BUILDING A VOICE FOR PEACE AND SECURITY ONLINE

The Cybersecurity Tech Accord's First Five Years

Cybersecurity Tech Accord
The voice of the technology industry on international cybersecurity

CONTENTS

FIVE YEARS IN REVIEW: LETTER FROM SECRETARIAT 03

THE FIRST ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER 05

ABOUT THE CYBERSECURITY TECH ACCORD 09

NEW SIGNATORIES ANNOUNCEMENT 09

TIMELINE OF FIVE YEARS OF COOPERATION 10

OUR COMMITMENT IN ACTION 14

- Strong Defense 15
- No offense 17
- Capacity Building 19
- Collective Response 21

OUR PARTNERS 24

SIGNATORY SPOTLIGHT 26

SIGNATORIES 28

FIVE YEARS IN REVIEW

Letter from the Secretariat
April 2023

In April 2018, 34 global technology and security companies signed the Cybersecurity Tech Accord, a watershed agreement among the largest-ever industry coalition committing to defend all customers everywhere from malicious cyberattacks, irrespective of where they originate, and to not participate in offensive cyber operations.

The pledge our signatories first signed five years ago was much more than a simple rubber-stamp agreement: it marked the beginning of a journey of collaboration and the establishment of a partnership unlike any other in our industry. Over the last five years, the Cybersecurity Tech Accord has evolved to play an increasingly important role as the voice for the technology industry on matters of peace and security online and grown into the largest industry-led effort of this kind. Today, our membership has reached 156 signatory companies from across the world pledging to work together to improve the security, stability, and resilience of our shared cyberspace. This nearly 5X expansion of the signatory base demonstrates the importance of our initiative and our work, as well as the growing awareness across the tech sector that our industry needs to take more responsibility for advancing responsible behavior and a rules-based and rights-respecting online world.

Much has changed in five years and today's world is not the same as when our organization began in 2018. The Cybersecurity Tech Accord was founded in the wake of devastating cyberattacks like WannaCry and NotPetya, incidents orchestrated by criminal organizations and nation states that crippled enterprises around the world and caused then unprecedented losses in the billions of dollars. As alarming as those attacks were, however, they were not the high-water mark. Conflict in cyberspace has only escalated in the years since. Over the past five years, the use of cyberweapons and cyberspace as a domain of conflict has accelerated drastically. This acceleration is, in part, tied to new market trends like the rapid rise in popularity of cyber mercenaries by states and the quick uptake of new technologies for malicious uses. The Center for Strategic & International Studies recorded more than 130 significant cyberattacks on government agencies, defense, and tech companies in 2022 alone.

Certainly, the most concerning development in recent years has been the use of cyber operations in an armed conflict. The world no longer needs to speculate about what "cyberwarfare" will look, as the illegal Russian invasion of Ukraine forever transformed the nature of armed conflict as the first ever example of large-scale hybrid warfare. What were once isolated malicious cyber incidents and operations, have become well-funded, strategic, large-scale cyberattack campaigns integrated with and complimenting kinetic military operations. It is clear that cooperation between governments and the technology industry must remain a priority, as our industry continues to actively detect, defend and disrupt attempts to undermine peaceful technology.

The technology landscape has shifted dramatically as well. Internet of Things (IoT) devices that were once novel are now ubiquitous, bringing with them added cyber risk and new responsibilities while consumer awareness remains low. While increased connectivity brought by the rise of IoT devices and other technology advancements are helping address urgent societal challenges – from improving education and healthcare to advancing agriculture, business growth, and job creation – the Cybersecurity Tech Accord recognizes that there is need for a strong global baselines for improved security in the next generation of technology products and services.

From the beginning, the Cybersecurity Tech Accord has played an active role in representing the technology industry at multilateral and multistakeholder forums on international cybersecurity, including most notably at the United Nations (UN). The Cybersecurity Tech Accord has for years

been the leading industry organization to provide input into the work of the UN's Open Ended Working Groups on information security, the Ad-Hoc Committee on the establishment of a Cybercrime Treaty, the Programme of Action on ICT, and the UN's Conference on Disarmament. We have also engaged extensively with and represented the technology industry at the Internet Governance Forum, Global Forum for Cyber Expertise, the World Economic Forum, and the Paris Peace Forum, where we were proud to chair a working group of the French Government's Paris Call for Trust and Security in Cyberspace, on supporting multistakeholder inclusion at the UN.

OUR FIVE-YEAR ANNIVERSARY IS AN OPPORTUNITY FOR US TO REFLECT ON OUR WORK TO DATE, THE FUTURE OF OUR INITIATIVE, AND THE FUTURE OF OUR INDUSTRY.

As we look to the next five years, uncertainty and instability in cyberspace are likely to continue amid rising geopolitical tensions. While unfortunate, this underscores the need for our coalition to exist; to uphold responsible practices for our industry and to inform international discussions to promote peace and security online. The Cybersecurity Tech Accord is confident that the role of responsible and engaged industry actors will only grow more important in the years ahead. We will continue to advocate for the inclusion of industry in international discussions on global norms, international law, and best practices when it comes to cybersecurity.

In line with the commitment we made five years ago to report publicly on our progress in achieving our goals,[1] the following report provides a comprehensive review of our activity over the past five years. Like every year, the Cybersecurity Tech Accord uses this opportunity to spotlight our signatories, our partners, and the organizations and individuals who are aligned with our mission to ensure the safe and open use of the internet is protected. This report also includes a new section that the Cybersecurity Tech Accord is committing to publish every year: *The Annual State of International Cybersecurity Thermometer from the Cybersecurity Tech Accord*, an assessment made by our industry community taking stock of the current state of conflict and security online, and how it has changed over the past year.

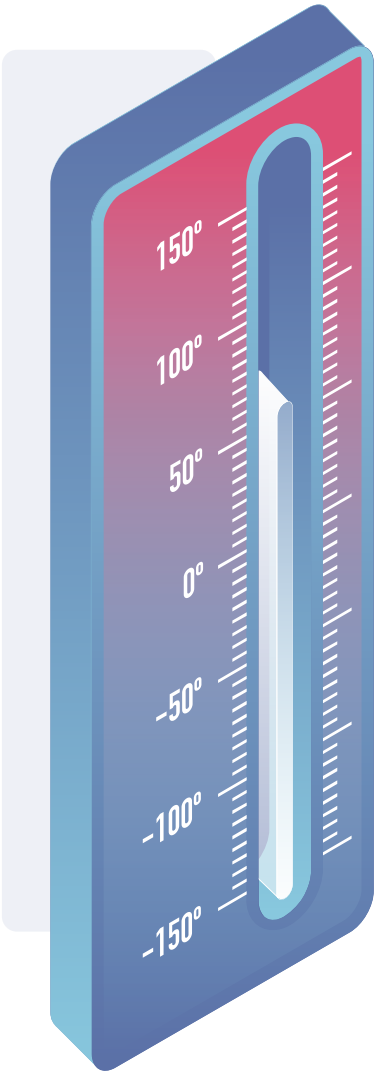
Edoardo Ravaioli
Head Secretariat

1 Find our previous Annual Reports on our website: 2018 In Review, 2019 In Review, 2020 In Review, and Year in Review 2021.

THE FIRST ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER

Taking the temperature of cyber conflict

Launched in 2018, the Cybersecurity Tech Accord is a coalition of more than 150 global technology companies committed to foundational cybersecurity principles for responsible industry behavior. In the years since, the coalition has served as the voice of the technology industry in discussions around peace and security online as the world has continued to sleepwalk into seemingly ever-escalating cyber conflict. This trend is untenable, and the international community should not simply accept that with each passing year the breadth and severity of malicious activity online will escalate – especially when it comes to state cyber operations. To help address this, the Cybersecurity Tech Accord is launching the "State of International Cybersecurity Thermometer", an annual assessment provided by our community of industry experts. The Thermometer aims to take the "temperature" of current cyber conflict, evaluating developments over the past year and their contributions to overall cyber stability and security.
This evaluation will be expressed on a Celsius thermometer and based on common water temperatures for reference, with the following scale in mind:



100° AND ABOVE CYBER WARFARE

This "gaseous" state reflects the chaotic and dangerous conditions past a boiling point. This would suggest the use of cyber operations – for destruction, espionage, and influence – in the context of an armed conflict or war that has harmed and/or targeted civilians. While the scale and severity of such cyber warfare can vary, this abuse of technology that harms innocent people is obviously the worst-case scenario. Evidence of this would be the wonton use of cyber operations in warfare in violations of international norms and/or international legal requirements that puts non-military targets at risk.

0° – 99° CYBER CONFLICT

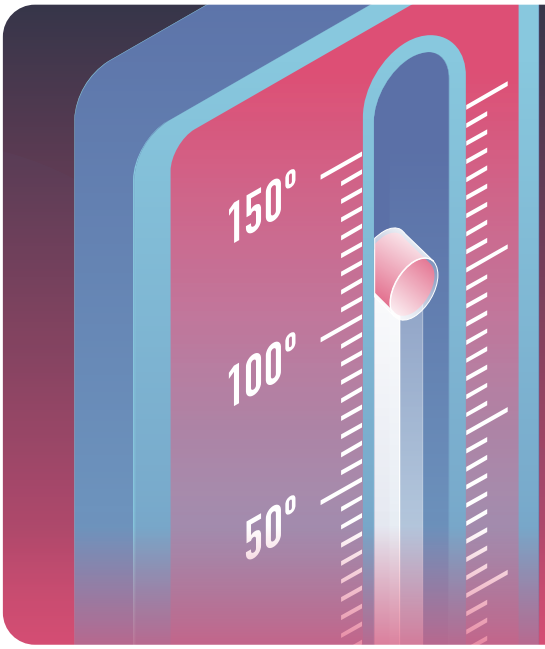
This "liquid" state reflects some degree of cyber conflict short of armed conflict or warfare. It would be characterized by a lack of clarity around international expectations online and/or some degree of inability to uphold or enforce such expectations. Evidence of this would include reckless cyber activity by nation state actors, regularized abuses by other sophisticated actors, and limited progress in diplomatic forums to advance a global framework for responsible state behavior online.

LESS THAN 0° CYBER STABILITY

This "solid" state reflects stability in international cybersecurity. It would require the existence of a clear rules-based order online with a robust international system in place to uphold such expectations. This would be characterized by a scarcity of state-sponsored cyber operations that violate international norms, as well as limited threats posed by other sophisticated actors.

Cyberspace has emerged as a distinct domain of conflict, as evidenced by the growing number of states dedicating military and diplomatic resources to it and the increasing frequency of offensive cyber operations. As with other physical domains of conflict, it is essential to build the necessary rules, processes and institutions to promote stability, security and human rights online, and to discourage abuses.

In evaluating the annual state of cyber conflict, the Cybersecurity Tech Accord considers significant developments from the past year across three criteria: (i) diplomatic and institutional progress, (ii) the scale and nature of cyber conflict, and (iii) technological developments.



IN 2023, THE CYBER CONFLICT THERMOMETER NOW READS 100°, THE "BOILING POINT."

This evaluation is based on several increases in cyber conflict in the past year, most notably the widespread use of cyber operations in Russia's war in Ukraine that began in 2022. Despite some positive signs of necessary institutional development to address escalating cyber conflict, there was insufficient diplomatic progress in the past year to suggest that the international system is prepared to promote accountability for behavior that violates established international expectations. We consider this a shift in the wrong direction, as the temperature would have been considered below 100° in prior years.

Major indicators and developments in past year driving this evaluation:

Diplomatic and institutional progress

NEGATIVE

Limited progress within UN working group:

In the face of rising geopolitical tensions and the widespread use of cyber operations in warfare, the UN working group tasked with deliberating responsible state behavior online has made very limited progress. The working group has consistently voted to exclude participation of relevant nongovernmental stakeholders, including the Cybersecurity Tech Accord and other industry voices, in a series of formal substantive meetings over the past year. Unfortunately, there has been seemingly no political will among member states for cooperation in establishing accountability measures or necessary new norms for responsible behavior online. The UN General Assembly also voted to establish a "Programme of Action" on cyber in the past year that could serve as a more robust and inclusive body in the future, but much will depend on how it is structured and implemented.

Global investment in cyber diplomacy:

It's important to have the necessary diplomatic capacities to engage on matters of peace and security online as geopolitical tensions rise. It was encouraging to see the United States (US) last year pass the Cyber Diplomacy Act and elevate the status of these issues by establishing a new Bureau for Cyberspace and Digital Policy at the State Department, led by a new Ambassador-at-Large. Similarly, the European Union (EU) debuted a more streamlined approach and expanded investment in digital diplomacy last summer when it announced plans for a new office focused on these issues to be opened in Silicon Valley. Meanwhile, Singapore continues to advance cyber diplomacy capacity building via its investment in the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) that provides associated trainings and workshops with partner countries.

Scale and nature of cyber conflict

Cyberwar in Ukraine:

Beginning in February of last year, cyber operations have been regularly employed in the world's first ever large-scale hybrid war: Russia's illegal invasion of Ukraine. This unprecedented use of cyber capabilities – both destructive attacks and information operations – has been coordinated with kinetic activities and targeted both government and civilian infrastructure. This has included reports of cyberattacks against the most sensitive infrastructure, including nuclear power plants, illustrating that apparently no targets are off limits.

Multistakeholder response in Ukraine:

While the use of cyber operations by Russia in Ukraine has been a very concerning development, the response from industry and civil society has been a bright spot. Numerous companies, including many Cybersecurity Tech Accord signatories, stepped up early in the conflict to provide support to protect sensitive Ukrainian data and infrastructure from cyberattacks. This included hardening defenses, migrating data to more secure environments, and in some cases, taking action against cyber operations.

Escalating numbers of sophisticated attacks:

The scale and sophistication of cyberattacks continued to increase in raw numbers over the past year. According to data maintained by CSIS, there were more than 130 "significant cyber incidents" reported in 2022, continuing an upward trend of more than a decade now.

Aligned opposition to cyber mercenaries:

The market for cyber mercenaries — private companies that develop offensive cyber tools — has been growing for years. But in recent months, we've witnessed increased unified opposition to their use. This was reflected in an Executive Order from the Biden administration in the US that curbs their use, as well as the principles on how industry can push back on cyber mercenaries released by the Cybersecurity Tech Accord.

Rise of "hacktivist" groups:

Beyond government-led cyber operations, the invasion of Ukraine has also brought about a significant rise in activity from politically motivated but independent malicious hacker groups on either side of the war. And the phenomenon is not limited to that one theatre, as there has been a notable spike in hacktivist activity in recent months around the world spurred on by geopolitical tensions elsewhere.

Technological developments

Attacks on ICT supply chain:

Over the past year there has been increased targeting of the ICT supply chain, in particular by state actors – compromising technology elements to target users and customers downstream. This kind of compromise, including the targeting of software update mechanisms, is inherently indiscriminate and irresponsible as it involves compromising numerous unintended computer systems in the process.

Rise of Artificial Intelligence (AI):

Certainly, the largest technology story of the past twelve months has been the rise of next-generation generative AI programs. Given the novelty of this advancement, it is difficult to determine what its full impact will be on security across the digital ecosystem. Early benefits will include security applications that help to address the cybersecurity skills shortage by improving analytics, security practices, and automating certain processes at scale. To be sure, there will also be malicious applications to support offensive activities, but on balance near-term applications will help improve ecosystem security.

Taken together, despite some positive accomplishments, the major events of the past year have served to increase geopolitical tensions and conflict online to an unprecedented level. We look forward to working across diplomatic forums as a coalition and in our respective capacities as technology companies over the next year, to promote a rights-respecting and rules-based order for the online world to better protect our users and customers everywhere. We are hopeful that when we revisit this evaluation in 2024, the temperature of cyber conflict will have cooled significantly around the world.

ABOUT THE CYBERSECURITY TECH ACCORD

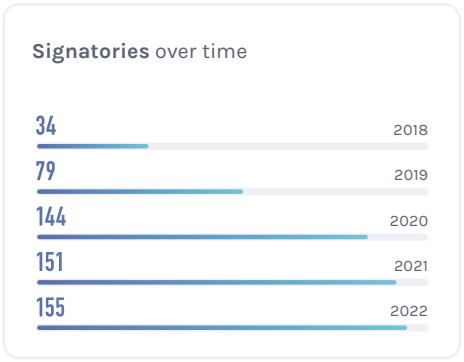
Founded in 2018, the Cybersecurity Tech Accord is a coalition of over 150 global technology firms committed to four basic cybersecurity principles – better defense, no offense, capacity building and collective action.

We believe that protecting the online environment is in everyone's interest and that all stakeholders have a role to play – especially the tech sector. To this end, we strive to be the industry's voice on peace and security in cyberspace. We are committed to responsible behavior that helps protect and empower our users and customers, thereby improving the security, stability and resilience of our online world.

36
Numbers of **Signatory Blogs** published

15
Numbers of **Signatory Case Studies**

155
Numbers of **Signatories**



19
Numbers of **Industry Events**

19
Numbers of **Training Webinars**

11
Numbers of **Reports** published

43
Numbers of **consultation responses** provided and statements delivered published

NEW SIGNATORIES ANNOUNCEMENT

adb

AEGIS INNOVATORS

Lenovo

Infosys

SUMMIT

ZENDATA

TIMELINE OF FIVE YEARS OF COOPERATION

2018

17 APRIL

Global technology companies sign the Cybersecurity Tech Accord, to defend customers everywhere from attacks by cybercriminals and state actors.

AUGUST

Campaign on Restoring WHOIS Access

Calls on ICANN to expedite solutions for legitimate third-party access to WHOIS data.

Routing security Norms

Endorses Mutually Agreed Norms for Routing Security to increase resilience and security.

JULY

Civil Society Collaboration

Announces consultative workshops with civil society to identify and collaborate on peace and security online.

APRIL

Recommendations on Confidence Building

Publishes recommendations supporting the Organization of American States (OAS) on adopting confidence-building measures for cyberspace.

MARCH

Annual Report 2018

Publishes 2018 Year In Review highlighting impactful initiatives and partnership from first year in existence.

OCTOBER

Commitments in Action

Begins publishing case study examples of signatory Commitments in Action, showcasing cybersecurity best practices by leading companies.

DECEMBER

Participation in UN OEWG

Joins the UN Open-Ended Working Group's dialogue on responsible state behavior and delivers statements of multistakeholder collaboration.

JANUARY

2020

Apps 4 Digital Peace Contest

Launches Apps 4 Digital Peace contest with the UN Office of Disarmament Affairs.

MARCH

Co-Chairs Paris Call Working Group

Joins French Ministry of Foreign Affairs' initiative to chair the Paris Call working group on multistakeholder inclusion in UN cyber dialogues.

FEBRUARY

Report on State-Sponsored Attacks

Releases survey report, with the Economist Intelligence Unit, on state-sponsored cyber-attacks on business.

2021

NOVEMBER

Cyber Hygiene Compendium

Releases a compendium of cyber hygiene practices in support of Paris Call principle #7.

APRIL

CVD policy milestone

100 Tech Accord signatories adopt CVD policies.

151 Signatories

Surpasses the 150 signatories milestone.

Updated ETSI statement

Releases statement welcoming increased activity and alignment on a common approach to improve IoT security.

SEPTEMBER

Coordinated Vulnerability Disclosures Call

Supports GFCE call for industry adoption of coordinated vulnerability disclosure (CVD) policies.

Capacity Building Webinars

Launches series with GFCE on cybersecurity best practices.

OCTOBER

Support for DMARC

Endorses Domain-based Message Authentication, Reporting & Conformance (DMARC), with the Global Cyber Alliance (GCA).

FEBRUARY

GSCS Singapore Norm Package

Welcomes new norms from the Global Commission on the Stability of Cyberspace. Calls on EU Commission to address cyber hygiene.

2019

UN High Level Panel on Digital Cooperation

Calls for UN's Panel on Digital Cooperation to sign Paris Call, oppose cyberattacks anywhere and empower users to defend themselves.

NOVEMBER

Paris Call Signatory

Endorses the Paris Call for Trust and Security in Cyberspace, a landmark multistakeholder agreement.

FEBRUARY

Annual Report 2019

Publishes 2019 Year in Review highlighting impactful initiatives and partnership from second year in existence.

MARCH

MANRS Adoption by Cloud Providers

Partners with Internet Society to develop actions allowing cloud providers and Content Delivery Networks (CDN) to help secure large hubs of the Internet from routing problems.

APRIL

CISO Blog Series

Launches blog series asking signatories: "What keeps your CISO up at night?"

JULY

Hack Back Whitepaper

Publishes "No Hacking Back: Vigilante Justice vs. Good Security Online" whitepaper, supporting Paris Call principle #8.

Contribution to Geneva Dialogue

Provides feedback to the Geneva Dialogue's background document to support stability of the digital environment.

MAY

Consumer IoT Security Initiative

Launches *"Stay Smart. Stay Safely Connected"* campaign with Consumers International on risks and best practices for consumer IoT products.

MAY

Annual Report 2020

Publishes 2020 Year In Review highlighting impactful initiatives and partnership from third year in existence.

Third Anniversary

Celebrates three years of the Cybersecurity Tech Accord.

Paris Call WG3

Announces that the Tech Accord will lead working group 3, focused on supporting *the continuation of UN negotiations with a strong multi-stakeholder approach.*

JULY

RightsCon 2021

Discusses threat posed by state-sponsored cyberattacks and the importance of cooperation during RightsCon 2021.

AUGUST

Paris Call WG3 Statement

Issues statement on behalf of WG3 claiming discussions on cyberspace security need to be more inclusive.

SEPTEMBER

Multistakeholder Manifesto

Launches a *Multistakeholder Manifesto on Cybercrime* in collaboration with the CyberPeace Institute and more than 60 other private sector and civil society organizations.

DECEMBER

Multistakeholder Manifesto on Cybercrime

Widens reach of manifesto by publishing it in all six UN languages.

2022

FEBRUARY

UN OEWG on cybersecurity

Releases statement affirming position that the UN OEWG needs multistakeholder inclusion following December session.

IoT device security statement

Collaborates with Consumers International and I am the Cavalry to release a statement supporting consumer IoT device security.

MARCH

International Women's Day

Celebrates women in cybersecurity with #MyCybHerStory campaign.

Podcast series

Launches "Patching the System," a limited podcast series into pressing international cybersecurity challenges.

MAY

Milestones in IoT security

Celebrates first anniversary of the "Executive Order on Improving the Nation's Cybersecurity."

DECEMBER

Support EU plan to reinforce cyber defense capabilities

Announces support the EU's plans to Strengthen ICT Supply-chain Security and plans for EU-wide Cyber Defense

OCTOBER

IoT security resources

Re-launches updated resource to support manufacturers in developing more secure IoT devices for consumers.

UN Cybercrime Treaty Negotiations

Provides input into the Third Session of the Ad Hoc Committee on Cybercrime.

JANUARY

Intersessional OEWG on ICT

Delivers statement during UN OEWG discussing confidence building measures to increase trust between governments online.

2023

World Economic Forum Event

Hosts an event in Davos focused on Industry leadership for IoT Security in partnership with WiseKey.

MARCH

UN Cybercrime Treaty Negotiations

Signatories deliver remarks during the Second Intersessional meeting of the Ad Hoc Committee on Cybercrime.

OCTOBER

UN General Assembly

Announces support of joint civil society statement on cyber peace and security along with 13 signatories.

UN Programme of Action

Releases statement expressing excitement regarding the UN "Programme of Action" on cybersecurity.

Effective Cyber Diplomacy White Paper

Debuts "Towards effective diplomacy: A guide to best practices and capacity building" white paper.

NOVEMBER

Budapest Convention on Cybercrime

Expresses support and appreciation for the convention during its 20th anniversary.

Third Anniversary of Paris Call WG3

Presents results of the Working Group 3 of the Paris Call.

Bureau of Cyberspace and Digital Policy

Announces support of new bureau at the U.S. Department of State focused on advancing international cybersecurity, internet freedoms and broader digital policy issues.

JULY

Hybrid Warfare

Releases statement discussing the technology industry and the age of hybrid warfare following Russia's invasion of Ukraine.

Annual Report 2021-2022

Launches 2021-22 Annual Report highlighting impactful initiatives and partnership from fourth year in existence.

UN Cybercrime Treaty Negotiations

Signatories deliver remarks during the Second Intersessional meeting of the Ad Hoc Committee on Cybercrime.

AUGUST

UN Conference on Disarmament

Delivers remarks on the role of stakeholders in supporting state capacity-building in ICT security.

EU Digital Diplomacy Office

Welcomes announcement that the EU plans to launch a new digital diplomacy office in Silicon Valley.

Multistakeholder Statement on OEWG Veto

Issues statement regarding member state veto of accreditation request to take part in OEWG on security of and in the use of information and communications technologies.

APRIL

#MyCybHerStory Webinar

Celebrates women in cybersecurity with #MyCybHerStory campaign.

Cyber Mercenaries

Releases set of principles to guide the technology industry to help curb the dangerous and rapidly growing market of cyber mercenaries.

FIVE YEARS OF THE TECH ACCORD

OUR COMMITMENT IN ACTION

In 2018, the Cybersecurity Tech Accord was founded around four basic cybersecurity principles to guide the technology industry to act responsibly, to protect and empower their users and customer, and thereby improve the security, stability, and resilience of cyberspace.

Five years on, our principles continue to drive our work, and this anniversary provides us an opportunity to reflect on how our four foundational principles have guided our shared commitment and efforts. The section below attempts to take a comprehensive stock of the numerous initiatives and partnerships that the Cybersecurity Tech Accord and its signatories have undertaken over the past five years in support of these principles.

1. Strong Defense

We will protect all of our users and customers everywhere.

We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.

We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

2. No Offense

We Will Oppose Cyberattacks On Innocent Citizens And Enterprises From Anywhere.

We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.

We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

3. Capacity Building

We Will Help Empower Users, Customers And Developers To Strengthen Cybersecurity Protection

We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.

We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

4. Collective Response

We Will Partner With Each Other And With Likeminded Groups To Enhance Cybersecurity.

We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.

We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

Strong defense

Cyber Hygiene

As part of our commitment to the Paris Call on Trust and Security in Cyberspace which we first endorsed in November 2018, Cybersecurity Tech Accord signatories committed themselves to taking forward one of the agreement's nine principles: *Principle #7 – Support efforts to strengthen an advanced cyber hygiene for all actors.* The Cybersecurity Tech Accord worked to advance the importance of cyber hygiene by promoting good practices critical to responding to a changing threat environment through individual and collaborative efforts with like-minded organizations, including the CyberGreen Institute, the Global Cyber Alliance, and the Internet Society. In 2020 we launched **a three-part video series** – part one on introducing cyber hygiene, part two on the email security protocol DMARC, and part three on the ways to protect from DNS threats – that introduces the basics of cyber hygiene, highlighting some of the most critical steps organizations can take to keep themselves safe.

Cyber Defence vs "Hacking Back".

To support Paris Call Principle #8: No private hack back, the Tech Accord produced in 2020 **a whitepaper titled "No Hacking Back: Vigilante Justice vs. Good Security Online"**, in order to highlight how this principle should be upheld without jeopardizing essential security practices. The whitepaper provides a deep dive into what is considered inadvisable and illegal "hack back" activities versus valuable forward-leaning "active defense" security practices employed widely by the technology industry today. It serves as an essential guide for policymakers seeking to better understand the boundaries of industry action in cyberspace to prevent and deter cyberattacks by criminals, and why "hack backs" are not a suitable way to address the increasing number of threats.

Case Studies on Strong Defense

As part of our commitment to "strong defense," in 2019 we began an initiative to showcase **Case Studies** of how our signatories were implementing the first principle of the Cybersecurity Tech Accord, to protect all users and customers everywhere. Our signatories provided a wide range of responses about how their organizations deliver on the commitment. Activities included building human firewalls, protecting small and midsize businesses, securing software developments, providing businesses with strategic domain name management, ensuring data integrity, building multi-layered security and so much more. These not only demonstrate responsible behavior by respective company signatories, but also serves as an example for companies from across the industry looking for innovative security practices.

IoT Security

Everyone needs to play their part to make our online environment more secure – that includes governments, private organizations, and individual users. But anyone's ability to act begins with an awareness of the security risks that technology can pose. That is why in 2020, the Cybersecurity Tech Accord launched the initiative **"Stay Smart. Stay Safely Connected"** with Consumers International to raise awareness around the importance of consumer IoT device security for average users as well as manufacturers. The campaign aimed to bring consumers and manufacturers closer together by recognizing that both have critical and distinct roles to play in protecting IoT products from cyber-threats. While manufacturers have a primary responsibility to design these products to be secure, it is important for consumers to be aware of cyber risks and to know the steps they can take to use these products safely.

In addition, in 2022, through the World Economic Forum's Council of the Connected World, leaders from the Cybersecurity Tech Accord, Consumers International and I Am the Cavalry, representing more than 400 organizations globally, collaborated to recognize an emerging consensus on baseline cyber security provisions for consumer IoT devices. **Our joint statement** highlighted five consensus capabilities on what baseline expectations should be reflected across all consumer devices to improve security: i) no universal default passwords, ii) adopting a vulnerability disclosure policy, iii) keeping software updated, iv) securing data, and v) securing communications. These five capabilities are each reflected in over 100 different standards around the world and should be the highest priorities for device manufacturers and vendors to adopt to keep consumers safe. The statement itself was endorsed by over 100 multistakeholder organizations around the world – including prominent government cybersecurity agencies.

In October 2022, the Cybersecurity Tech Accord re-launched a section of our website to support consumers and manufacturers in developing more secure internet of things (IoT) devices for consumers. The section, focused on consumer IoT device security, is built around the five security capabilities highlighted in our joint statement. **The updated IoT resource hub** is intended for device manufacturers, providing resources, good guidance and examples from Cybersecurity Tech Accord signatories to support the adoption of these five security capabilities. The IoT subsection of our website also serves as a repository for broader government guidance and standards for consumer IoT device security, and resources provided by Cybersecurity Tech Accord signatories. It also features expert guidance for consumers themselves seeking to optimize the security of the most common IoT products.

Zero Trust

A "Zero Trust" cybersecurity model has been one of the most important innovations in organizational risk management in recent years, but although it constitutes a fundamental shift in mitigating risk, it is still not widely adopted or even understood. That is why, throughout Cybersecurity Awareness Month in October 2022, the Cybersecurity Tech Accord aimed to break down the core elements of "Zero Trust" architecture by launching a blog series titled **"Never Trust, Always Verify".** The series featured expert voices from across Cybersecurity Tech Accord signatories breaking down what Zero Trust is, what it isn't, and how to have an informed conversation to ensure organizations are employing best practices for security. The series included entries on: Zero Trust in IT and OT systems by Schneider Electric; *Strong authentication for Zero Trust by Balasys; Zero Trust access policies by Safe PC Solutions; and Threats that necessitate Zero Trust by Contrast Security.*

No Offense

Hybrid Warfare

After Russia's invasion of Ukraine in February 2022, and as the cyber dimension of the conflict intensified, the Cybersecurity Tech Accord and its signatories published a statement **the role of the technology industry in the age of hybrid warfare.** Our signatories reaffirmed their commitment to protect their respective customers who may be impacted by cyberattacks employed in the war. Our signatories called on the international community to respect international humanitarian law and provide more clarity on international law obligations in cyberspace, enforce broader transparency, consider new norms and expectations for states, and build more space for multistakeholder inclusion. In May 2023, our organization hosted an in-person **event at the World Economic Forum**, sponsored by one of our signatories, Wisekey. The event featured leaders from the Tech Accord's signatory companies who discussed the unique role that the technology industry has played recently and historically in addressing the cyber elements of the war in Ukraine, and the multistakeholder cooperation necessary to establish a rules-based order in cyberspace.

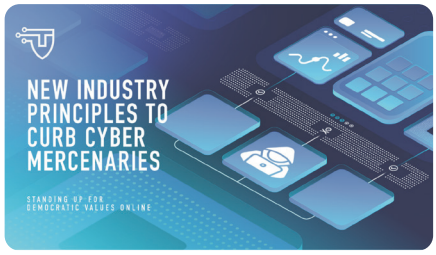
New Technologies for Digital Peace

Amidst escalating numbers of sophisticated cyberattacks, it is clear that bringing greater security and stability to cyberspace requires new ideas compared to what has worked in other domains of conflict, as well as collaboration across stakeholder groups. That is why in 2020 the Cybersecurity Tech Accord partnered with the United Nations Office of Disarmament Affairs (UNODA) to launch **Apps 4 Digital Peace**, a first-of-its-kind competition, to stimulate new thinking from innovating young minds across the world. The goal of the competition was to develop original technology-based solutions, such as mobile applications, to both help limit the use of the internet as a domain of conflict, and to increase the stability of our online environment. This exciting cybersecurity competition for young innovators concluded with the announcement of the Cybersecurity Tech Accord's top three contest winners. Each winner, Fsociety, Maktab, and Cyber Teens, was selected for their new and innovative ideas that help limit the use of the internet as a domain of conflict or harm and increase the stability of our online environment.

Responses to Nation State Cyberattacks

In an effort to understand businesses' perceptions of, and responses to, state-led and -sponsored cyberattacks and to identify effective policy solutions to mitigate the threat, in 2021 the Cybersecurity Tech Accord partnered with The Economist Intelligence Unit (EIU) to launch a study titled **"Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats."** 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 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.

Cyber Mercenaries



In 2023 the Cybersecurity Tech Accord, with support from other industry players, was proud to release a new set of principles to guide the technology industry to help curb the dangerous and rapidly growing market of **cyber mercenaries**. This term refers to a wide range of companies which now develop and sell offensive cyber capabilities and services, generally to government customers. Their operations involve the cultivation and proliferation of "zero-day" exploits and malicious software that undermines the security of peaceful technology, and which have been widely used to violate human rights and democratic principles online. At a high level, the five principles charge companies to:

1. *Take steps to counter cyber mercenaries' use of products and services to harm people;*
2. *Identify ways to actively counter the cyber mercenary market;*
3. *Invest in cybersecurity awareness of customers, users and the general public;*
4. *Protect customers and users by maintaining the integrity and security of products and services;*
5. *Develop processes for handling valid legal requests for information.*

Technical Capacity Building

In 2018, to enhance efforts to secure the online environment, the Cybersecurity Tech Accord partnered with the Global Forum on Cyber Expertise (GFCE), a global multistakeholder platform aiming to strengthen cyber capacity building and expertise through the exchange of best practices. As part of our partnership, the Cybersecurity Tech Accord launched **a series of webinars on cybersecurity technical best practices** with the aim of increasing the understanding of key cybersecurity topics for emerging markets, and of addressing the growing need to respond to the cybersecurity skills gap across different sectors. The topics of the webinars ranged from cloud computing to various cybersecurity basics, including encryption, browser protection, ransomware, and phishing. Also in 2018, our initiative started sharing thought-leadership pieces from our signatories in a blog series that focused on **"What keeps CISOs up at night?"**. Over the years, we featured more than 36 blog posts providing a further look into what is on top of mind for industry leaders.

Cyber Diplomacy

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. That's why to celebrate Cybersecurity Awareness Month in 2021, the Cybersecurity Tech Accord published a study titled: **"Towards effective cyber diplomacy: A guide to best practices and capacity building."** The report provided tools for cybersecurity diplomats and a roadmap to help countries build up their cyber diplomacy capabilities. In particular, the report aims to 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.

Addressing the Gender Gap

To honor International Women's Day, in 2022 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 were shared to send 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. 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.

The #MyCybHerStory campaign became an annual program, and for International Women's Day 2023, we hosted an interactive career webinar titled **"#MyCybHERStory – exploring cybersecurity careers for women and girls with industry leaders"**, where women leaders from our community of

signatories shared their experiences in the industry with women and girls interested in pursuing a career in cybersecurity. Participants heard from our industry leaders about their respective career paths and learned how they chose the right path and concentration according to their skillset and interests.

Cybersecurity Awareness

Every year in October, the Cybersecurity Tech Accord participates in **Cybersecurity Awareness Month**, an annual awareness campaign intended to encourage greater safety and protection among all computer users. In October 2018, the Cybersecurity Tech Accord signatories drafted **ten concrete and simple steps** that individuals can take to better protect themselves online. These are based on the tips the signatories have shared over the years encouraging users to stay safe online and can be found on our website.

In October 2019, the Cybersecurity Tech Accord compiled a **list of resources and initiatives** developed by its signatories to improve cybersecurity awareness but also went beyond our own resources, listing some of the many readily available materials intended to improve the cybersecurity awareness and capabilities of governments, organizations and individuals. By promoting and sharing these materials, we aimed to contribute to building a more safe and secure online world for everyone.

Additionally, the Cybersecurity Tech Accord, in collaboration with the United Kingdom's Foreign & Commonwealth Office (FCO), produced and released a **comprehensive whitepaper on the state of cybersecurity awareness and associated campaigns across the Commonwealth of Nations**. The whitepaper provides industry guidance to support cybersecurity awareness programs and catalogues awareness raising activities throughout the Commonwealth. The report captures a wide array of different approaches, including initiatives from across five continents including some of the world's largest and smallest countries, detailing different approaches to promoting cybersecurity awareness based on respective capacities, needs and cultures.

Addressing the Cyber Skills Gap

The cybersecurity skills shortage we are experiencing today is leaving many organizations struggling to keep up with the ever-changing threat landscape. To demonstrate its commitment to improve the security, stability and resilience of cyberspace, as well as its principle to provide capacity building, in 2018 the Cybersecurity Tech Accord published a whitepaper titled ***"Addressing the cybersecurity skills gap through cooperation, education and emerging technologies".*** The whitepaper underscored the critical need for industries to adopt and implement emerging technologies such as Artificial Intelligence (AI) and machine learning, among others, to increase cybersecurity and scale responses in an environment in which cybersecurity positions remain unfilled by qualified professionals, and current cybersecurity teams are being stretched thin.

Confidence Building Measure in Cyberspace

Trust and cooperation are key to cybersecurity, for both companies and governments. Acknowledging that **confidence building measures** are a pivotal tool that helps governments promote security and stability online, in 2019 the Cybersecurity Tech Accord recommended ways on making these more effective.

Multistakeholderism at the United Nations

Ever since our launch in 2018, the Cybersecurity Tech Accord has aimed to serve as the industry's voice on peace and security online. Our signatories strongly believe that establishing safeguards to protect the online environment is in everyone's interest, and that industry, governments and civil society all have a role to play in achieving this goal. For this reason, throughout the work of the Cybersecurity Tech Accord, we have aimed to enable greater participation of the private sector in the global discussions on cybersecurity and have extensive experience in engaging with several international and multilateral fora, including the **Open-ended Working Group** on security of and in the use of information and communications technologies and the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Our initiative also provided input into the work of the **UN High Level Panel** on Digital Cooperation in 2018, and in the work of the **UN Conference on Disarmament** in 2022.

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). The past couple of years were 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 behaviour in this new domain. As the OEWG started its latest mandate (2021-2025), we have been continuing to seek 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 behaviour 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 digital diplomacy capabilities.

Additionally, in the context of the negotiations over a proposed **new cybercrime convention 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 the **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 throughout the 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.

In 2021, 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 made a case for enhanced collaboration across stakeholder groups around these issues and provides recommendations on ensuring greater inclusivity in the UN dialogues on cybersecurity.

Coordinated Vulnerability Disclosure Policies

In 2018, we called for governments to follow the United Kingdom and United States' examples in adopting vulnerability equities processes and put forward a set of principles to guide those efforts. We also endorsed the GFCE's set of good practices for organizations on the adoption of vulnerability disclosure policies. Most significantly, Cybersecurity Tech Accord signatories agreed to put **vulnerability disclosure policies in place** across our signatory base.

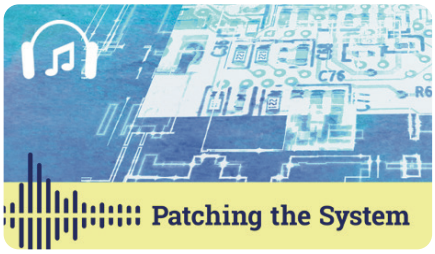
Joint Call by Internet Society to G7 and Commonwealth of Nations Report

In 2019 the Cybersecurity Tech Accord joined nearly 50 other organizations in c**alling on the G7 governments to prioritize cybersecurity** and not to require technology companies to "modify their products or services or delay patching a bug or security vulnerability to provide exceptional access to encrypted content; turn off 'encryption-on-by-default'; cease offering end-to-end encrypted services; or otherwise undermine the security of encrypted services."

CyberPeace Foundation

In 2020, the Cybersecurity Tech Accord partnered with the CyberPeace Foundation in the **Global CyberPeace Challenge**, a competition that encourages youth innovators from around the world to promote peace in cyberspace by solving crucial techno-social issues. The global competition was divided into three parts: CyberPeace Policy & Strategy Challenge, Peace-a-thon, and Capture the Flag (CTF), each designed to inspire solutions to critical real-world problems. We supported the competition focused on CyberPeace Policy & Strategy, a competitive crisis simulation where participants respond to a realistic international cybersecurity incident. The exercise aims to understand the policy and strategic challenges associated with managing a crisis on an international level, underpinned by the technical, operational, geopolitical, and legal questions that surface.

Patching the System Podcast



In 2022, 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 series**, which engaged signatories from the Cybersecurity Tech Accord and 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 cybercrime treaty negotiations, ICT supply chain security, the dangers posed by cyber mercenaries, and protecting the ever-growing world of "smart" devices.

OUR PARTNERS

The Cybersecurity Tech Accord strongly believes that a collaborative, multistakeholder approach is vital to addressing the growing and transnational challenges pertaining to peace and security online, and to crack down on the malicious use of information and communication technologies (ICTs).

That is why, in the last year, as an engaged member of the multistakeholder cybersecurity community, Cybersecurity Tech Accord continued to partner with governments, civil society groups, and like-minded industry players on a range of initiatives.

Thanks to our partnerships, we were able to reach new audiences, create more awareness of the most pressing issues of the online world, and advocate together for shared goals. Here is how some of the partners we have worked with highlighted the importance of our collaboration:

Paris Peace Forum

"The Cybersecurity Tech Accord has been a major step in affirming the responsibility of the industry to secure a free, open and stable cyberspace. As an active supporter of the Paris Call for Trust and Security in Cyberspace, the Cybersecurity Tech Accord community has been instrumental in the development of several action-oriented frameworks or operation recommendations such as the 2021 report on "Advancing the UN negotiations with a strong multistakeholder approach". Five years after its launch and at a time when meaningful stakeholder inclusion in multilateral cyber discussions is key, the Cybersecurity Tech Accord is more relevant than ever as rising tensions across the Globe call for meaningful cooperation of all actors, whether public or private, to defend global cyber stability and everyone from cyber harms".

PARIS PEACE FORUM

Jérôme Barbier
Head of Outer Space, Digital and Economic Issues,
Paris Peace Forum

United Nations Office for Disarmament Affairs (UNODA)

"Multistakeholder, private-sector-led initiatives like the Cybersecurity Tech Accord have played an important role in supporting the promotion and operationalization of international norms for responsible State behavior. Broad stakeholder engagement has been and will continue to be critical to ensuring the peace and security of cyberspace."

United Nations | Office for Disarmament Affairs

Katherine Prizeman
Political Affairs Officer, Science, Technology and International Security Unit,
United Nations Office for Disarmament Affairs (UNODA)

I Am The Cavalry

"It's great to see agreement from so many organizations around the urgent need to raise the defensive posture in IoT, and give buyers and operators the capabilities they need to safeguard themselves and their families against harm."

I AM THE Cavalry

Beau Woods
Cyber Safety Ambassador,
I Am The Cavalry

ICT4Peace Foundation

"Effective governance for a secure and peaceful cyberspace requires translating human rights standards to a format that works for ICT companies. Recognizing this need, the Cybersecurity Tech Accord recently launched its Cybersecurity Tech Accord Principles limiting offensive operations in cyberspace, which is aimed squarely at the burgeoning cyber mercenary industry, and which very much align with ICT4Peace's From Boots on the Ground to Bytes in Cyberspace: A Mapping Stud on the use of ICTs in Security Services by Commercial Actors published in September 2022. The Tech Accord's principles are an essential step towards ensuring a safe and accessible online environment that also protects our human security. ICT4Peace Foundation welcomes the Accord's commitment to inclusive governance and its efforts to raise awareness about the use of ICTs in security services provided by private commercial actors. ICT4Peace is pleased to work together with the Tech Accord's in order to make a safe and peaceful cyberspace a reality".

Anne-Marie Buzatu
Executive Director,
ICT4Peace Foundation

World Economic Forum

"Cybersecurity continues to be a major risk for people and businesses worldwide. Through the World Economic Forum's Council on the Connected World, the Cybersecurity Tech Accord, Consumers International and I am the Cavalry collaborated to recognize an emerging consensus on five baseline security provisions for consumer IoT devices. For the first time, over 100+ technology providers, security researchers, hacker and consumer groups, and government agencies voiced the need for manufacturers to adopt minimum security provisions as a starting point. This call to action sets the stage further for understanding how to take a security-by-design approach and reducing fragmentation of cybersecurity best practices internationally not only to protect people's safety and privacy, but also enabling manufacturers to adopt agreed upon best practices."

Dr. Anu Devi
Lead, Centre for Urban Transformation,
World Economic Forum

CyberPeace Institute

"Fight against cybercrime should not come at the expense of fundamental human rights. It is of utmost importance to repeat it today, while the United Nations (UN) is currently engaged in a multiannual process with the aim of establishing a global cybercrime treaty, via the open-ended Ad Hoc Committee (AHC). Considering this compelling moment in the history of international cyber policy, in a truly multistakeholder effort the CyberPeace Institute and the Cybersecurity Tech Accord initiative published the Multistakeholder Manifesto. The overarching message of the Manifesto, supported by over 60 civil society and industry representatives, is that human-centric principles are central to any cybercrime legislation. Cybercrime poses new risks and threats to people's rights and livelihoods, but countering cybercrime, its impact and the harm it might cause, should not come at the expense of a free and open Internet. The Manifesto calls to ensure that any convention countering the criminal use of ICTs protects victims, preserves an open Internet and upholds basic human rights and freedoms guaranteed under existing international UN and other treaties."

Francesca Bosco
Senior Advisor Strategy and Partnerships,
CyberPeace Institute

SIGNATORY SPOTLIGHT

What motivated your company to join the Tech Accord?

In a world of constant transformation, and after almost 100 years of history, Telefónica's commitment to progress based on innovation, sustainability and inclusiveness only makes sense if we put technology at the service of people, everywhere, in any country. Technology is the tool that allows us to connect better in our daily lives, with our families, customers, businesses.

And to reach the full potential of digital technologies, trust is an essential lever, powered by the fair utilization of digital capabilities for the good of society and the prevention and avoidance of cyberthreats. Cybersecurity Tech Accord foundational principles were fully aligned with our own. The Tech Accord is unique in its aim to accelerate the implementation and improvement of cybersecurity globally, through the participation of businesses, governments, and individuals.

Alejandro Becerra
Group Information Security Director,
Telefonica

Which of the Tech Accord's principles resonates most with your company's mission and why?

The second principle, "We will oppose cyberattacks on innocent citizens and enterprises from anywhere", as it follows our mission to make the world safe. We also will continue to support our customers against any and all attacks against them, whether they are commercial customers or individual consumers around the world. This principle is critical for governments to support as well as attacks against a nations' critical infrastructure could cause severe harm against innocent people there. This is one reason why our Zero Day Initiative's bug bounty event, Pwn2Own, has a specific event focused on SCADA and critical infrastructure products to identify new zero-day bugs that can be patched by the vendors.

Ed Cabrera
Chief Cybersecurity Officer,
TrendMicro

What would you like to see the Tech Accord lean into in the next five years?

"Collaboration across the supply chain. Undoubtedly, we're seeing the emergence of threat actor activity inside the supply chain, which then has the potential to harm many others. The Tech Accord has already done a lot of work around that in terms of raising awareness and having actual tangible outcomes around hardening and better defense. But the reality is that threat actors are pivoting, and so the Tech Accord should pivot. We need to look more at how we can crack that whole ecosystem approach – who is responsible for what, how that knits together. We also need to think through protocols so we can better collaborate in these situations."

Mark Hughes
President Security,
DXC Technologies

What Tech Accord accomplishment from the past five years are you most proud of and why?

The consistent engagement of the Cybersecurity Tech Accord across diplomatic forums has given the industry unified a voice, at the UN and beyond, in discussions of peace and security online for the first time. And this is essential as the technology industry develops, owns and operates most of what we consider "cyberspace," so we need to be included to inform discussions around setting expectations for responsible behavior.

Tom Burt
Corporate Vice President, Customer Security and Trust,
Microsoft

CYBERSECURITY TECH ACCORDS SIGNATORIES

As we begin our new journey into the next five years of our organization, we continue to 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 or contact our secretariat at info@cybertechaccord.org

Flowmon
Driving Network Visibility
FRAMEWORK
SECURITY
GDATA
Gigamon
GitHub
GitLab
Globant
Greenlight
INFORMATION SERVICES
GREYCORTEX
gtd
guardtime
HCS
Business Solutions
working smarter with IT
HITACHI
Inspire the Next
[H]matix
hp
Hewlett Packard
Enterprise
IMPERVA
ImmuniWeb®
AI for Application Security
indra
minsait
INFINIT
CONSULTING
Infosys
integrity
partners
International
SOFTWARE SYSTEMS
intuit
JUNIPER
NETWORKS
KOOLSPAN
LaSalle Consulting Partners
LawToolBox.com
Lenovo
LinkedIn
LIREX.COM
IT INNOVATIONS
LogRhythm
Madison Computer Works
MANDIANT
MarkMonitor
Protecting brands in the digital world
MediaPRO
Cybersecurity & Privacy Education
mercado libre
Meta
Microsoft
Moback
NEC
NetApp
nielsen
NOKIA
NORTHWAVE
Intelligent Security Operations
NTT
onShore
SECURITY
ORACLE
orange
Panasonic
panda
pango
pax8
percipient.ai
predica.
PROFESSIONAL
OPTIONS
QOMPLX:
QAssociates
REDSEAL
Resecurity
reveal
Rockwell
Automation
RSA
SAFE PC CLOUD
safetica
salesforce

SAP
Schneider Electric
Scitum
secucloud
Secure Soft
SecurityScorecard
SHARP
SILENT BREACH
SONDA
SSRD
STACKPATH
STRATA Information Technology
stripe
StrongConnexions
SUMMIT
SWITCHFAST
Synack
TADGROUP
TANIUM
TIM
Telefónica
telelink
tenable
ThreatModeler
TREND MICRO
UNISYS
USLicensing Group
US Medical IT
VALIDY
vmware
VU
WCA TECHNOLOGIES
WIPFLi
WISeKey
WITH secure
ZENDATA

FOR INFORMATION ON THE CYBERSECURITY TECH ACCORD,
PLEASE EMAIL INFO@CYBERTECHACCORD.ORG