CYBERSECURITY TECH ACCORD

YEAR 7 REPORT

Cybersecurity Tech Accord
The voice of technology industry on international cybersecurity

CONTENTS

LETTER BY THE SECRETARIAT

Much has changed over the past seven years, since 34 global technology and security companies signed the Cybersecurity Tech Accord in 2018: a unique agreement among an ambitious industry coalition committing to defend all customers everywhere from cyberattacks, regardless of where they originate, and to not participate in offensive cyber operations.

Since 2018, the global cybersecurity landscape has only grown in complexity - a direct result of the geopolitical instability the world has been experiencing, which could not leave the cyber realm unaffected. The number and sophistication of cyber- attacks has continued to rise globally, amplifying the urgency of taking a unified approach on cybersecurity at the international level. While rapid advancements in new and emerging technologies such as AI present a transformative potential for cybersecurity defenders, these new technologies have also meant an increase in the potential attack surface for malicious actors. As more and more organizations race to adopt AI in their operations, cybercriminals are also finding new ways to use AI to exploit vulnerabilities and enhance their attacks. The borderless nature of the internet and the global adoption of AI technology mean that governments and industry must recognize the imperative of robust AI cybersecurity and work together to ensure that the balance is shifted on the side of the defenders.

Amidst these growing concerns, the Cybersecurity Tech Accord has continued to play a unique and important role as the voice of the technology industry on matters of peace and security online. We are proud to have continued to grow and that we have become one of the largest industry-led efforts of this kind, and we resolve to continue to focus on improving standards for cybersecurity through multistakeholder cooperation. Some of our key initiatives from the past year include launching our “Cybersecurity Tech Accord in the Age of AI” blog series, exploring challenges and opportunities for industry brought by the advent of this technology.

We have also continued to consistently engage in relevant dialogues at the United Nations on Internet governance including the Open-Ended Working Group on ICT and the UN Convention on Cybercrime, continuing our efforts to push for more inclusive multistakeholder processes at the UN. Another area of pressing concern has been the need to update international protections to reflect the new reality of warfare in the 21st century, which now often includes a cyber component. With this consideration in mind the Cybersecurity Tech Accord endorsed the Red Cross Digital Emblem pledge, aiming to provide key industry support for a critical initiative: the creation, by the Red Cross, of a distinctive digital emblem to serve as a cyberspace analog to the traditional red cross, red crescent and red crystal emblems.

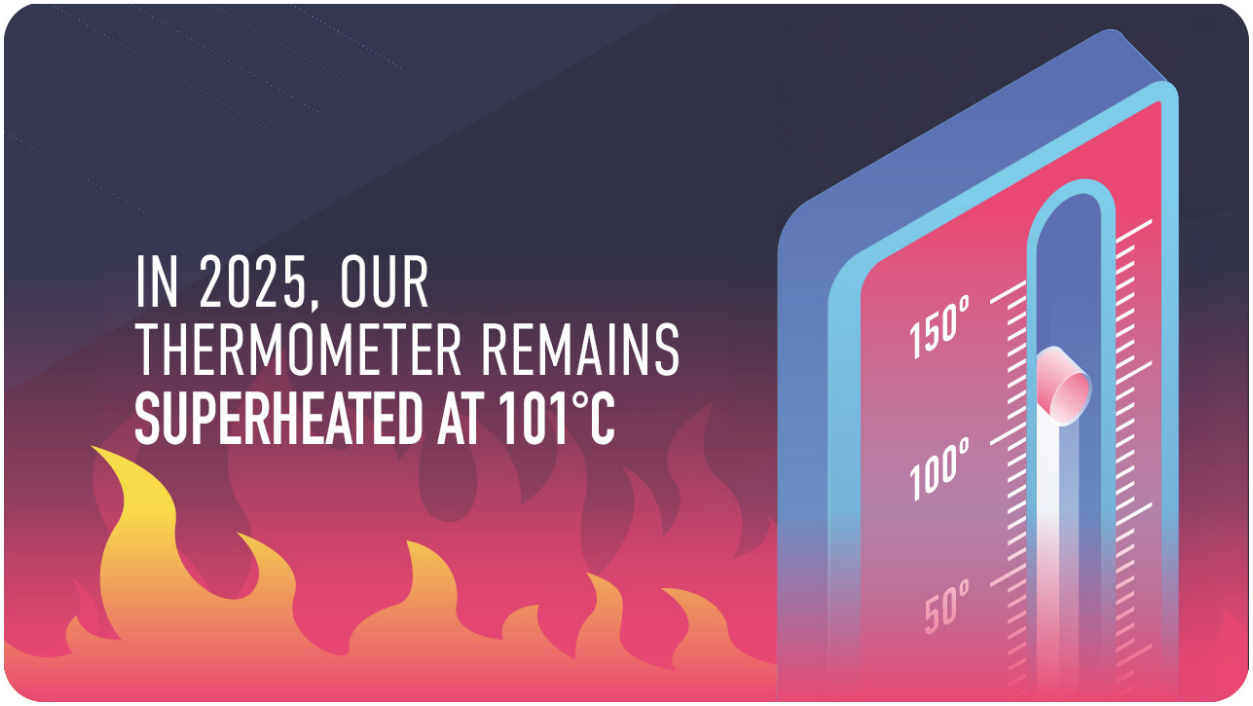
In 2024, we also continued to assess the global state of cybersecurity through our annual State of International Cybersecurity Thermometer, an assessment made by our community taking stock of the current state of conflict and security online. This year, our assessment found that peace and security online has remained stable at 101 degrees – a concerning state, showing no significant improvement, despite some slow progress.

As the world continues to grapple with the reality of new threats, greater instability, and complexity in the cyber domain, the Cybersecurity Tech Accord intends to remain a reliable and consistent advocate in support of developing meaningful multistakeholder solutions, and a trusted source of industry expertise.

The Cybersecurity Tech Accord Secretariat

ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER

INTERNATIONAL CYBERSECURITY THERMOMETER



In 2023, the Cybersecurity Tech Accord launched the "State of International Cybersecurity Thermometer," an annual measure to track the progress of escalation (or de-escalation) of conflict online. We asserted in 2023 that the world had reached a metaphorical "boiling point" of cyber warfare and placed our first Thermometer reading at 100 degrees. In 2024, our coalition of technology and cybersecurity companies from across the tech industry assessed 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 was largely due to the geopolitical tensions and conflict online that had continued to escalate in throughout the year.

In 2025, our assessment is that although the sophistication and impact of nation state cyberattacks has continued to increase, there have been encouraging developments that have helped improve security online and give cause for hope looking forward. For this reason, our assessment is that, on balance the Cybersecurity Thermometer has remained at 101 degrees from last year.

Several recent diplomatic and institutional developments have shown positive signs that governments and international institutions are taking seriously the issue of security in cyberspace, 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 an 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:

Counterproductive developments at the United Nations (UN) through adoption of flawed Cybercrime Treaty

Originally intended to deliver a targeted instrument to counter the growing threat of cybercrime, the UN negotiations on a cybercrime convention produced, after years of negotiations, a broad UN treaty that risks undermining both privacy and security in the digital world. The UN General Assembly adopted the treaty in December 2024, despite concerns from civil society and industry, including the Cybersecurity Tech Accord, that the treaty could be misused by governments to criminalize a broad range of activities online and lead to grave human rights violations.

Limited progress at United Nations (UN) level on establishing a permanent mechanism for ICT security dialogues

Discussions at the UN level on the establishment of a future permanent UN mechanism on international security in ITCs (information and communication technologies) have made limited progress. Although the second Open-ended Working Group (OEWG) on ICTs will conclude its proceedings in 2025, and states recognize the need for such a mechanism to be established for dialogues on ICT security to continue, no agreement has been yet reached on the nature, objectives and modalities of this mechanism.

World Governments make progress in curbing the cyber mercenary market

One year after its launch in February 2024 as a joint initiative by France and the United Kingdom, at the 2nd Pall Mall Conference in April 2025 the two governments announced the formal launch of a new Code of Practice for governments. The Code aims to guide states to mitigate against potential misuse and proliferation of Commercial Cyber Intrusion Capabilities (CCICs). In its proceedings thus far, the Pall Mall Process successfully embraced a multistakeholder approach by acknowledging the importance of public-private partnership, and welcoming industry and civil society input in the development of the Code of Practice for states, which has already been endorsed by 21 states. This is a promising path forward in curbing the cyber mercenary market, although it remains to be seen whether this commitment will translate into action by states, through putting into practice the various important provisions included in the Code.

Tensions in transatlantic relationships threaten progress in cybersecurity cooperation

The recent tensions in transatlantic relations, marked by, among others, distinct domestic politics and disagreements over security issues, may risk threatening the progress achieved in recent years in enhancing cooperation on cybersecurity, through efforts such as the Cyber Dialogues and the Trade and Technology Council. Any steps back in this cooperation would be detrimental to the stability of the global cyber ecosystem as a whole. Despite current disagreements on other policy areas, transatlantic convergence on cybersecurity should be maintained and proactively fostered, given the transborder nature of cybersecurity, and the international dimension of cybersecurity policies.

Governments and industry take steps to address global cyber skills gap

Against a backdrop of escalating cyber threats globally, there is growing awareness among governments and businesses that the existing cybersecurity skills gap worldwide is a challenge that must be urgently tackled through a multistakeholder approach. Through collaboration across sectors and between governments, last year has seen progress being made on fostering a skilled cyber workforce capable of addressing evolving threats. At EU level, ENISA, the EU's cybersecurity agency, published this year the Cybersecurity Education Maturity Assessment

report, aiming to develop a maturity assessment model for the evaluation of EU Member States' cybersecurity education level in primary and secondary schools, and to share recommendations and best practices among countries. It also launched the Cyber Education platform, a tool designed to enhance cyber education across the EU by acting as a central hub for cybersecurity educational resources, tailored for primary and secondary schools in Member States. On the industry side, Cybersecurity Tech Accord signatory Cisco pledged to equip 1.5 million people in the EU with cybersecurity and digital skills by 2030. In the US, the Biden-Harris administration launched the 'Service for America' recruitment program to address the 500,000-strong cybersecurity job gap.

POSITIVE

International Criminal Court releases draft policy to address cyber-enabled war crimes

Following the announcement in 2023 by the Prosecutor of the International Criminal Court (ICC) announced that his office would expand its jurisdiction to include investigations of cyber-enabled war crimes, the ICC launched in spring 2025 a draft Policy on cyber-enabled crimes, which is currently open for public consultation. This welcome development shows alignment with the new realities of modern warfare, where cyber operations are intrinsic to conflicts, and can cause serious harm to civilians. The Policy deals with crimes within the jurisdiction of the ICC, which are criminalized directly under international law, and does not address ordinary cybercrime, which is dealt with by domestic law. Once published, the Policy will guide the future work of the ICC on crimes under the Rome Statute committed or facilitated by cyber means.

SCALE AND NATURE OF CONFLICT ONLINE

NEGATIVE

Evolution of cyber warfare

The ever-intensifying use of cyber operations has demonstrated the effectiveness and efficiency of hybrid warfare, profoundly reshaping how wars are conducted in today's interconnected world. As the lines between state and non-state actors continue to blur—fueled by increasing collaboration between hacking or hacktivist groups and government-affiliated entities—cyberattacks on critical infrastructure have become more frequent and disruptive.

TECHNOLOGICAL DEVELOPMENTS

POSITIVE

Law enforcement makes progress in the fight against cybercrime

The beginning of 2024 witnessed law enforcement agencies worldwide successfully launch major operations disrupting cybercrime, compromising platforms used by cybercrime groups to carry out phishing attacks and deploy ransomware.

During "Operation Cronos", law enforcement authorities from 10 countries disrupted the criminal operation of the notorious LockBit ransomware group at every level, severely damaging their capability. LockBit uses a ransomware-as-a-service (RaaS) model and consistently conceived new ways to stay ahead of its competitors. Its double extortion methods added more pressure to victims, raising the stakes of their campaigns. One of its notable tactics was the creation and use of the malware StealBit, which automates data exfiltration. According to a detailed analysis by Cybersecurity Tech Accord signatory TrendMicro, thanks to the efforts of law enforcement, LockBit's operations were seriously hampered, its reputation in the cybercrime world was tarnished, and several affiliates' identities were disclosed. In an encouraging sign for the global fight against cybercrime, Operation Cronos also involved asset freezes and travel bans issued against the ransomware group's administrator and developer, who currently has a 26-count indictment against him in the US.

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 and that all stakeholders have a role to play. To that end, we are committed to responsible behavior that helps protect and empower our users and customers. Over the last six years, we have worked to grow our coalition, establish partnerships across stakeholder groups, and drive dialogue and progress in international cybersecurity forums.

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

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

Our Initiative continues to grow and since our last report published in April 2024, two new signatories have joined our growing list of now 163 companies:

motorola

"We are excited to join the Cybersecurity Tech Accord to collaborate with global technology companies in enhancing the security, stability, and resilience of network-connected products. Together, we can better protect our customers and users from malicious threats."

Andrew Wheeler
Director of Software Engineering
Motorola

Logically

"Logically was inspired to join the Cybersecurity Tech Accord because we strongly align with its mission to foster an open forum for collaboration and diverse perspectives on safeguarding civilians and improving the resilience of cyberspace. At Logically, our core mission is to empower our customers, partners, and peers to be Cyber First and Future Ready. By joining the Tech Accord, we reaffirm our commitment to contributing to a safer digital world through shared knowledge, cooperation, and innovation, ensuring that we collectively strengthen the security and stability of the global cyberspace."

Zack Finstad
Vice President, Cybersecurity
Logically

privacybee

"We joined Cybersecurity Tech Accord because we believe strongly that the future of cybersecurity includes a layer of External Data Privacy, which is an emerging space only recently brought to light by the surge of AI-generated spear phishing that weaponizes exposed employee PII. These conversations are beginning to happen across InfoSec professionals, and we'd like to be a positive part of that dialog."

Harry Maugans
Founder & CEO
Privacy Bee

PECB

"PECB is committed to advancing global cybersecurity standards, and joining the Cybersecurity Tech Accord allows us to collaborate with like-minded organizations to create a safer digital world. By uniting our expertise, we aim to set new benchmarks in cybersecurity resilience and innovation."

Erdet Grajçevci
Global Brand Strategist
PECB

moonlock

"Moonlock joined the Cybersecurity Tech Accord to reinforce its dedication to creating a safer digital environment. As a cybersecurity tech for humans, Moonlock believes in a world where people are seamlessly protected by technology. By collaborating with industry leaders, Moonlock aims to enhance users' protection from emerging cyber threats and contribute to the global effort in advancing cybersecurity standards."

Anastasiia Kiosieva
Public Relations Specialist
MacPaw

PABLOSEC

"Joining the Cybersecurity Tech Accord underscores our commitment to collaborative defense against emerging cyber threats. We believe cybersecurity is a shared responsibility, requiring active partnership and transparency across industries. By aligning ourselves with global leaders dedicated to cybersecurity principles, we aim to strengthen trust, enhance resilience, and protect the digital ecosystem for our clients and the broader community."

Pablo Jose Trevino Llorens
Director
Pablosec

GEOGRAPHICAL DISTRIBUTION

North America
60%

EMEA
30%

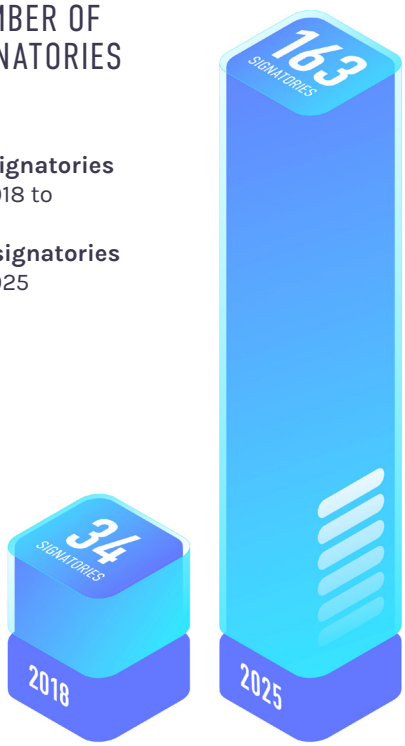
LATAM
5%

APAC
5%

NUMBER OF SIGNATORIES

34 Signatories
in 2018 to

163 signatories
in 2025



OUR COMMITMENT IN ACTION

After six years of collaboration, our foundational principles remain the driving force behind our collective actions. Since our 5-year anniversary in 2023, the Signatories of the Cybersecurity Tech Accord and its Secretariat have continued to uphold our mission of protecting cyberspace.

PRINCIPLE 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.

"THE CYBERSECURITY TECH ACCORD IN THE AGE OF AI" BLOG SERIES

In 2024, the Cybersecurity Tech Accord placed strong emphasis on exploring the multifaceted and evolving intersection of AI and cybersecurity, through launching "The Cybersecurity Tech Accord in the Age of AI": a timely blog series assessing the challenges and opportunities for industry brought about by the emergence of generative artificial intelligence (AI).

The blog series examined the current landscape and capabilities of AI models, the implications for cyber risk, and the immense potential of widespread AI adoption for enhancing cybersecurity. Drawing on insights from our diverse signatories, this series aimed to articulate principles, best practices, gaps, barriers, and recommendations to equip the industry to harness the benefits and mitigate risks posed by AI in cybersecurity. It also proposed a framework for ensuring responsible and trustworthy AI-driven cybersecurity. The series delved into the demand and supply of AI-based cyber defense solutions and skills and discussed the pivotal role and responsibilities of the tech industry in fostering innovation and collaboration. Finally, it also aimed to delineate the roles and responsibilities of the various stakeholders within the AI cybersecurity ecosystem.

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

ICRC

RED CROSS DIGITAL EMBLEM PLEDGE

Last year, on International Human Rights Day – 10th December –, the Cybersecurity Tech Accord endorsed the Red Cross Digital Emblem pledge. This endorsement marked a significant step in adapting international protections to the realities of 21st-century (digital) warfare. This initiative, launched by the Red Cross aims to create a distinctive digital emblem that serves as a cyberspace analog to the traditional red cross, red crescent, and red crystal emblems. The endorsement underscores the Tech Accord's commitment to fostering a secure and stable cyberspace, especially in times of conflict. The digital emblem must be granted the same legal protections under international humanitarian law to ensure it remains a marker of safety and aid in times of need.

The Cybersecurity Tech Accord's support for the digital emblem project reflects its strong and active commitment to promote an inherently secure, and stable cyberspace. By partnering with the International Committee of the Red Cross (ICRC) and other industry stakeholders, the Cybersecurity Tech Accord aims to operationalize the digital emblem and champion principles

that promote respect for international humanitarian law in cyberspace. This initiative is part of the Tech Accord's broader mission to create a secure, stable, and inclusive digital environment.

CYBERMERCENARIES

Last year, the Cybersecurity Tech Accord has continued to play a prominent role in global efforts to counter the growing threat of cyber mercenaries and the commercial intrusion-as-a-service market. Our engagement continued with the Pall Mall Process, an initiative launched by the UK and French governments, which culminated in a declaration endorsed by over 25 governments, reaffirming commitments to limit the harms caused by private sector offensive actors. The Tech Accord, alongside several of its signatories, contributed to this multistakeholder dialogue and has since remained actively engaged.

In October, we participated in the consultation launched by Pall Mall Process ahead of the Paris Peace Forum. In our submission, the Tech Accord emphasized the need for increased state transparency and stronger mechanisms for private sector due diligence, building on its prior advocacy and aligning with the expanded U.S. State Department initiative to counter spyware. The Accord then participated in the Pall Mall Process meeting at the Paris Peace Forum in November, highlighting the breadth of government action since the previous spring and advocating for continued multistakeholder collaboration.

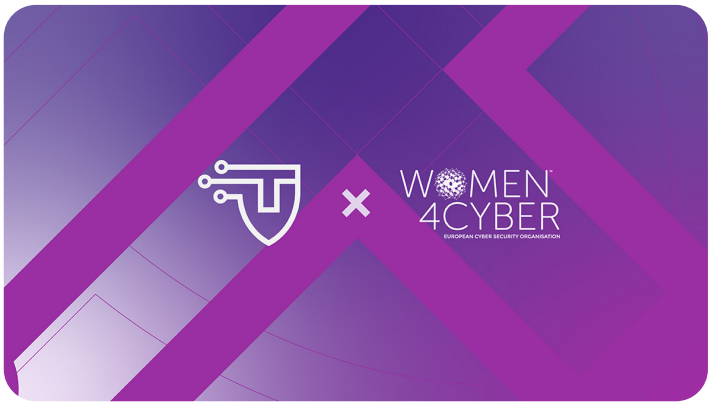
Looking ahead, the Tech Accord working group is developing a taxonomy and scoring criteria to help industry actors evaluate the risk posed by cyber mercenary firms. This framework is intended to support companies in making more informed decisions about partnerships and supply chains, reinforcing responsible corporate behavior in cyberspace. The Accord remains committed to advancing practical, principles-based solutions, and will continue leveraging its collective voice to call for greater accountability and action from both industry and governments to curb the proliferation of private sector offensive cyber capabilities.

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.



INTERNATIONAL WOMEN'S DAY 2024

The Cybersecurity Tech Accord firmly believes that International Women's Day is an opportunity to highlight the importance of gender diversity and the need for more women in cybersecurity professions.

Continuing our tradition of campaigns aimed at supporting women's inclusion in cybersecurity, in 2024, the Cybersecurity Tech Accord partnered with Women4Cyber, a like-minded organization dedicated to promoting women in cybersecurity careers. The Tech Accord supported the flagship Women4Cyber mentorship programme by providing mentors, through some of the women leaders in our community who served as mentors in the programme, and raising awareness of the programme.

On 27 March 2024, we co-hosted an interactive career webinar titled "Cybersecurity Tech Accord X Women4Cyber Mentorship Programme: Bridging the Cybersecurity Gender Gap". The session featured women leaders from our community of signatories, facilitating a fruitful exchange of views and experiences. Participants had the opportunity to hear from leaders discussing their journeys in the cybersecurity workforce and the essential skills needed to succeed in this field. Additionally, attendees received information about the Women4Cyber Mentorship Programme and how to get involved as mentees, directly from women mentors. They also received

valuable tips on choosing the right career path within cybersecurity. The Cybersecurity Tech Accord aimed to provide a platform for women to engage in constructive dialogue, promoting discussions and actions on the latest cybersecurity trends and highlighting the important role women play within the cybersecurity community.

"REQUIRED UPDATE" THREAT INTELLIGENCE NEWSLETTER

"Required Update", our quarterly threat intelligence newsletter launched in 2023, continues to serve as a resource for government stakeholders and the global cyber diplomacy community. It provides timely updates, analysis, and curated cybersecurity resources from Cybersecurity Tech Accord signatory companies, helping to inform ongoing cyber diplomacy dialogues. The newsletter aims to bridge the gap between the private sector and policy communities by highlighting industry insights that can shape and support international cybersecurity discussions.

You can register for the newsletter at: https://cybertechaccord.org/required-update-cybersecurity-tech-accord-launches-quarterly-threat-intelligence-newsletter/. We welcome suggestions or topic requests for future editions and encourage you to reach out to the Cybersecurity Tech Accord Secretariat at info@cybertechaccord.org .

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

In 2024, as the negotiations for a UN Convention on Cybercrime came to an end, the Cybersecurity Tech Accord continued its advocacy to ensure that the treaty does not impose undue harm on the private sector. As an accredited member, our focus since 2021 has been to ensure the outcome of the negotiations are fit for purpose in addressing cybercrime globally.

The Cybersecurity Tech Accord played an active and strategic role in the negotiations surrounding the UN Convention on Cybercrime. Although the Convention was adopted in August 2024 despite the group's reservations on the final text, the Tech Accord in close partnership with non-governmental and civil society partners, successfully advocated for significant improvements to the text.

Key wins included blocking provisions that would have enabled direct data requests to providers, preserving critical safeguards in contentious articles, and preventing harmful criminalization of minors for consensual image sharing. The group also maintained strong advocacy for the protection of cybersecurity researchers, journalists, and penetration testers from unjust prosecution. In parallel to these policy engagements, the Tech Accord mounted an effective communications campaign that shaped global public opinion and, with widespread media coverage framing the Convention in a critical light.

UN OEWG ON ICT ADVOCACY

In 2024, the Cybersecurity Tech Accord participated and delivered statements during the Informal Dialogues with the Chair of the meeting of the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG), which took place in May and December 2024. Despite being rejected accreditation and being barred from participating in the official discussions since their start, the Cybersecurity Tech Accord has long advocated for greater multistakeholder participation in UN cyber processes, and has been providing input into the work of the OEWG since 2019. With the OEWG coming to

an end in 2025, we continue to advocate for meaningful multistakeholder inclusion in this process, as we believe that modalities allowing any single state to veto individual stakeholders are not fit for purpose.

As the OEWG comes to an end, the Cybersecurity Tech Accord continues to believe that the success of the Programme of Action (PoA) on cybersecurity proposed by France, or any other permanent mechanism that follows the OEWG, will depend on its ability to facilitate multistakeholder inclusion in building and maintaining a rules-based order online. In our engagement with the UN, we have therefore stressed that any successor mechanism to the OEWG should ensure modalities similar to the ones established for the Ad-Hoc Committee on Cybercrime, which have proven to be successful and valuable, are the minimum starting place for stakeholder participation. We strongly believe that the scope of a permanent mechanism should include capacity building, should monitor progress and build consensus, and should update and ser new norms that address emerging and unforeseen cyber threats.

POSITIVE AGENDA

As the Open-ended Working Group (OEWG) concludes its mandate in 2025, there is a pressing need to steer member states toward a more inclusive and implementation-focused process that emphasizes accountability. In response to increasing demands from authoritarian governments for a cybersecurity convention at the United Nations, the Cybersecurity Tech Accord is developing a “positive agenda” through a series of expert consultations. These consultations, primarily engaging international legal scholars across regions, aim to reinforce existing international law and norms on responsible state behavior in cyberspace while identifying additional measures to reduce state-driven cyber conflict and protect fundamental freedoms. The first consultation was held in Brussels in June 2024 with European legal experts, followed by a second event in New York City on October 24, which gathered legal experts from across North America.

OUR PARTNERS

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC)

"The International Committee of the Red Cross (ICRC) has been pleased to engage with the Cybersecurity Tech Accord (CTA) on the Digital Emblem Project. The Digital Emblem Pledge, adopted by the CTA in December last year, is an important step in the effort to ensure that international humanitarian law (IHL) remains fit-for-purpose in cyberspace.

The digital emblem is a technological marker being developed that will signal the protection, during armed conflict, of the digital assets of the medical services as well as certain digital humanitarian infrastructure. In other words, it will extend to cyberspace the function the Red Cross, Red Crescent, and Red Crystal emblems have had over the last 160 years in the physical world. By signing the pledge, CTA members demonstrated their commitment to respecting and reinforcing humanitarian protections everywhere – including online.

The Digital Emblem Pledge has been critical in raising awareness and mobilizing industry leaders to support the development, recognition, and future use of the digital emblem. This collaboration also marks an important step building further bridges between the tech industry and IHL, ultimately helping minimize the humanitarian consequences of cyber operations in armed conflict.

By pledging to ensure that their products and services are developed, designed, distributed, and used in compliance with the principles and rules of international humanitarian law, the digital emblem pledge also serves as a catalyst for further unity towards common, humanitarian goals. As harmful cyber activities continue to increase during armed conflict, the ICRC values the engagement with the CTA as a meaningful step toward protecting vulnerable persons affected by armed conflict and identifying meaningful solutions to address contemporary challenges therein."

Samit D'Cunha
Legal Advisor
International Committee of the Red Cross

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

OUR PREVIOUS REPORTS

YEAR 1 REPORT (2018)

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

YEAR 2 REPORT (2019)

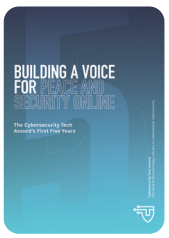
View report:
https://cybertechaccord.org/new-report-2019-year-in-review/

YEAR 3 REPORT (2020)

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

YEAR 4 REPORT (2021)

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



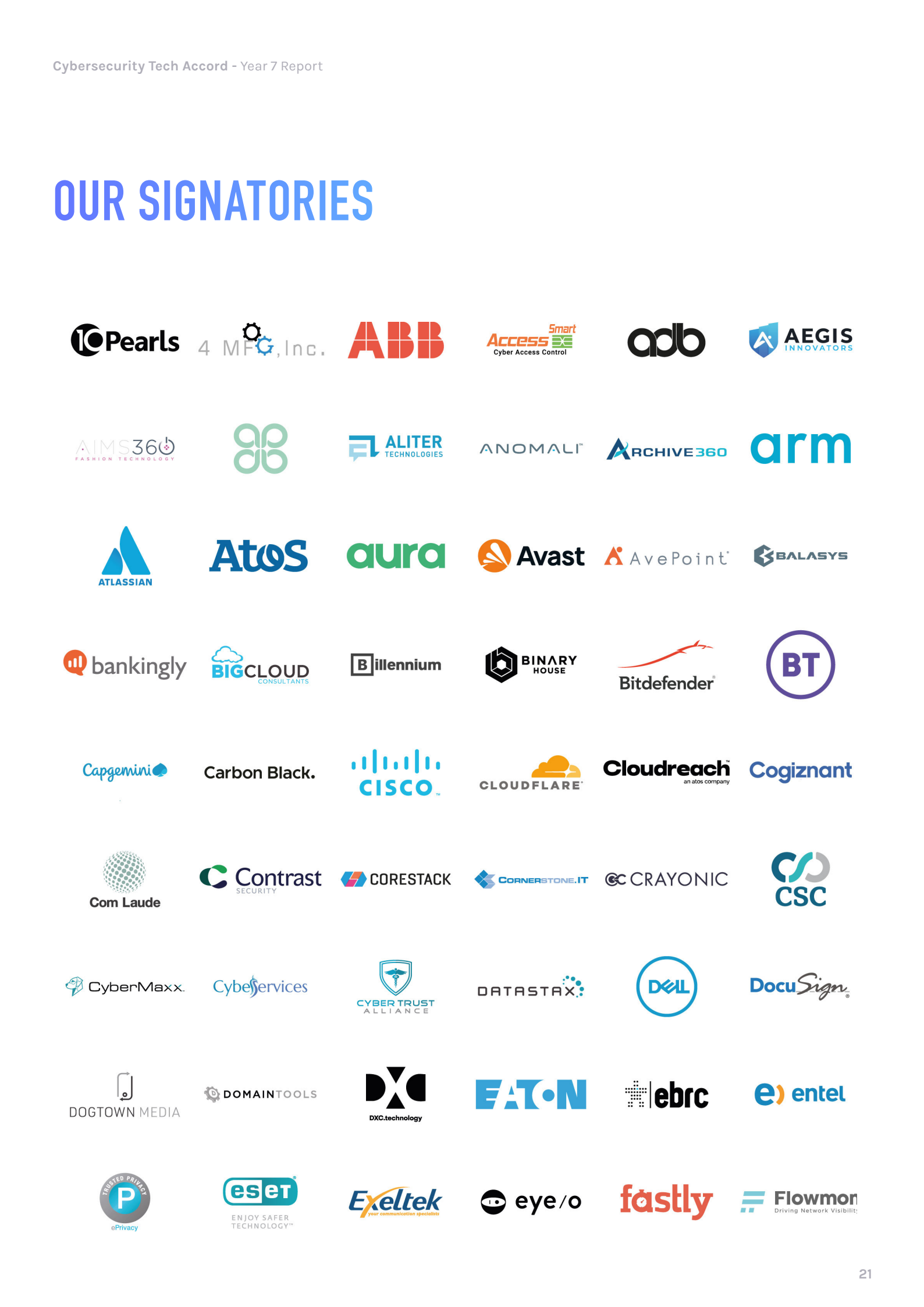
YEAR 5 REPORT (2022)

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

YEAR 6 REPORT (2023)

View report:
https://cybertechaccord.org/cybersecurity-tech-accord-launches-year-six-annual-report/

OUR SIGNATORIES




FRAMEWORK
SECURITY


G DATA


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


Kontent.ai


KOOLSPAN


LaSalle Consulting Partners


LawToolBox.com


Lenovo


LinkedIn


LIREX.COM
IT INNOVATIONS


Logically


LogRhythm


Madison Computer Works


MANDIANT


MarkMonitor
Protecting brands in the digital world


MediaPRO
Cybersecurity & Privacy Education


mercado libre


Meta


Microsoft

Moback

moonlock

motorola

NEC

NetApp

nielsen

NOKIA

NORTHWAVE
Intelligent Security Operations

NTT

ORACLE

orange

PABLOSEC

Panasonic

panda

pango

pax8

PayPal

PECB

percipient.ai

predica.

privacybee

PROFESSIONAL
OPTIONS

QOMPLX:

Associates

REDSEAL

Resecurity


reveal
Rockwell Automation
RSA
SOFE PC SOLUTIONS
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
WCA TECHNOLOGIES
WIPFLI
WISeKey
WITH secure
ZENDATA