CYBERSECURITY TECH ACCORD

YEAR 6 REPORT

Cybersecurity Tech Accord
The voice of technology industry on international cybersecurity

CONTENTS

LETTER BY THE SECRETARIAT 3

ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER 4

ABOUT THE CYBERSECURITY TECH ACCORD 8

OUR COMMITMENT IN ACTION 10

OUR PARTNERS 19

OUR PREVIOUS REPORTS 21

OUR SIGNATORIES 22

LETTER BY THE SECRETARIAT

Over the past six years, the Cybersecurity Tech Accord has grown into the world's largest coalition of technology companies focused on improving cybersecurity through multistakeholder cooperation. Today, it serves as the voice for our industry on matters of international peace and security online.

At this pivotal moment of global digital transformation, our mission is more critical than ever. New technologies continue to improve lives and connect people around the world, while at the same time, escalating conflict online threatens to undermine and destabilize the digital ecosystem. Artificial intelligence is transforming the capacity of organizations to counter cyber threats at unprecedented scale, while malicious actors are exploring how to use this technology to improve their attack methods. As geopolitical tensions and rivalries continue to drive state-sponsored cyberattacks of increasing severity – including in Russia's ongoing invasion of Ukraine – it is clear that we need more cooperative efforts to improve security and raise expectations for responsible behavior online.

These concerns have driven us to step-up our engagement in relevant dialogues at the United Nations (UN) over the past year, to drive greater recognition of international norms for states. Most notably, we called for UN member states to recognize a new norm to prohibit cyberattacks that could compromise the integrity of the ICT supply chain. We continue to push for more inclusive, multistakeholder processes at the UN, including in the working group responsible for improving the application of international law and norms online. The efforts of these working groups would greatly benefit from regular input from the industry responsible for developing and maintaining the majority of the digital ecosystem.

Another area of pressing concern this past year has been the ongoing proliferation of cyber mercenaries, firms that develop and sell malicious tools and services, largely to governments. The existence and growth of this market undermines security by incentivizing the retention and exploitation of vulnerabilities instead of responsible disclosure. This is why, our coalition has worked over the past year to support responsible industry practices to push back on cyber mercenary operations, and began tracking government-led efforts to start placing meaningful boundaries on the cyber mercenary market itself.

We also stepped up our advocacy in the negotiations of the first UN cybercrime convention. Throughout successive rounds of negotiations, we have urged member states to remove fundamentally harmful provisions and provide explicit protections for security researchers at risk of being inadvertently criminalized for their vital work discovering and responsibly disclosing vulnerabilities. This important work continues ahead of the expected conclusion of negotiations this summer.

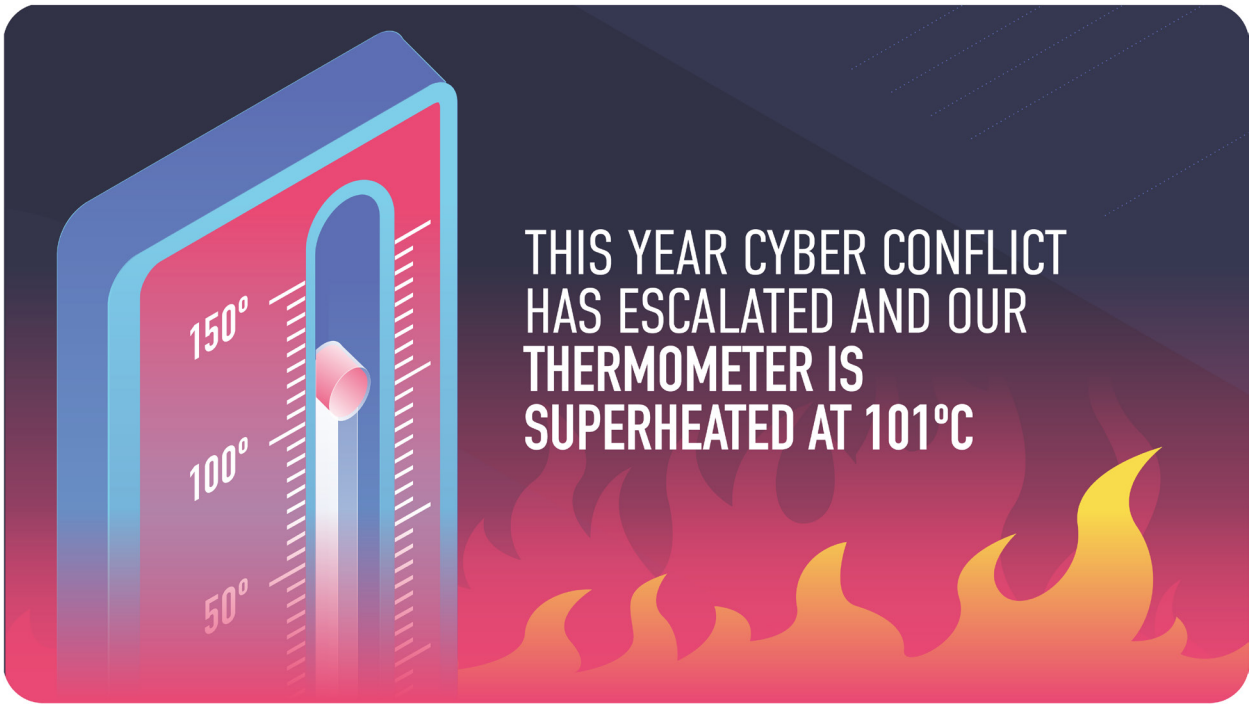
Last year we launched our annual State of International Cybersecurity Thermometer, an assessment made by our community taking stock of the current state of conflict and security online. This year, our assessment found that peace and security online has continued to deteriorate, despite some progress, inching the International Cybersecurity Thermometer one degree higher to 101 degrees.

Over the past year, our signatories have showcased their commitment to our coalition's mission – leveraging their knowledge and thought leadership through several initiatives. This report takes stock of a year of work advancing our shared principles for a more secure, safe, stable and trusted online world. We hope you enjoy it and welcome your comments at info@cybertechaccord.org.

The Cybersecurity Tech Accord Secretariat

ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER

INTERNATIONAL CYBERSECURITY THERMOMETER **TICKS ONE DEGREE HIGHER IN 2024.**



Last year, the Cybersecurity Tech Accord launched the "State of International Cybersecurity Thermometer," an annual measure of how conflict online has escalated or deescalated. Following Russia's widespread use of cyber operations in its invasion of Ukraine, we asserted in 2023 that the world had reached a metaphorical "boiling point" of cyber warfare and placed the first Thermometer reading at 100 degrees. In 2024, our coalition of cybersecurity professionals from across the tech industry assess that peace and security online has continued to deteriorate, despite some meaningful progress, on balance inching the International Cybersecurity Thermometer one degree higher, to 101 degrees.

This determination reflects an urgent situation and is due largely to the geopolitical tensions and conflict online that has continued to escalate in the past year. Overall, the sophistication and impact of nation state cyberattacks has increased without regard for international rules and norms. Nevertheless, there have been encouraging developments in the past year, including technological advancements and evolutions in the international system that have helped improve security and give cause for hope looking forward. Advances in AI are yielding some immediate security benefits for defenders. Meanwhile, governments and international institutions are increasingly working together to strengthen deterrence and promote responsible behavior online. We hope that these positive developments will continue and begin to have a meaningful impact on the state of conflict online in the next year.

The State of International Cybersecurity Thermometer aims to provide a clear and objective assessment of the current cyber landscape. It seeks to identify key trends and developments over the past year and outlines measures necessary to enhance stability and security in the digital realm moving forward. As with last year's evaluation, the major developments considered in making our determination are spread across three categories: i) diplomatic and institutional developments, ii) the scale and nature of conflict online, and iii) technological developments. Each of the major developments included in this year's evaluation are detailed below, with an indication as to whether they have had a positive, negative, or neutral overall impact on the security landscape.

WHAT THE READING REFLECTS

100° AND ABOVE CYBER WARFARE

This "gaseous" state reflects chaotic and dangerous conditions past a boiling point. This suggests the use of cyber operations in the context of an armed conflict that has harmed and/or targeted civilians.

Evidenced by:

- Use of cyber operations in war in violation of international norms and/or law
- Ineffective deterrence

0° - 99° CYBER CONFLICT

This "liquid" state reflects a degree of cyber conflict short of warfare. It is characterized by a lack of clarity around international expectations online and/or an inability to uphold such expectations.

Evidenced by:

- Reckless cyber activity by nation states
- Regularized abuses by nonstate actors
- limited progress in diplomatic forums

LESS THAN 0° CYBER STABILITY

This"solid"state reflects stability in international cybersecurity. It requires the existence of a clear rules-based order online with a robust international system to uphold such expectations.

Evidenced by:

- Scarcity of state sponsored cyber operations that violate international norms
- limited threats posed by other actors

DIPLOMATIC AND INSTITUTIONAL DEVELOPMENTS:

Limited progress and counterproductive developments at the United Nations (UN)

As the international organization responsible for maintaining global peace and security, member states of the UN in the past year have once again made limited progress towards a more secure online world as cyber conflict has continued to escalate. The UN working group tasked with setting and upholding expectations for responsible state behavior online failed to recognize any new norms or to support implementation of existing ones, and has been unable to facilitate regular, meaningful multistakeholder inclusion. Meanwhile, separate negotiations of a UN cybercrime convention have raised significant concerns around protections for human rights and the important work of security researchers from industry and civil society.

Multistakeholder commitments on cyber mercenaries

After years of rapid growth in an uncontrolled market, governments – led by France, the UK, and the US – are finally taking further steps to curb the market for cyber mercenaries. These groups make and sell offensive cyber tools, largely to government customers, using a business model that undermines the security of peaceful technology and discourages the responsible disclosure of vulnerabilities. New commitments by governments, and the launch of the multistakeholder Pall Mall Process, highlight important first steps on a promising path forward.

International Criminal Court to address cyber-enabled war crimes

Last fall, the Prosecutor of the International Criminal Court (ICC) announced that his office would expand its jurisdiction to include investigations of cyber-enabled war crimes. This initiative aligns with the evolving nature of modern warfare, where cyber operations increasingly play a pivotal role and can put civilians at serious risk. the Prosecutor's office has subsequently hosted gatherings to develop this policy further. Such proactive measures by international justice bodies are needed to ensure they are able to meet their mandate and enforce international obligations online.

Targeted and collective cyber sanctions

This year marked a significant advancement with the initiation of the first trilateral cyber sanctions. In a coordinated effort, Australia, the UK, and the US imposed sanctions on a Russian threat actor responsible for a 2022 ransomware attack against an Australian healthcare insurer. This joint action underscores the importance of international collaboration in combating cyber threats and sets a precedent for future cooperative sanctions. The commitment of countries to stand together with their partners underscores the importance of collective responses in maintaining cybersecurity and deterrence.

NATO Cyber Defense Pledge

Amid the widespread use of cyber operations in Russia's invasion of Ukraine, it is encouraging to see the NATO alliance enhance its cooperation on cyber defense. At the NATO Summit last summer, allied nations announced a new vision for how cyber defense will contribute to NATO's overall deterrence and defense posture, in the face of rising threats. This includes commitments to strengthen national cyber defenses as a priority.

The EU Cyber Resilience Act (CRA)

The CRA is a landmark piece of European Union (EU) legislation expected to be finalized during the second half of 2024, establishing significant cybersecurity requirements for manufacturers of products with digital elements throughout their product lifecycle. Like the General Data Protection Regulation (GDPR) in 2018, compliance with the CRA will set a de facto minimum standard for companies operating across regions. While much of the CRA's contents will certainly improve cybersecurity, there remain concerns that the required reporting of unpatched vulnerabilities could increase cyber risk. Ultimately the impact of the CRA will depend on how it is implemented in the months ahead.

SCALE AND NATURE OF CONFLICT ONLINE

Evolution of cyber operations in warfare (Ukraine and beyond)

The unrestrained use of cyber operations in the armed conflict by Russia in Ukraine continued throughout the second year of the war and is once again the leading reason why we have determined the state of international cybersecurity to be past a proverbial "boiling point." The cyber operations aligned with kinetic strikes that targeted Ukrainian agriculture last summer is just one example of how these attacks can cause widespread and indiscriminate harm. Moreover, given escalating tensions in other regions, there are increasing concerns about the imminent use of cyber operations in other geopolitical conflicts that have been escalating as well.

Trends in nation state activity

The overall volume of nation state threat activity remained at the same level and has persisted over the past year, according to data maintained by the Center for Strategic and International Studies (CSIS) tracking the number of significant cyber incidents each year. However, while the total number of nation state cyberattacks remained consistent, the attacks themselves demonstrated a growing willingness to target critical infrastructure and increasing sophistication. The last year saw notable attacks against civilian water utilities, elections infrastructure, and energy systems, all in apparent violation of established international norms. And state-sponsored cyber operations are increasingly using living-off-the-land techniques to maintain access to systems over a longer period of time, effectively pre-positioning for potentially more damaging attacks in the future.

Development of cybersecurity in the financial and insurance markets

Financial and insurance markets are also responding to the risks posed by escalating cyber conflict. Last summer, the Securities and Exchange Commission (SEC) adopted new transparency and disclosure rules to better inform investors. New legislation is also aimed at improving resilience in the financial sector, such as DORA in Europe (also impacting the IT sector), which entered into force in 2023. The cyber risk insurance market is also growing alongside threats – this includes expanded insurance coverage. and growing Iinsurance premiums (IMF – Chap3) are growing and there is, with a widening gap in the inclusion of SMEs in cyber protection and an increased reliance on cyber rating agencies, which are growing in number though they remain unregulated and not subject to transparency measures. It is too early to tell what ultimate impact these changes will have on the overall security landscape.

TECHNOLOGICAL DEVELOPMENTS

Artificial Intelligence (AI) adoption to augment security/amplify attacks

New AI models are increasingly being integrated into security architecture in ways that are giving advantages to defenders working to identify and mitigate malicious code in a vast sea of data. This includes leveraging AI to discover of the most advanced threats and attacks that pose a national security risk. As with any new and consequential technology, there are malicious uses of AI as well, perhaps most notably to improve social engineering for phishing attacks. However, early research that AI is currently doing far more to improve security than undermine it.

Increasingly sophisticated ransomware attacks

While the overall number of ransomware attacks in the past year not increased, there has been a marked rise in the number of human-operated ransomware attacks and in the sophistication of the campaigns themselves. Attackers are using complicated methods of evading detection and appear to be conducting more narrowly tailored hands-on-keyboard attacks and, unfortunately, finding more success in the process.

ABOUT THE CYBERSECURITY TECH ACCORD

THE CYBERSECURITY TECH ACCORD IS A **GLOBAL COALITION OF 158 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 technology 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, that all stakeholders have a role to play, and we are committed to responsible behavior that helps protect and empower our users and customers. Over the last six years, we have driven dialogue and progress in international cybersecurity while growing our coalition and our partnerships across stakeholder groups.

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

STRONGER DEFENSE

We will protect all of our users and customers everywhere.

NO OFFENSE

We will oppose cyberattacks on innocent citizens and enterprises from anywhere.

CAPACITY BUILDING

We will help empower users, customers and developers to strengthen cybersecurity protection.

COLLECTIVE RESPONSE

We will partner with each other and with like-minded groups to enhance cybersecurity.

NEW SIGNATORIES

We continue to grow and are proud to welcome two new signatories:

PayPal

"Cross-industry initiatives like the Cybersecurity Tech Accord, which engage policymakers and civic stakeholders across a breadth of issues, are critical to addressing the challenges of the 21st century. At PayPal, we believe the world's ability to enhance global cybersecurity will be determined by the strength of our collective collaboration, which is the galvanizing force behind the Cybersecurity Tech Accord".

Jen Silk
Senior Director, Head of the Office of the CISO
PayPal

Kontent.ai

"As Kontent.ai, our decision to join the Cybersecurity Tech Accord was based on our commitment to cybersecurity. We recognize the importance of industry collaboration with like-minded organizations to enhance the security and resilience of cyberspace. By joining this initiative, we can act as a voice of the industry, advocating for stronger cybersecurity and information protection in the digital space. Our participation in the Tech Accord also allows us to contribute to and benefit from the collective knowledge and efforts of the group, working together to protect our customers and users".

Matej Zachar
Chief Information Security Officer – Kontent.ai

OVERVIEW OF OUR SIGNATORY BASE

NUMBER OF SIGNATORIES

34 Signatories
in 2018 to

158 signatories
in 2024

GEOGRAPHICAL DISTRIBUTION

North America
58%

EMEA
29%

LATAM
7%

APAC
5%

Africa
1%

OUR COMMITMENT IN ACTION

After six years of collaboration, our foundational principles continue to drive our agenda forward.

PRINCIPLE 1: STRONGER 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.

PATCHING THE SYSTEM SEASON 2

In October 2023, in partnership with GZERO Media and Microsoft, the Cybersecurity Tech Accord launched season two of "Patching the System", a podcast series as part of GZERO Media's Global Stage Podcasts, moderated by Ali Wyne, Senior Analyst at Eurasia Group. This season focused on the international systems and organizations fostering peace and security online bringing together voices from government and civil society alongside signatories of the Cybersecurity Tech Accord to tackle the most pressing issues at the intersection of geopolitics and technology.

Season 2 featured five episodes of the series:

Episode 1	Guests
"How cyber diplomacy is protecting the world from online threats" focused on the role of cyber diplomats, the threats they are combatting, and how they work with public and private sectors to accomplish their goals.	**Benedikt Wechsler** Switzerland's Ambassador for Digitization **Kaja Ciglic** Senior Director of Digital Diplomacy at Microsoft
Episode 2	Guests
"Cyber mercenaries and the global surveillance-for-hire market" focused on what governments and private enterprises are doing to combat the growth of the cyber mercenary industry.	**Eric Wanger,** Senior Director for Technology Policy, Cisco **Stéphane Duguin,** CEO of the Cyberpeace Institute
Episode 3	Guests
"Foreign influence, cyberspace, and geopolitics" looked at the world of foreign influence operations and how policymakers are adapting.	**I Teija Tiilikainen** Director of the European Center of Excellence for Countering Hybrid Threats **Clint Watts** General Manager of the Microsoft Threat Analysis Center
Episode 4	Guests
"Would the proposed UN Cybercrime Treaty hurt more than it helps?" highlighted the many problematic provisions included in the proposed Russia-sponsored UN cybercrime treaty as negotiations continue - and why they cause more problems than they solve.	**Nick Ashton-Hart** Head of Delegation to the Cybercrime Convention Negotiations for the Cybersecurity Tech Accord **Katitza Rodriguez** Policy Director for Global Privacy at the Electronic Frontier Foundation.
Episode 5	Guests
"Can governments protect us from dangerous software bugs?" delved into how software vulnerabilities are discovered and reported, what government regulators can and can't do, and the strength of a coordinated disclosure process, among other solutions.	**Dustin Childs** Head of Threat Awareness at the Zero Day Initiative at Trend Micro **Serge Droz** From the Forum of Incident Response and Security Teams (FIRST).

CISO BLOG SERIES

Last year, the Cybersecurity Tech Accord CISO blog series continued to showcase what individual signatories are doing to move cybersecurity forward by highlighting initiatives and establishing thought leadership. Our signatories regularly submit blog posts focused on issues that are close to their organization's mission and aligned with the Tech Accord's principles.

In 2023, the CISO blog series featured entries from Kontent.ai, Summit V, Aegis Innovators and onShore Security:

Matej Zachar, CISO of Kontent.ai, wrote about the immense potential value of AI and argued that the risks and challenges it brings must be addressed by many different stakeholders, not just those who are hands-on with the technology.

Jared Hoskins, CEO of Summit V, discussed why his company recommends that airport and aircraft operators expand on the four requirements of new TSA directives and begin developing policies and procedures that mirror those issued to the oil and gas and rail industries.

Reza Palizban, President and Co-founder of Aegis Innovators, wrote about the Biden administration's new cybersecurity strategy, emphasizing the transition towards passwordless authentication as a crucial step in enhancing IT security amidst evolving threats, productivity gains they bring, and alignment with the Zero Trust framework, urging businesses and cybersecurity practitioners to adopt this proactive defense measure.

Stel Valavanis, Founder, President and CEO of onShore Security, examined the potential business, security and political implications of the Biden Administration's new five-pillared cybersecurity strategy.

OUR CISO BLOGS AT A GLANCE

NOVEMBER 8, 2023 **BY MATEJ ZACHAR, CISO, KONTENT.AI**

NAVIGATING THROUGH RESPONSIBLE AND SECURE AI

READ BLOG

"AI security and privacy are crucial and complex issues that require the collaboration and coordination of a multitude of stakeholders, such as users, developers, regulators, and policymakers."

JULY 5, 2023 **BY JARED HOSKINS, CEO, SUMMIT V**

TSA CYBERSECURITY DIRECTIVE FOR AIRPORTS & AIRCRAFT OPERATORS

READ BLOG

"Without an accurate picture of what these systems are and the critical endpoints that are responsible for their normal operations, it is incredibly difficult to design and implement the necessary security controls required to protect them."

2023 **BY REZA PALIZBAN, PRESIDENT AND CO-FOUNDER OF AEGIS INNOVATORS**

THE UNITED STATES EXECUTIVE BRANCH'S INFLUENCE ON CYBERSECURITY: EMBRACING PASSWORDLESS AUTHENTICATION IN THE ZERO TRUST ERA

READ BLOG

"Embracing a Zero Trust mindset requires acknowledging the potential of a breach. Yet, it is here that passwordless technologies shine, significantly lowering the risk of identity compromise. "

MAY 11, 2023 **BY STEL VALAVANIS, FOUNDER, PRESIDENT AND CEO, ONSHORE SECURITY**

BIDEN'S CYBERSECURITY ANNOUNCEMENT - SOME SUBTLE POINTS ARE BEING LOST

READ BLOG

"By making this announcement, the Biden administration is sending a clear warning to cyber attackers that it's no longer business as usual."

PRINCIPLE 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

CYBER MERCENARIES PRINCIPLES

In March 2023, the Cybersecurity Tech Accord released a set of principles to help the technology industry curb the dangerous and rapidly growing market for "cyber mercenaries", a term which refers to a wide range of companies which now develop and sell offensive cyber capabilities and services, generally to governments.

The principles against cyber mercenaries, which build on the Cybersecurity Tech Accord's founding commitments, 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 the cybersecurity awareness of customers, users and the general public;
4. Protect customers and users by maintaining the integrity and security of products and services; and
5. Develop processes for handling valid legal requests for information.

In November 2023, the Paris Peace Forum released the new Paris Call Blueprint on Cyber Mercenaries, which was developed by a coalition within the Paris Call for Trust and Security in Cyberspace and builds on the industry principles released by the Cybersecurity Tech Accord. The multi-stakeholder group issued several recommendations aiming to address this phenomenon, including the development of clear acceptable use guidelines (for Governments), safeguarding of ICT exports from malicious use, preventing their purchase by non-State actors, and the adoption of appropriate internal oversight mechanisms. The Blueprint emphasizes that this challenge requires multistakeholder cooperation and our initiative continues to engage at the multilateral and international level to tackle this growing threat.

As part of our work on cyber mercenaries, we have committed to providing an update on government actions taken against cyber mercenary firms alongside the next gathering of the Paris Peace Forum, in November 2024.

PRINCIPLE 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.

ICT SUPPLY CHAIN SECURITY BLOG SERIES

The Cybersecurity Tech Accord increased our advocacy around protecting the ICT supply chain. In December 2023 we launched our ICT Supply Chain Security Blog series, a statement on our renewed calls for a new global norm on ICT supply chain, and hosted a hybrid event on the side-

lines of the UN open-ended Working Group on security of and in the use of information and communications technologies (OEWG) focused on better protecting the ICT supply chain.

The Tech Accord's "Securing the Digital Backbone" blog series features perspectives from our signatories exploring the pressing and complex issue of ICT supply chain security, including:

- Dr. LaTrea Shine, Director of Supply Chain Security at Lenovo, explored how Software Bill of Materials (SBOM) is not ready for widespread implementation and called for immediate action to address concerns and enhance SBOM's impact across the software supply chain.
- Jesus Muñoz Miguelañez, Global Director of Operational Security and Nuria Talayero, Head Digital Public Policy, Telefónica, discussed how companies can better protect their supply chain to reduce risk and enable a more agile response and how policymakers can ensure protection of global supply chains.

OEWG ON ICT SIDE EVENT: STRENGTHENING SUPPLY CHAIN CYBERSECURITY

As part of our effort on amplifying the need to tackle ICT Supply Chain attacks at the International level, the Cybersecurity Tech Accord hosted a side event during the December 2023 session of the open-ended Working Group on security of and in the use of information and communications technologies (OEWG) to discuss how we can prevent and mitigate threats like the SolarWinds and Kaseya attacks while ensuring resilience and innovation in the digital ecosystem. The event was an opportunity to discuss how the international norms of state behavior should better prevent attacks that are inherently indiscriminate and potentially put thousands of organizations at risk.

STATEMENT CALLING FOR NEW NORM TO PROTECT THE ICT SUPPLY CHAIN

The Cybersecurity Tech Accord called for new norms to protect the ICT supply chain as part of our engagement with the informal sessions of the United Nations' open-ended Working Group on security of and in the use of information and communications technologies (OEWG). During a stakeholder consultation the meeting in December 2023 the Cybersecurity Tech Accord called for the United Nations to agree an international norm to prohibit state-sponsored cyberattacks targeting ICT supply chains. The Tech Accord stated that such cyberattacks can never be consistent with responsible state behavior as they are inherently indiscriminate, irresponsibly disrupting individual citizens' lives and livelihoods.

INTERNATIONAL WOMEN'S DAY 2023

The Cybersecurity Tech Accord believes that International Women's Day presents an opportunity to reflect on the state of the cybersecurity industry's and drive for gender equality. International Women's Day is a reminder of the strides achieved in fostering gender equality across various sectors. It also highlights the continuing obstacles encountered by women in predominantly male-dominated fields, including cybersecurity.

Following 2022's campaign "#MyCybHerStory" where the Cybersecurity Tech Accord put a spotlight on the women who make up our cyber community, last year we continued the campaign by hosting an interactive career webinar exploring cybersecurity careers for women and girls with industry leaders. Women representatives of our Signatory base shared their experiences with women from different ages and professional backgrounds interested in pursuing a cyber career. The Cybersecurity Tech Accord encouraged participants to ask questions and hear from women leaders about their career paths and learn how to identify the right path according to their skillset and interests. We aimed to provide women the platform to engage in a constructive dialogue, promoting discussions and action on the latest cybersecurity trends and the important role women play within the cybersecurity community.

REQUIRED UPDATE NEWSLETTER

In July 2023, we launched "Required Update", our threat intelligence newsletter, to help government stakeholders and cyber diplomacy communities around the world access relevant cybersecurity resources and analysis from the private sector. The newsletter provides quarterly updates to diplomatic communities, informs and supports cyber diplomacy dialogues and features the latest insights and intelligence from across our signatory base.

PRINCIPLE 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.

UN CYBERCRIME NEGOTIATIONS

The Cybersecurity Tech Accord has been actively taking part in the negotiations of the world's first global treaty to address law enforcement cooperation on cybercrime (AHC) since negotiations started in 2021. Our objective has been to ensure the resulting treaty is fit for purpose without compromising cybersecurity or lawful operations of industry.

After the publication of a gravely concerning first draft text in June 2023, we significantly increased our advocacy. The Secretariat of the Cybersecurity Tech Accord, represented by expert Nick Ashton-Hart, worked throughout the two-week, sixth session of the AHC negotiations, alongside other industry and civil society partners urging member states to make changes to address the serious shortcomings we identified in our statement to the committee.

A new draft of the Convention was published on 28 November 2023, which failed to address the many significant shortcomings that we, the rest of industry, and all of civil society had highlighted. If adopted as written the treaty would have significantly weakened cybersecurity, eroded data privacy, reduced rather than facilitated exchanges between law enforcement and undermined internationally recognized online rights and freedoms.

In December 2023, we issued a press release and organized media outreach to ensure the status of the negotiations and shortcomings of the current draft were made public. On January 16, 2024 the Secretariat and the CyberPeace Institute published a new statement revisiting the "Multistakeholder Manifesto" that was launched at the start of the negotiations in 2021, which takes stock of the negotiations and highlights the areas where the treaty needs significant modifications.

The fight is not over, and we will continue to work throughout the remainder of the negotiations to address the draft's many flaws.

OUR PARTNERS

WOMEN4CYBER

"The Women4Cyber Foundation and the Cybersecurity Tech Accord have joined forces to address the gender gap in cybersecurity. The Tech Accord is contributing to one of our most impactful initiatives: our flagship mentorship programme, which is addressed to women at all careers stages, and provides support from securing their first job to guiding them through specialisation and career advancement.

In the ongoing edition of our programme, we aim to mentor 500 women from across Europe. The Tech Accord signatories make this possible by volunteering their employees as mentors. These mentors, equipped with valuable expertise, share real life advice and empower women to navigate the intricate landscape of cybersecurity. Additionally, as part of our collaboration, on the occasion of International Women's Day 2024, Tech Accord and Women4Cyber jointly organised a webinar where Tech Accord leaders shared their personal journeys within the cybersecurity workforce, emphasising the variety of paths within cybersecurity and sharing essential skills needed for success.

This partnership underscores the importance of collaboration across entities, countries, and sectors to achieve our shared goal of advancing inclusivity in cybersecurity. Together, we champion diversity, knowledge sharing, and excellence."

Saskia Brugman
Strategic Partnerships and Activities Coordinator
Women4Cyber Foundation

CYBERPEACE INSTITUTE

"The collaboration between the CyberPeace Institute and Cybersecurity Tech Accord mobilised cybersecurity community members behind our statement to the United Nations Committee negotiating the Cybercrime Convention. This initiative revisited our previous 2021 publication of a Multistakeholder Manifesto calling on Member States engaged in the cybercrime negotiations to prioritise protecting victims; protect human rights and existing international law; and to maintain an open, free, and trusted Internet.

By revisiting the Manifesto in January 2024 at a crucial moment of negotiations, we drew attention to the fact that the substantive input provided by the stakeholder community had not been reflected. We rang alarm bells that the Convention risked facilitating, rather than reducing, cybercrime by significantly weakening cybersecurity, eroding data privacy and trust, increasing conflicts of

laws, and undermining online rights and freedoms. We urged states to adhere to the principles outlined in our Manifesto in shaping a new cybercrime treaty.

The two organizations leveraged our knowledge of the UN process and expertise to produce a relevant and timely statement that members of the cybersecurity community could get behind and demonstrated the weaknesses and risks of the text being negotiated. Efforts by the cybersecurity community seem to have had impact. Member States agreed to "suspend" the meeting and did not adopt the Convention. Informal discussions are now taking place with a view to reconvening later this year.

The Tech Accord is building cooperation and advocating for treaties, policies and regulations that promote cybersecurity contributes to international cyber governance, and has an important convenor role in raising the collective voice of its members and others for a safer online environment".

Charlotte Lindsey
Chief Public Policy Officer
CyberPeace Institute

Coalition for Online Accountability

COALITION FOR ONLINE ACCOUNTABILITY (COA)

"The Tech Accord constitutes a powerful and well respected voice concerning the critical importance of responsible and pragmatic practices to address the escalating threats of cybercrime. The Tech Accord's willingness to engage with a multitude of organizations and to provide insights and guidance to governments and policy makers contribute great value as we collectively seek to diminish cyberattacks and cybercrime across the board".

Dean S. Marks
Emeritus Executive Director & Legal Counsel
Coalition for Online Accountability (COA)

OUR PREVIOUS REPORTS

YEAR 1 REPORT (2019)

View report:
https://cybertechaccord.org/new-report-2018-in-review/

YEAR 2 REPORT (2020)

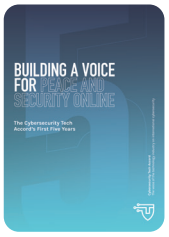
View report:
https://cybertechaccord.org/new-report-2019-year-in-review/

YEAR 3 REPORT (2021)

View report:
https://cybertechaccord.org/2020-in-review-cybersecurity-tech-accord-in-2020/

YEAR 4 REPORT (2022)

View report:
https://cybertechaccord.org/cybersecurity-tech-accord-launches-2021-2022-annual-report/



YEAR 5 REPORT (2023)

View report:
https://cybertechaccord.org/building-a-voice-for-peace-and-security-online-the-cybersecurity-tech-accords-first-five-years/

OUR SIGNATORIES


LaSalle Consulting Partners
LawToolBox
Lenovo
LinkedIn
LIREX.COM IT INNOVATIONS
LogRhythm
Madison Computer Works
MarkMonitor
Protecting brands in the digital world
MediaPRO
mercado libre
Meta
Microsoft
Moback
NEC
NetApp
nielsen
NOKIA
NORTHWAVE
NTT
onShore SECURITY
ORACLE
orange
Panasonic
panda
pango
pax8
PayPal
percipient.ai
predica.
PROFESSIONAL OPTIONS
QOMPLX:
Associates
REDSEAL
Resecurity
reveal
Rockwell Automation
RSA
SOFEPC 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
TRACER
TREND MICRO
UNISYS
USLicensing Group
US Medical IT
VALIDY
vmware
VU
TECHNOLOGIES
WIPFLI
WISeKey
WITH secure
ZENDATA