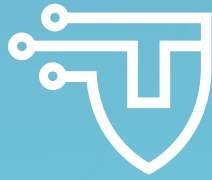


# YEAR IN REVIEW

2021-2022



**Cybersecurity Tech Accord**

The voice of the technology industry on international cybersecurity

# CONTENTS

WHO WE ARE	03
LIVING UP TO OUR PRINCIPLES	08
OUR PARTNERSHIPS	14
TECH ACCORD SIGNATORIES	17

## WHO WE ARE

### About the Cybersecurity Tech Accord

The Cybersecurity Tech Accord is a global coalition of over 150 technology firms committed to advancing trust and security in cyberspace. Since our founding in 2018 with 34 signatories, we have provided a voice for the tech industry to support the protection, stability and resilience of our online world. We firmly believe that protecting this environment is in everyone’s best interest and that all stakeholders have a role to play. To that end, we are committed to responsible behavior that helps protect and empower our users and customers. Over the last four years, we have worked to grow our coalition, establish partnerships across stakeholder groups, and drive dialogue and progress in international cybersecurity forums.

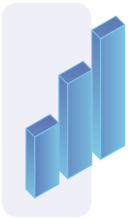
We continue to live our values through our four founding principles:



**1. Stronger Defense:**  
We will protect all of our users and customers everywhere.



**2. No Offense:**  
We will oppose cyberattacks on innocent citizens and enterprises from anywhere.




**3. Capacity Building:**  
We will help empower users, customers and developers to strengthen cybersecurity protection.



**4. Collective Response:**  
We will partner with each other and with like-minded groups to enhance cybersecurity.

Why We Do What We Do

Our priorities	The threats we see
 <p>Ensuring the international community declares cyberattacks against the ICT supply chain out-of-bounds in all instances, including attacks targeting the software update process.</p>	<p>In the US, supply chain attacks rose by 42% in the first quarter of 2021, impacting up to seven million people [Quantum PC].</p>
 <p>Calling for greater international safeguards against cyberattacks targeting the healthcare sector, including classifying healthcare facilities as critical infrastructure in international norms.</p>	<p>Forty-five million people were impacted by healthcare cyberattacks and subsequent data breaches in 2021, an all-time high [Fierce Healthcare].</p> <p>33% of third-party data breaches in 2021 targeted healthcare organizations [Security Magazine].</p>
 <p>Improving the security of connected consumer products by promoting and implementing agreed standards and best practices.</p>	<p>The Internet of Things (IoT) is amplifying the potential cyberattack surface. It is estimated that there are already over 21 billion IoT devices worldwide, and their number will double by 2025 [GARP.org].</p>
 <p>Exposing and helping address the threat posed by private sector offensive actors, or ‘cyber mercenaries.’</p>	<p>Currently <i>estimated</i> to be worth up to \$12 billion, the market for these actors is expected to continue to grow as more companies enter the business of producing and selling dangerous cyber surveillance tools.</p> <p>Private mercenary-style surveillance and hacking groups used Facebook and Instagram to target 50 thousand people in more than 100 countries in 2021 [Technology Review].</p>

Our priorities	The threats we see
 <p>Supporting states in finding solutions to tackle cybercrime while ensuring that internationally rules are recognized to preserve an open internet and to respect fundamental freedoms online.</p>	<p>It is estimated that global cybercrime costs will grow by 15% per year over the next five, reaching \$10.5 trillion annually by 2025, up from \$3 trillion in 2015. This could be the greatest transfer of economic wealth in history [Cybersecurity Magazine].</p>
 <p>Helping address state-led and sponsored cyberattacks by engaging in international discussions on responsible state behavior in cyberspace.</p>	<p>Nearly 80% of nation-state activity targeted enterprises, while 21% focused on consumers. The most targeted sectors were government (48%), NGOs and think tanks (31%), education (3%), intergovernmental organizations (3%), IT (2%), energy (1%), and media (1%). Microsoft alerted customers of nation-state attack attempts 20,500 times in the past three years [Computer Weekly].</p> <p>According to Microsoft, Russia is the source of the lion’s share of nation-state cyberattacks perpetrated in the past year (58%), followed by North Korea (23%), Iran (11%), China (8%), and South Korea, Vietnam, and Turkey all with less than 1% representation [DarkReading].</p>

## A Year In Review: Letter From The Secretariat

Since its launch in 2018, the Cybersecurity Tech Accord has worked to be the technology industry's voice on matters of peace and security in cyberspace and to uphold a commitment to protect users and customers everywhere from evolving cyber threats. As cyberspace continues to emerge as a domain of conflict and competition between states, and criminal activity continues to grow online, the Cybersecurity Tech Accord sets the foundation for the industry's engagement in global efforts to protect a safe and secure online world. Over the last four years, more than 150 technology companies globally have joined as signatories in this effort, committing to shared principles for industry responsibility – *strong defense, no offense, capacity building, and collective action*.

This past year again witnessed continued escalation in the scale and sophistication of malicious activity online committed by a wide range of actors. And beyond these trends, the tragic and unjustified war in Ukraine has ushered in a new age of cyber operations integrated with modern warfare. Cyberattacks have played a large role in the efforts to destabilize Ukraine since before the invasion started, and the conflict is now the first example of large-scale hybrid warfare. Unlike conventional military threats, responding to these cyberattacks has required unprecedented cooperation between government and the private sector, with many Cybersecurity Tech Accord signatories working to detect and defend Ukrainian infrastructure and data.

Against this backdrop, defending a rules-based and rights-respecting online world is more pressing than ever. The international community must act with appropriate urgency to this end, which will require cooperation across stakeholder groups. In the past year, the Cybersecurity Tech Accord has worked to advance this mission by providing guidance and input across diplomatic forums. This includes engaging in the United Nations (UN) dialogues on responsible state behavior online, leading a working group of the Paris Call for Trust and Security in Cyberspace, and working with partners across industry, government, and civil society to improve cybersecurity practices and strengthen international expectations online.

Throughout this report, you will find examples of these efforts and the breadth of activity the Cybersecurity Tech Accord has engaged in over the past year to step up and take more responsibility as an industry for cybersecurity trends and challenges. We are grateful to the numerous partners from across stakeholder groups that are featured in this report who have helped drive this work over the past year. Looking ahead, we encourage others from the technology industry to join our efforts, and those from other stakeholder communities to review the contents of this report and consider additional ways we might cooperate towards a more peaceful and secure online world together.

As the world continues to grapple with new cyber threats and hybrid warfare, and with how to respond in order to bring greater security and stability to the digital domain, the Cybersecurity Tech Accord will continue to be a reliable and consistent advocate in support of developing meaningful solutions. We stand ready to provide expertise and advice on how to ensure technology is used for the peaceful purposes it was intended for.

Sincerely,  
The Cybersecurity Tech Accord Secretariat

## Signatory Spotlight: Eva Chen, Trend Micro, CEO



### 1. What motivated your company to join the Cybersecurity Tech Accord as a signatory?

Trend Micro has been a leader in cybersecurity for the past 34 years and our mission is to make exchanging digital information safe. The Cybersecurity Tech Accord was established to improve cybersecurity around the world by working with many different types of organizations and nation/states. As such, it was a natural fit for our company to help start this Accord and we're proud to be a founding signatory and to contribute our vast knowledge and resources to the cause.

### 2. What do you believe are the greatest cybersecurity threats that organizations face today?

The cyber risks facing businesses today are plenty, from extortion attacks like ransomware and targeted attacks by sophisticated malicious actor groups, to even cyber warfare from nation/states. Many organizations today are challenged with understanding their attack surface and minimizing the risks associated with this lack of visibility to ensure they can stave off an attack. The lack of trained personnel is also a major challenge for global organizations, as they cannot fill many of the cybersecurity roles they need. Finally, the lack of cooperation with many nation/states who harbor malicious actors and allow them to continue to attack businesses, needs to be addressed by world leaders.

### 3. What unique perspective on security challenges does your company bring to the Cybersecurity Tech Accord?

Trend Micro's vast experience in combatting cyber threats over our 34 years and the depth and breadth of our research have allowed us to address cyber challenges across an entire organization's network. We are able to invest in innovative technologies to address these threats across the endpoint, messaging, network, cloud, and even into IoT/Industrial IoT, as with smart homes, factories and vehicles. Our unified cybersecurity platform approach through Trend Micro One gives us a unique difference in this industry that can help businesses deal with their entire attack surface. We also are able to utilize our resources to help educate people around the world with our CPITS program that regularly trains new cybersecurity professionals from varied backgrounds, which is helping address the talent shortage. Finally, we are able to give back to communities around the world through our vast corporate social responsibility programs like building houses in the Philippines, donating funds for earthquake relief in Japan, working with local parent-teacher organizations in the United States, or providing Safe Surfing e-posters to 100 schools in Belgium. We also empower our employees to share their time and expertise with others.

### 4. How do you see our efforts in the space evolving in the coming years?

The Cybersecurity Tech Accord can take advantage of its broad support by continuing to work with diverse global signatories to bring much needed visibility to the need for improved cybersecurity. The ability to participate in initiatives like the UN Open-Ended Working Group on Cybersecurity or working with the Cyber Peace Institute support. Many Tech Accord initiatives are helping to bring light to cybersecurity in areas that need addressing like the Consumer IoT working group, Women in Tech, and bringing light to the need for a vulnerability disclosure process. All of these initiatives are helping to shed light on the need to improve cybersecurity around the world for any organizations or helping nation/states understand the needs of their citizens and organizations within their countries.

### 5. Where do you see the Cybersecurity Tech Accord making the biggest impact?

The Tech Accord will have the biggest impact through the continued recruiting of signatory organizations from around the world and across diverse industries that will help bring higher visibility to cybersecurity. The ability to have a voice in nation/state discussions around cybersecurity could be a very big opportunity to bring a much needed role of the private sector having a say in how nation/states address cybersecurity. Trend Micro will continue to support the Cybersecurity Tech Accord in the future with our expertise, resources, and our passion for making the world safer.



Eva Chen  
Trend Micro, CEO



# LIVING UP TO OUR PRINCIPLES

## How we Live Up to Our Principles

As we celebrate the Cybersecurity Tech Accord’s fourth anniversary, we reflect on the four foundational principles that have guided our shared commitment and efforts. Most importantly, we look at the initiatives that define us as the leading industry voice on peace and security in cyberspace. Our work spans industry engagement by supporting our signatories to do more to improve cybersecurity for users and customers everywhere and high-level policy advocacy around critical issues concerning cyberspace security. The past year has been particularly fruitful. We led the way on multistakeholder inclusion in the context of the United Nations dialogues on responsible state behavior in cyberspace. The year was also about industry collaboration and broader multistakeholder initiatives on issues ranging from cybercrime to IoT security.

### Principle 1: Stronger Defense

**Securing the next generation of connected consumer products:** Although the advent of the Internet of Things (IoT) has brought incredible benefits to consumers, it also ushered in new cybersecurity risks. Governments, IoT device manufacturers, security researchers and consumer groups alike have a role in making IoT devices more secure and ensuring that the benefits outweigh these evolving risks. In recognition of this challenge, the Cybersecurity Tech Accord partnered with Consumers International, I am The Cavalry and the World Economic Forum to launch a [statement](#) in support of the global consensus forming around five baseline security capabilities for consumer IoT products. The statement garnered the support of over 100 organizations. Widespread implementation of these five security capabilities will be an important step towards a future where every consumer can expect basic security features in their connected devices. Consumer-facing IoT devices must:

- 1 **Not have default universal passwords;**
- 2 **Implement a vulnerability disclosure policy;**
- 3 **Keep software updated;**
- 4 **Have secure communication; and**
- 5 **Secure personal data.**

We encourage governments worldwide to promote these provisions and urge manufacturers and vendors to take immediate action to implement them.

#### Spotlighting the risk of cyberattacks on governments, private sector companies and consumers.

In partnership with GZERO Media and Microsoft, the Cybersecurity Tech Accord launched a 5-part podcast series titled: *Patching the System* as part of GZERO Media’s Global Stage Podcasts. The podcast series focused on engaging signatories from the Cybersecurity Tech Accord as well as business leaders and experts from the cybersecurity community to discuss crucial issues of importance to the tech industry. Each week the podcast focused on a different subject, including: hybrid warfare, UN treaty negotiations, ICT supply chain security, the dangers posed by cyber mercenaries, and protecting the ever-growing world of "smart" devices.



**Addressing threats emanating from state actors in cyberspace:** State-led and sponsored cyberattacks are an increasingly pressing issue causing geopolitical instability and impacting the security of government organizations, businesses and individuals. Our survey "*Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats*," conducted in partnership with the Economist Intelligence Unit and published early last year, has served as our guiding light and continues to inform our initiatives. The findings revealed that more than 500 director-level or above executives from businesses in the Asia-Pacific, Europe and the United States perceive these attacks as a major threat. . The results were sobering and highlighted the need for a fundamental shift in security planning and an increased urgency for effective policy solutions at the national and international levels. Over 80 percent of executives confirmed they were more concerned about their organization falling victim to state-led or -sponsored cyberattacks than five years ago and that COVID-19 had heightened that risk further. As potential solutions, private sector leaders and security experts across different industries worldwide flagged stronger international economic and political cooperation as essential to address these challenges and cultivate a more secure and stable online environment.



### Principle 2: No Offense

#### Advocating for responsible state behavior in cyberspace in the context of the United Nations (UN) dialogues on cybersecurity:

As the leading industry voice on peace and security in cyberspace, the Cybersecurity Tech Accord has consistently sought active participation in the UN dialogues on the security and use of information and communications technologies (ICT). Last year was marked by several important milestones as both the UN Open-Ended Working Group (OEWG) and UN Group of Governmental Experts (GGE) on ICT security adopted consensus reports confirming international law’s applicability to cyberspace and the framework of 11 norms for responsible state behavior in this new domain. As the OEWG started its

2021-2025 mandate last year, we continued seeking engagement and joined the informal consultations with stakeholders held by the OEWG Chair, Ambassador Burhan Gafoor. In our interventions, we focused on:

- The need to recognize cyberattacks against the ICT supply chain as off-limits as well as to agree on specific prohibitions against cyberattacks on healthcare organizations;
- The importance for states to release independent statements on how they understand international law applies to state behavior in cyberspace to promote transparency and build consensus; and
- The need for capacity building efforts to be recognized and encouraged by the OEWG to focus on improving cyber governance and digital diplomacy capabilities.

**Building a united multistakeholder front for a new, balanced cybercrime convention:**

In the context of the negotiations over a proposed new cybercrime treaty at the UN, which began in January 2022, the Cybersecurity Tech Accord joined the CyberPeace Institute and over 60 other private sector and civil society organizations in launching a **Multistakeholder Manifesto on Cybercrime**. The Manifesto calls on states to balance all attempts to tackle cybercrime with the need to protect fundamental freedoms and human rights online and preserve a free and open internet. The document lays out principles to guide governments in the upcoming negotiations. In particular, the Manifesto encourages governments to establish an inclusive process in which industry can provide technical expertise, and civil society can highlight what is required to protect human rights. In short, the Manifesto clarifies that a new cybercrime convention cannot be negotiated behind closed doors and must prioritize the needs of victims over the needs of states. Initially launched in French and English in October 2021, the Manifesto was translated into Arabic, Mandarin, Russian and Spanish and relaunched in December to ensure a wider geographical reach.



**Calling for multistakeholder participation at the United Nations:**

Last year, the Cybersecurity Tech Accord successfully chaired the Paris Call Working Group 3 (WG3) on "advancing the UN negotiations with a strong multistakeholder approach." More than 80 stakeholders from the broader cybersecurity community participated in our online workshops, including representatives from governments, academia, industry and civil society organizations. The French Ministry for Europe and Foreign Affairs followed the proceedings of WG3 closely and shared their ambitions around reforming the UN dialogues on cybersecurity, including plans for a more structured engagement with stakeholders. As part of this work, we produced a study titled: **"Multistakeholder Participation at the UN: the need for greater inclusivity in the UN dialogues on cybersecurity."** The study was the result of months of engagement and discussions. Addressed to policymakers and diplomats that will design the next generation of cyber diplomacy at the UN, the study makes a case for enhanced collaboration across stakeholder groups around these issues and provides recommendations on ensuring greater inclusivity in the UN dialogues on cybersecurity.



**Principle 3: Capacity Building**

**Supporting the development of governments' cyber diplomacy capabilities:**

International cybersecurity cannot be based on dialogues from a limited number of cyber powers alone. In our connected world, all nations must help establish, uphold and abide by international commitments to improve security for all. To honor Cybersecurity Awareness Month, the Tech Accord published a study titled: *"Towards effective cyber diplomacy: A guide to best practices and capacity building."* The report provides tools for cybersecurity diplomats and a roadmap to help countries build up their cyber diplomacy capabilities. In particular, the report to supports 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. Just as closing the so-called "digital divide" is essential to building an inclusive global economy, the inclusion of all countries in cyber diplomacy negotiations is imperative for building a secure, equitable and rights-respecting online world that reflects a diversity of interests and needs.

**Tech Accord signatories on pressing cybersecurity challenges and solutions:**

Last year, security experts from several Cybersecurity Tech Accord signatories continued to shed light on pressing cybersecurity challenges and solutions and the ways organizations can better protect from evolving cyber threats, through pieces including:

- Top Six OEM IoT Security Challenges to Tackle in 2021 (Arm)
- A connected world needs unified cybersecurity standards (Eaton)
- Cybersecurity capacity building: A foundational element of international peace and stability online (Microsoft)
- Improving Security Posture Through The 4-step Gap Analysis Process (Pax8)
- The Question Your Cyber Team Must Answer: What's (Unintentionally) Exposed to the Internet? (RedSeal)

- [Email Protection 101 \(Safe PC Cloud\)](#)
- [Governments and Industry Must Collaborate to Address Third-Party Security Threats \(Schneider Electric\)](#)
- [SolarWinds Hack Calls for New Approach to Cyber Defenses \(Synack\)](#)
- [Risk Management for Vulnerabilities \(Trend Micro Inc.\)](#)

**Celebrating women in cybersecurity:**

To honor International Women’s Day, we launched the campaign [#MyCybHerStory](#). Throughout March 2022, our signatory representatives shared their stories about finding and thriving in a career in cybersecurity. The stories of these inspiring women sent a clear message to women and girls everywhere that might embark on this professional journey: cybersecurity needs your talent, representing all dimensions of diversity, now. As we know, cybersecurity is a field in constant evolution that requires a diverse workforce. However, data proves that the sector is affected by a major talent gap that is especially pronounced when it comes to gender. Diverse perspectives are also crucial to international political discussions on cybersecurity, namely the United Nations (UN) dialogues on responsible state behavior in cyberspace. Problems related to digital peace and security are extremely complex, requiring a multitude of voices around the negotiating table with expertise on issues from technical to geopolitical.



**Discussing ways to rein in cyberattacks by states:**

Over the last decade, RightsCon has brought business leaders, human rights advocates, governments, technologists and journalists together to address critical issues at the intersection of human rights and technology. In 2021, the Cybersecurity Tech Accord was honored to host the workshop, "Playing by the Rules: working together to reign in nation-state cyberattacks." The session included a panel of experts who examined the evolving threat posed by state-sponsored cyberattacks, their impact on businesses and society and the government’s role in addressing this pressing issue in cyberspace. The session provided an opportunity to bring together the multistakeholder community forming around the Paris Call WG3, which was tasked with exploring ways to make future UN discussions on cybersecurity more inclusive.



"Ensuring diversity of backgrounds and experiences of cybersecurity professionals is vital in a world where threat actors are extremely skilled and evolve every day. No one perspective is sufficient to provide answers to today’s cybersecurity challenges. Moreover, when gender is a factor in narrowing the pool of people pursuing cybersecurity careers, we exacerbate the already problematic shortage of cybersecurity skills."

**Statement by the Cybersecurity Tech Accord and Women4Cyber.**



**Principle 4: Collective Response**

**Rethinking the international dialogues on cybersecurity:** Our experience chairing the Paris Call Working Group #3 (WG3) on advancing multistakeholder inclusion in cybersecurity dialogues in the United Nations (UN), highlighted how global engagement in cybersecurity requires structural changes to increase inclusivity in the constantly evolving digital domain. We were **excited** to see the proposal by several governments for a UN "Programme of Action" (POA) on cybersecurity to serve as a standing body to facilitate greater cooperation and diplomacy for stability in cyberspace. The Cybersecurity Tech Accord has long advocated for greater multistakeholder participation in the UN cybersecurity dialogues – especially regarding the technology industry. Recently, the French government, supported by over 50 other states, introduced a proposal calling for a "Programme of Action for advancing responsible State behaviour in cyberspace" at the UN. And while the PoA remains just a proposal, for the time being, it has the potential to structure a more impactful and consequential dialogue moving forward. The Cybersecurity Tech Accord stands ready to engage with this new forum and will continue to **engage** in international discussions on cybersecurity, including the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG) and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Cybercrime Treaty).



# OUR PARTNERSHIPS

As an engaged and active member of the multistakeholder cybersecurity community, in the last year, the Cybersecurity Tech Accord partnered with governments, like-minded businesses, civil society groups, and academics on a range of initiatives. Collaboration is core to our mission, and we see it as fundamental to comprehensively and inclusively addressing the increasing cybersecurity threats that our world faces.

Over the course of last year, our partnerships allowed us to reach new audiences, dive deeper into the issue of multistakeholder participation in cybersecurity governance through studies and position papers, and advocate for shared goals. Here is how some of the partners we have worked with highlighted the importance of our collaboration:

**Dr. Madeline Carr**  
Professor of Global Politics  
and Cybersecurity & Co-  
Director of the Doctoral  
Training Centre for  
Cybersecurity, University  
College London



"Throughout 2020, the Research Institute in Sociotechnical Cyber Security (RISCS) partnered with the Cybersecurity Tech Accord, Consumers International, and Meet the Cavalry to take action on improving the cybersecurity of connected consumer devices. We worked together through the World Economic Forum Council on the Connected World to develop a consensus statement promoting five positive steps manufacturers and service providers can take to mitigate the security vulnerabilities introduced by consumer IoT devices. Through the WEF Council, we carried out an intensive consultation period and presented this statement to a diverse set of stakeholders in industry, academia, the third sector and government to seek feedback and input. In February 2022, we launched the statement with the support of over 100 endorsers.

A powerful element of this initiative was how we were able to work together through the WEF to establish a consensus statement from such a diverse stakeholder group. The process itself highlighted the extent to which these different groups need to collaborate on cybersecurity to effectively represent the technical, economic, human, and organizational factors that shape both the problems and the solutions that arise from emerging technology. The commitment of those tech companies working through the Cybersecurity Tech Accord to act responsibly, protect and empower users and customers, and improve the security, stability, and resilience of cyberspace is central to what we set out to achieve with this initiative. Engaging tech companies in a positive, constructive way to improve cybersecurity outcomes is essential, and this initiative demonstrated how effective that kind of collaboration can be."

**Anne Marie Buzato**  
Vice-President and  
COO of ICT for Peace  
Foundation



"Effective governance for a secure and peaceful cyberspace requires meaningful participation by all relevant stakeholders, including civil society and the private sector. To this end, the Cybersecurity Tech Accord launched a series of working group sessions focused on how to best include the multistakeholder community in UN (GGE and OEWG) processes.

ICT4Peace Foundation was pleased to chair one of these sessions, which examined other examples of multistakeholder governance processes to inspire multilateral working groups. Through these discussions, participants were able to identify challenges, opportunities and lessons learned from other multistakeholder initiatives that could be applied to designing effective governance and oversight frameworks for cyberspace. In this digital space, governments, companies and civil society have their particular areas of expertise or "effective control." As such, successful governance can only be achieved when these different actors each identify their specific expertise and work together in concert towards a common set of goals. Ultimately, this should help ensure a safe and accessible online environment that brings us together to work, learn and play to realize the potential of a safe and peaceful cyberspace. The work of the Tech Accord is essential in making that vision a reality."

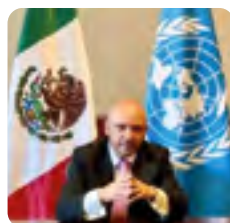
**Klara Jordan**  
Chief Public Policy Officer  
at Cyberpeace Institute



"The Cybersecurity TechAccord played a key role in mobilizing global industry players for a joint multistakeholder initiative with the CyberPeace Institute to outline a set of principles to inform the negotiations of the UN Cybercrime Convention to ensure the process respects the free, open, secure, and peaceful cyberspace and strengthens the rule of law. "



**Isaac Morales**  
Ministry of Foreign  
Affairs of Mexico  
Vice-President and  
COO of ICT for Peace  
Foundation



"Partnering with Cybersecurity Tech Accord has resulted in a one of the most substantive and timely collaborations I've had as representative of Mexico to cyber issues. By joining the RighthstCon2021 Panel titled: *Playing by the Rules: working together to reign in nation-state cyberattacks*, I experienced firsthand the commitment of the Cybersecurity Tech Accord to raise awareness and contribute to the international discussion on the core multilateral cybersecurity process.

By promoting plural and comprehensive debates and stimulating cooperation and development of cyber capabilities, the Cybersecurity Tech Accord has strived to provide the multistakeholder community with a unified voice and help governments around the world better address challenges in cyberspace.

Mexico and the Cybersecurity Tech Accord share the common interest of promoting the implementation of the UN norms for responsible state behavior in cyberspace as well as the applicability of international law and confidence building measures (CBMs) and capacity building programs to achieve the peaceful, responsible, open and safe use of information technologies. The Cybersecurity Tech Accord is a platform that allows us to visualize the enormous development potential that the use of these technologies represents, which is something that we should not ignore, since it is also a commitment to sustainable development, and at the same time, disseminates valuable knowledge on how to have safe technological infrastructures that allow the development of said potential."

**Daniel McBryde**  
Senior Policy  
Advisor for Global  
Affairs Canada

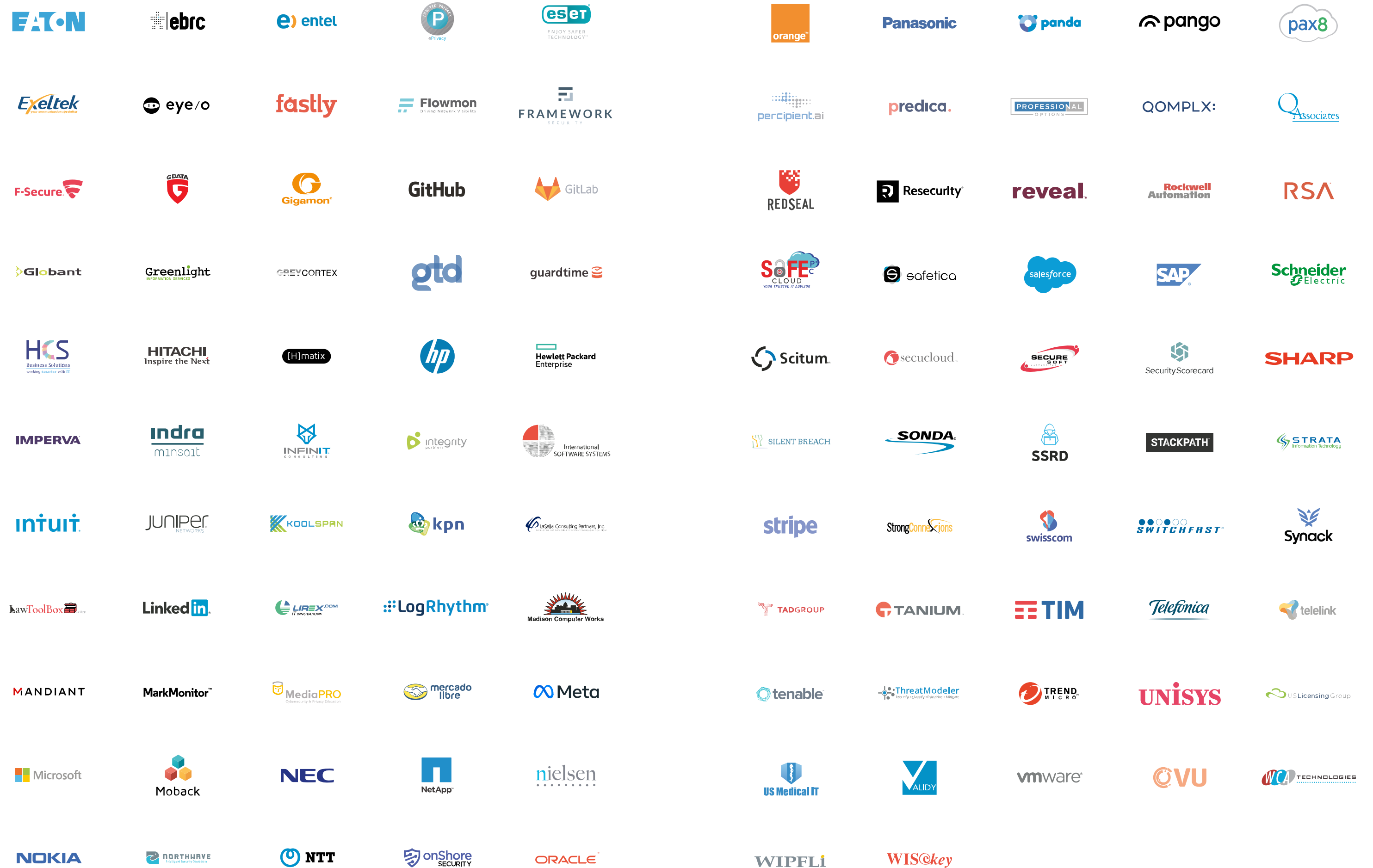


"Canada is a strong supporter of the multistakeholder approach in UN cyber processes. We fought for more transparent stakeholder modalities at the OEWG and are keen to do even better at an eventual UN cyber PoA. We were pleased to participate in meetings of the Paris Call's Working Group 3 on Supporting the Continuation of UN Negotiations with a Strong Multistakeholder Approach. This group generated many good ideas on stakeholder modalities and how to promote stakeholders' participation in UN cyber processes in both the formal and informal spaces."

## TECH ACCORD SIGNATORIES

We welcome others who share our commitment to the Cybersecurity Tech Accord principles to get involved and join this effort. For more information, visit [www.cybertechaccord.org](http://www.cybertechaccord.org) or contact our secretariat at [info@cybertechaccord.org](mailto:info@cybertechaccord.org)







FOR INFORMATION ON THE CYBERSECURITY TECH ACCORD,

PLEASE EMAIL [INFO@CYBERTECHACCORD.ORG](mailto:info@cybertechaccord.org)