proposes a new protocol for email authentication, while the MANRS initiative is focused on improving routing security. Importantly, while neither of these initiatives was created by the Cybersecurity Tech Accord or its signatories, they are both made more effective through the support and adoption by the group, who's companies have the ability to apply the initiatives at a much larger scale and protect more customers and users in the process.

**C. What form might cooperation among stakeholders in these areas take? What values and principles should underpin it?**

Possible examples of cooperation and value and principles that could be reflected in the area of cybersecurity were highlighted in the sections above.

## IV. DO YOU HAVE ANY OTHER IDEAS YOU WOULD LIKE TO SHARE WITH THE PANEL?

We would like to once again thank you for the opportunity to provide comments at the outset of the UN High Level Panel on Digital Cooperation. We remain excited about the mandate of the Panel and look forward to subsequent opportunities to work together and provide further input and guidance on issues related to cybersecurity. Should you have any questions that emerge based on our input, please do not hesitate to contact the Cybersecurity Tech Accord through our Secretariat.