CYBERSECURITY TECH ACCORD

YEAR 8 REPORT

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

CONTENTS

LETTER BY THE SECRETARIAT

The global cybersecurity landscape is entering a period of profound transformation. Over the past year accelerating technological change, most notably the rapid advancement of AI, has reshaped both the opportunities and the risks facing the digital ecosystem. These tools are already strengthening cyber defense but they are also lowering the cost and increasing the scale of malicious activity, enabling threat actors to operate with greater speed, scale, and sophistication.

At the same time the strategic role of cyberspace in geopolitical competition continues to intensify. Cyber espionage operations are growing in scale and complexity and cyber capabilities are routinely integrated into military operations. As a result the boundary between cyber conflict and broader security dynamics is blurred, raising urgent questions about how existing norms are applied, how escalation is managed, and how stability can be preserved.

Against this backdrop international cooperation is more important than ever. The convening of the UN Global Mechanism on ICTs in the Context of International Security and other international cybersecurity cooperation efforts reflects a recognition that cybersecurity requires sustained, institutionalized dialogue. Yet this alone is insufficient, global efforts also need clear pathways for implementation, meaningful stakeholder participation, and practical mechanisms for cooperation or the global cyber community will fall short of delivering the decrease in malicious cyber behavior that is urgently needed.

It is in this challenging context that the Cybersecurity Tech Accord has continued to exemplify the unique and significant role of the technology industry as far more than a provider of technology - a partner in shaping and advocating for a more stable and secure digital environment.

Our work is guided by the core conviction that protecting cyberspace requires a rules-based order, grounded in responsible behavior, restraint, and cooperation across governments, industry and civil society.

Over the past year our initiatives have increasingly focused on translating this conviction into actionable priorities. Through our work on agentic AI we have emphasized that technological innovation must be accompanied by governance frameworks that embed security by design, ensure accountability, and preserve human oversight in high-risk contexts. At the international level we have continued to advocate for stronger multistakeholder engagement in UN processes, recognizing that effective cybersecurity frameworks cannot be developed by governments alone.

We are also proud to continue our work on greater gender inclusivity in cybersecurity through our annual International Women's Day campaign. We are grateful to H.E. Ms. Izumi Nakamitsu, UN Under-Secretary-General and High Representative for Disarmament Affairs, the Permanent Mission of the Kingdom of the Netherlands to the United Nations, and the Permanent Mission of El Salvador to the United Nations, for their involvement in the Tech Accord's "Breaking Barriers in Tech Careers" event.

We have also sought to address structural gaps in the global cybersecurity ecosystem. Our calls to strengthen the Common Vulnerabilities and Exposures (CVE) Program highlight the need for sustainable, shared stewardship of critical cybersecurity infrastructure. Our advocacy for international regulatory alignment reflects the growing risk that fragmented policies will undermine collective resilience. And through our continued engagement in initiatives such as the Pall Mall Process, we have called for greater transparency, oversight, and accountability in addressing the proliferation of cyber intrusion capabilities.

These efforts are grounded in a broader assessment: despite important progress, the overall state of international cybersecurity continues to deteriorate. Our 2026 Cybersecurity Thermometer now stands at 95 degrees Celsius which is an indication that the pace of malicious activity, combined with geopolitical tensions and technological disruption, is pushing the global system toward greater instability.

This trajectory is not inevitable but reversing it will require a step change in how stakeholders work together.

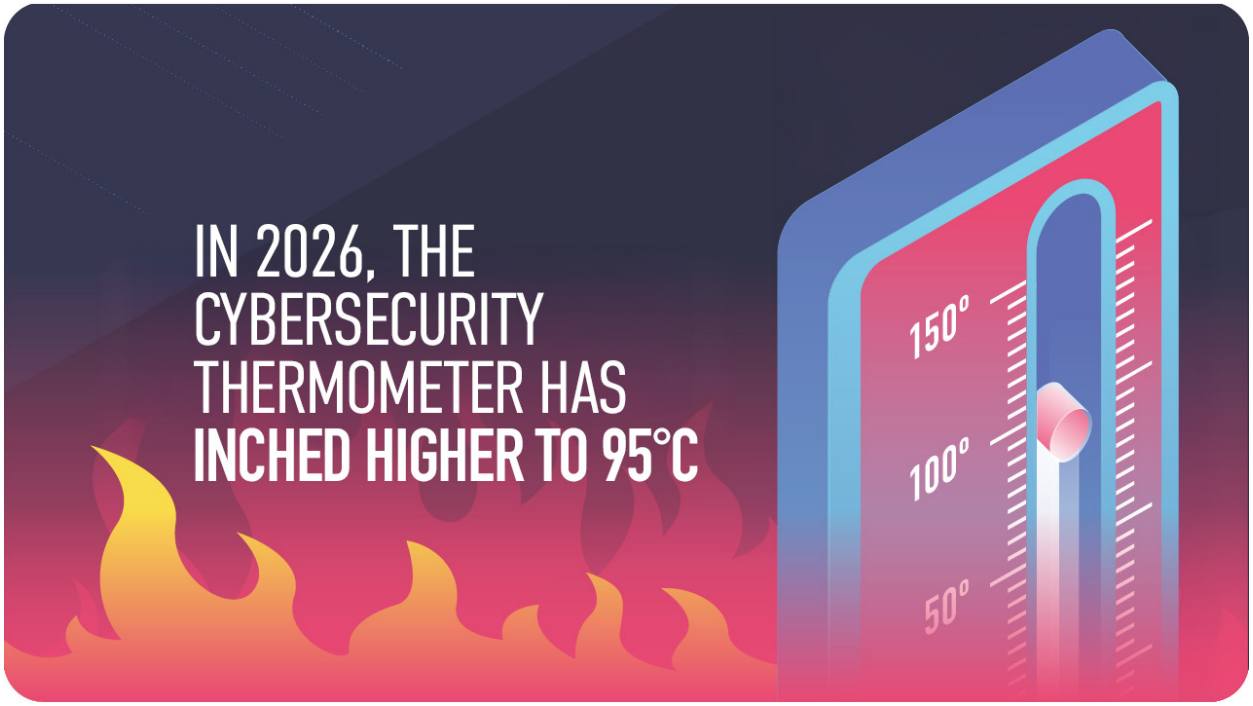
Looking ahead, the Cybersecurity Tech Accord is focused on advancing a positive, actionable agenda for global cybersecurity cooperation that moves beyond high-level principles to identify concrete areas where joint action can deliver real impact. This includes strengthening protection for critical infrastructure, improving supply chain security, expanding coordinated vulnerability disclosure, building global incident response capacity, and enabling more effective cross-border cooperation.

Our objective is clear: to help shape an international cybersecurity environment that is stable, open, and secure, where states exercise restraint, industry upholds its responsibility to defend users, and all stakeholders work together to reduce harm and strengthen collective resilience. Achieving this will require sustained leadership, deeper cooperation, and a renewed commitment to turning shared principles into practical outcomes.

The Cybersecurity Tech Accord Secretariat

ANNUAL STATE OF INTERNATIONAL CYBERSECURITY THERMOMETER

INTERNATIONAL CYBERSECURITY THERMOMETER



The Cybersecurity Tech Accord launched the first edition of the "State of International Cybersecurity Thermometer" in 2023, as an annual assessment of the global state of cyber conflict. **In 2026, although several positive developments create opportunities for improvement, the state of peace and security in cyberspace has grown worse, inching the Cybersecurity Thermometer to 95 degrees Celsius[1].**

This shift reflects the growing deployment and complexity of cyber capabilities in conflicts and military operations around the world, and alongside a broader rise in malicious cyber behavior. Developments in Ukraine, Iran, and Venezuela underscore that cyber activity is increasingly a critical component of warfare. Recent assessments from cybersecurity and intelligence agencies, such as an advisory notice issued in April 2026 by cybersecurity agencies in 10 countries, including the UK, Germany, and the U.S, have shown an increase in the volume and sophistication of cyber espionage operations by nation state actors, targeting critical infrastructure and causing disruption. Beyond cyberespionage, financially motivated attacks such as ransomware, extortion, and large-scale fraud continue to expand in frequency and impact, targeting both public and private sector organizations. At the same time, the growing industrialization of cybercrime and the use of AI to scale phishing, social engineering, and other malicious activity are making disruptive attacks faster, cheaper, and harder to defend against.

1 As demonstrated by the conflicts in Ukraine, Iran, and elsewhere, cyber operations are now a regular dimension of modern warfare to an extent that was not the case when we launched the thermometer. We have reassessed the scale of the Cybersecurity Thermometer to account for this, which is why the 2026 Thermometer reads 95 degrees Celsius, a lower number than in 2025.

Major advances in AI are reshaping the cybersecurity landscape: boosting defenders' capability to detect and respond, while also amplifying concerns about AI-enabled cyber risk. The capabilities that major foundation models globally are expected to reach within six to nine months is a watershed moment that requires a step change in international cybersecurity cooperation. Industry is stepping up to this challenge (Project Glasswing being a notable example) and demonstrating practical action to defend the world's cyber infrastructure. Governments and international institutions also showed a commitment to cooperation on responsible behavior in cyberspace with the launch of the UN Global Mechanism on ICTs in the Context of International Security. Although much work remains to be done, we hope that efforts like this can be built over the next year.

The State of International Cybersecurity Thermometer aims to provide a clear and objective assessment of the current cyber risk landscape. It seeks to identify key trends and developments over the past year and measures necessary to enhance digital stability and security. This year's developments fall into three categories: i) diplomatic and institutional developments, ii) the scale and nature of conflict online, and iii) technological developments. The sections below describe each development and note whether its overall impact on the security landscape was positive, negative, or neutral.

100° CELSIUS AND ABOVE EXTENSIVE CYBER WARFARE

Exceeding the boiling point signifies a chaotic, dangerous, and volatile situation, including cyber operations in the context of armed conflict that has harmed and/or targeted civilians.

Evidenced by:

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

0° - 99° CELSIUS CYBER CONFLICT

This "liquid" state represents 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
- Frequent, normalized abuses by nonstate actors
- Limited progress in diplomatic forums

LESS THAN 0° CELSIUS 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 it.

Evidenced by:

- Scarcity of state sponsored cyber operations that violate international norms
- Limited threats posed by other actors
- Increasing capacity for international cooperation by incident responders

DIPLOMATIC AND INSTITUTIONAL DEVELOPMENTS:

United Nations creates a permanent body for international cybersecurity policy

Following the conclusion of the second Open-ended Working Group (OEWG) on ICTs in 2025, the UN created a permanent body to address the role of states in international cybersecurity. The "Global Mechanism on ICTs in the Context of International Security" (or "GMech") is set to hold its first official meeting in July 2026.

A permanent body is a welcome development as it shows that the international community recognizes that this policy domain requires ongoing action, especially addressing the behavior of member-states. Regrettably, the GMech will operate on a consensus basis, in which member-states must all agree on any decisions. This will encourage lowest-common-denominator agreements and make policies that meaningfully reduce global cyber risk extremely difficult to adopt. The ongoing debate around the GMech's modalities, priorities, and agenda provides an early example of the challenges posed by strictly consensus decision-making. The organizational session of GMech in March 2026 demonstrated that the new forum will inherit the issues with the second OEWG on ICTs, including that it will be difficult to ensure meaningful non-governmental stakeholder participation.

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

In December 2025, the ICC Office of the Prosecutor launched a Policy on Cyber-Enabled Crimes under the Rome Statute, aiming to respond effectively to the evolving ways in which Rome Statute crimes may be committed. The Policy sets out the ICC's understanding of how its legal framework applies to conduct in cyberspace which may constitute crimes under its jurisdiction, such as genocide, crimes against humanity, and war crimes. These international crimes may be facilitated through cyberspace, and digital evidence may be key to establishing them. This welcome reinforcement that international law applies to cyberspace also reflects an understanding of the need to effectively address the cyber dimensions of modern conflict.

Limited progress made in curbing the cyber mercenary

According to several reports, including a study by the Economic Security Council of Ukraine and the Parliament of Ukraine, the global cyber mercenary market is expected to triple in size by 2033 despite international efforts to counter such activities. The study found little evidence that any of the countries that signed up to the Pall Mall Code of Practice have changed their behavior in handling cyber intrusion capabilities. In seven of the signatories (the United States, France, Germany, Italy, Hungary, Greece, and Ireland) spyware companies are still present or have technical infrastructure that allows the deployment of cyber intrusion capabilities.

The Cybersecurity Tech Accord will continue to draw attention to the danger posed by cyber mercenaries to the entire online ecosystem by enabling irresponsible use and allowing state and non-state actors to carry out offensive cyber operations. In anticipation of the upcoming Code of Practice for industry, whose role is equally significant, we call for a swift implementation of the Pall Mall Code of Practice by endorsing states to meaningfully restrict the cyber mercenary market.

National Cybersecurity Strategies increasingly shift towards offensive postures

In recent months, many states have updated their national cybersecurity strategies to encompass more offensive postures. Several governments are building on their defensive cyber capabilities by adding offensive cyber capabilities, designed to disrupt or destroy adversary systems.

While governments have a legitimate responsibility to ensure their national security increasing reliance on offensive cyber operations risks contributing to a cycle of escalation that undermines global stability, trust, and security. Increased offensive cyber activity may offer states some short-term strategic advantages but may damage the entire cybersecurity ecosystem over time. This shift requires international cooperation on common thresholds, and careful legal and diplomatic balancing to ensure transparency and respect for international norms.

Since its launch the Cybersecurity Tech Accord has been grounded in a clear commitment: signatories will not knowingly undermine the security of the online environment, and will oppose cyberattacks on innocent citizens and enterprises. We remain committed to the principle of "no offense" and call on states to recognize the importance of restraint, transparency, and adherence to the norms for responsible state behavior, prioritizing defensive over offensive actions.

NEUTRAL

Flawed UN Cybercrime Treaty moves towards implementation despite widespread criticism

The recently adopted UN Cybercrime Treaty, which aims to establish a global framework for preventing, investigating and prosecuting cybercrime by promoting international cooperation was signed in Vietnam in October 2025 by more than 70 states. Despite criticism from human rights groups and industry, including the Cybersecurity Tech Accord, regarding the broad scope and criminalization provisions and potential for weaponization of the treaty by authoritarian states, some countries are moving forward with the treaty's ratification and implementation.

During the adoption of the treaty it was agreed that the Ad Hoc Committee (AHC) that negotiated it would resume work one year after the Treaty was adopted to negotiate further provisions, including additional offenses, in a Protocol. That process has now begun and negotiations are scheduled for January 2027. During this phase it will be essential for democratic states to ensure that the Protocol can strengthen human rights safeguards in the treaty, advance transparency, and reduce the capacity for the Convention to be used contrary to the values of the UN Charter.

SCALE AND NATURE OF CONFLICT ONLINE

NEGATIVE

Cyber espionage operations by state actors intensify

According to an advisory notice issued in April 2026 by cybersecurity agencies in 10 countries, including the UK, Germany, and the U.S., China-nexus cyber actors are using large scale networks of compromised devices (covert networks) to carry out cyber attacks. While China-nexus actors' use of covert networks is well-documented, the notice warns that the actors are now using the tool strategically and at scale. A China-backed actor, flagged by cybersecurity agencies as a user of covert networks, has infiltrated critical infrastructure in the U.S. such as aviation and water systems. In addition, an assessment released by Finland's intelligence service in March 2026 stated that Russia and China continue to conduct extensive cyber espionage and influence operations targeting the country's technology sector, including cyber intrusions, traditional espionage and political influence campaigns. In Singapore, authorities announced in February 2026 that a China-linked group carried out a targeted campaign against all of the country's major telecommunications operators using advanced tools to infiltrate telecom networks and maintain long-term covert access. Recent Microsoft threat intelligence also shows how state-backed espionage operations are becoming more covert and resilient. In May 2026, Microsoft documented how the Russian-linked Kazuar malware has evolved into a modular peer-to-

peer botnet designed to maintain persistent, low-visibility access to target environments for long-term intelligence collection. Through our work, the Cybersecurity Tech Accord has encouraged businesses and users to play their part and help limit opportunities for cyber espionage by threat actors through improved cyber hygiene, such as better securing internet-connected network devices.

NEGATIVE

Deployment of cyber capabilities in military operations intensifies

The use of cyber capabilities in sustaining military operations has increased globally in intensity, complexity, and scope. According to a recent report by RUSI, cyber is now a critical capability in supporting reconnaissance and broader intelligence-gathering efforts in the time preceding a military operation: "mapping adversary networks; pre-positioning access within critical systems; and informing the planning of subsequent phases". The same report notes that in the case of U.S.-Israeli cyber operations in Iran the U.S. distilled two different roles for its Cyber Command: "as 'first-movers' in using 'non-kinetic effects' to shape the environment for the subsequent phases of the operation; and secondly, in maintaining a 'continuous layering' throughout the first 57 hours of the operation". Cyber capabilities were also deployed by the U.S., alongside kinetic force, to capture Venezuelan President Nicolás Maduro in Operation Absolute Resolve, although their precise role remains unclear.

In parallel, data from our signatory Resecurity identified that the Iran war has fast evolved into a multidomain confrontation where traditional strikes are tightly interwoven with cyber operations, electronic interference, and psychological warfare. Resecurity showed that hacktivist groups aligned with both sides have been involved in the conflict, executing DDoS attacks, website defacements, and reconnaissance missions targeting critical infrastructure and government resources across the Middle East. These digital campaigns are synchronized with physical operations to intensify operational impact and strategic pressure. Resecurity identified several key groups involved in the escalation, including Iranian-aligned hacktivist collectives such as Cyber Islamic Resistance and Cyber Fattah. The operations extend beyond disruption, as the parties to the conflict are also using cyber reconnaissance to support military targeting and assess damage, reflecting a coordinated approach to warfare where cyber operations are integrated with kinetic ones.

TECHNOLOGICAL DEVELOPMENTS

POSITIVE

Emergence of new capabilities in advanced AI systems increase AI-driven cyber risk while also greatly increasing the capacity of defenders to protect systems

The unveiling of Claude Mythos Preview in April 2026, a frontier AI model by Anthropic, which was followed shortly by OpenAI's GPT 5.5, have created an inflection point in the application of AI to cybersecurity. As part of the response Anthropic launched Project Glasswing, an initiative that brings together more than 40 major companies including Cybersecurity Tech Accord signatories Cisco and Microsoft, in an effort to ensure systemically critical systems and platforms are patched before equivalent capabilities are available to malicious actors. As part of Project Glasswing industry partners are using Mythos Preview as part of their cyber defense work and sharing insights with the wider industry to strengthen cyber defenses.

These systems can identify unknown vulnerabilities autonomously and carry out complex cyber operations with minimal human input. It achieved a 83.1% success rate on the CyberGym benchmark, an industry test of vulnerability detection, and autonomously identified thousands of zero-day vulnerabilities across every major operating system. Additionally, Mythos can analyze compiled binary code without access to

source code. While the full implications are still unfolding, it is clear that this marks a structural shift for cybersecurity. AI cyber capabilities are now so powerful that AI is fundamentally necessary to defend against attacks which leverage AI. It is likely that Mythos-class capabilities will be in wide circulation within six to nine months, so the race is on to secure critical systems globally before these tools are in wide circulation.

Under this new reality, organizations and governments must improve their cyber posture to both leverage and prepare for frontier AI. The imperative to deepen international cooperation to address cyber risks is more crucial than ever, before similar capabilities are developed by state actors known to sponsor cyberattacks (such as China and Russia). The Cybersecurity Tech Accord's is currently working on proposals to deliver positive action in reducing global cyberattacks and increase accountability for those that engage in them, through defining practical steps to pursue through international public-private partnerships.

ABOUT THE CYBERSECURITY TECH ACCORD

THE CYBERSECURITY TECH ACCORD IS A **GLOBAL COALITION OF MORE THAN 150 TECHNOLOGY FIRMS** COMMITTED TO ADVANCING TRUST AND SECURITY IN CYBERSPACE.

Since our founding in 2018 with 34 signatories we have provided a voice for the 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 eight years we have worked to 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.

GEOGRAPHICAL DISTRIBUTION

North America
60%

EMEA
30%

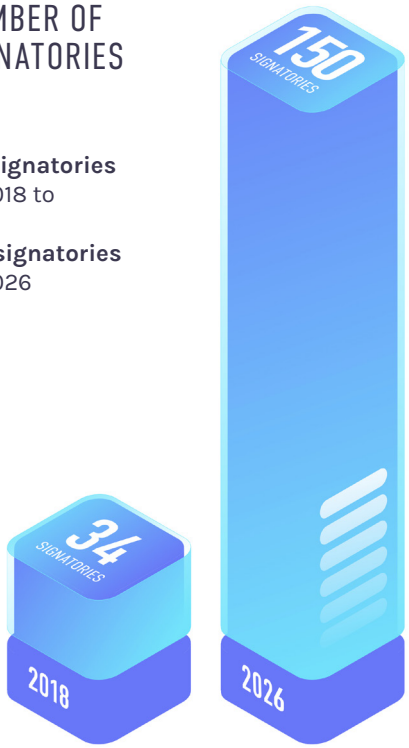
LATAM
5%

APAC
5%

NUMBER OF SIGNATORIES

34 Signatories
in 2018 to

150 signatories
in 2026



OUR COMMITMENT IN ACTION

After eight years our foundational principles remain the driving force behind our collective actions. Since our 5-year anniversary in 2023, our Signatories and our 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 the conducted by an individual, organization or government – irrespective of their technical acumen, culture, location, or the motives of the attacker.

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"

As agentic AI systems move rapidly from experimentation to deployment, the Cybersecurity Tech Accord has identified their governance and security implications as a central policy challenge. Unlike earlier forms of AI, agentic systems can set goals, act autonomously, and interact with sensitive environments capabilities that are already transforming cybersecurity by enabling real-time threat detection, adaptive defense, and automated response at scale. At the same time, this shift introduces a more complex risk landscape, including expanded attack surfaces, susceptibility to manipulation, diminished human oversight, and the potential for unintended

escalation. Against this backdrop, the series emphasizes that securing agentic AI is not simply a technical task, but a governance imperative requiring coordinated action across industry, governments, and civil society. Against this backdrop, the Tech Accord launched a **three-part blog** series that explored concrete use cases of agentic AI across sectors, with a focus on cybersecurity. The series highlighted how autonomous agents are already transforming incident response by enabling continuous threat detection, automated response, and scalable coordination.

As part of this series, the Cybersecurity Tech Accord advanced a set of policy recommendations to guide the responsible development and deployment of agentic AI. These include embedding security and governance principles from the outset through secure-by-design approaches and clear institutional guardrails; strengthening transparency and accountability by ensuring systems are auditable and their decision-making processes can be understood; and establishing defined thresholds for human-in-the-loop intervention in high-risk contexts. The Tech Accord also calls for continuous, real-time risk monitoring to detect and mitigate threats as they emerge, as well as for greater international alignment on standards and norms to ensure agentic systems operate in line with responsible behavior in cyberspace.

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.

Pall Mall Process

PALL MALL PROCESS ENGAGEMENT

Throughout the past year, the Cybersecurity Tech Accord alongside several signatories has remained actively engaged in the Pall Mall Process. This is an initiative by the UK and French governments which delivered a declaration endorsed by over 25 governments reaffirming commitments to curb the harms caused by the misuse of cyber intrusion capabilities by offensive actors.

In April 2025 the Cybersecurity Tech Accord took part in the 2nd Pall Mall Conference where UK and France announced the formal launch of a new Code of Practice for governments that aims to guide states to mitigate against misuse and proliferation of Commercial Cyber Intrusion Capabilities (CCICs). The Tech Accord submitted an official consultation response concerning the Code of Practice for States prior to its launch. Our key recommendations focused on the pillars of the Code of Practice dedicated to oversight and transparency. On oversight we recommend including provisions to ensure that the structures put in place are effective by reviewing their activity and ensuring their independence and impartiality. On transparency we recommended that the Code include provisions asking states to develop a standardized reporting format to support robust information sharing between governments.

In December 2025 the Tech Accord contributed to a consultation of the Pall Mall process on cyber intrusion industry practices to feed into the ongoing development of a set of industry guidelines for responsible development and use of cyber intrusion capabilities, complementary to the Code of Practice for states. We remain committed to playing an active role in global efforts to counter the growing threat of cyber mercenaries and the commercial intrusion-as-a-service market.

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.

Cybersecurity Tech Accord Event: "Breaking barriers in Tech Careers". *From left to right:* ***Kim van der Sluis****, First Secretary Political Affairs, Permanent Mission of the Kingdom of the Netherlands to the United Nations;* ***Naria Santa Lucia****, General Manager, Skills for Social Impact and US Community Engagement Microsoft Philanthropies;* ***Selene Giupponi****, Managing Director for Europe, Resecurity & Council Member, Women4Cyber Foundation;* ***H.E. Ms. Evelyn Wever-Croes****, Prime Minister of Aruba;* ***Allison Pytlak****, Senior Fellow and Director, Cyber Program, Stimson Center and moderator;* ***Edna Conway****, former Chief Security and Risk Officer at Microsoft and Cisco, and current Board Director, CEO, Non-Resident Scholar, Carnegie Endowment for International Peace, and Chief Operating & Risk Officer, TPO Group;* ***H.E. Egriselda López****, Permanent Representative of El Salvador to the United Nations;* ***Julia Rodríguez Acosta****, Minister Counsellor, Permanent Mission of El Salvador to the United Nations.*

INTERNATIONAL WOMEN'S DAY 2025 EVENT: "BREAKING BARRIERS IN TECH CAREERS"

The Cybersecurity Tech Accord firmly believes that International Women's Day is an opportunity to highlight the importance of gender diversity and inclusivity, and the need for more women in cybersecurity professions, but also in the broader digital sector. Currently, women comprise only 22% of the cybersecurity workforce. In line with this, in March 2025 we co-hosted a side event at the 69th session of the Commission on the Status of Women (CSW) at United Nations Headquarters in New York, titled "Breaking Barriers in Tech Careers". The session was organized in partnership with the Permanent Mission of the Kingdom of the Netherlands to the United Nations and the Permanent Mission of El Salvador to the United Nations. Our event brought together high-level representatives from government, the private sector, and the UN with opening remarks from H.E. Ms. Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs. The participants' interventions focused on the important progress made in the implementation of the Platform for Action and the achievement of gender equality and the empowerment of women, especially when it comes to education and training of women, and their participation in cybersecurity and STEM careers, but also on the work that remains to be done.

CYBERSECURITY TECH ACCORD STATEMENT ON THE COMMON VULNERABILITIES AND EXPOSURES (CVE) PROGRAM

In February 2026 the Cybersecurity Tech Accord issued a public statement calling for stronger international support for the Common Vulnerabilities and Exposures (CVE) Program, underscoring its status as critical global cybersecurity infrastructure. We reaffirmed the importance of the CVE Program as a foundational mechanism for identifying, cataloguing and sharing information on cybersecurity vulnerabilities worldwide, enabling coordinated risk management across both the public and private sectors.

The Cybersecurity Tech Accord highlighted that a strong and transparent CVE Program is essential to minimize exposure to cyber threats and to support responsible vulnerability disclosure at an international level. At the same time, we sought to draw attention to the structural challenges facing the long term sustainability of the CVE Program.

Despite its global importance, the program has historically relied heavily on oversight and funding from a limited number of stakeholders - notably the United States government. This model carries inherent risks for a resource relied upon by the global cybersecurity ecosystem. Our statement called for a shared resourcing model based on active participation by governments worldwide, urging governments to move beyond passive endorsement by contributing to its stewardship. This includes supporting sustainable funding models, aligning national vulnerability disclosure policies with global best practices, and engaging in governance structures that reinforce the program's transparency and effectiveness.

The statement also emphasized the importance of collaboration between governments, industry, and civil society to ensure that vulnerability information remains reliable, accessible, and globally interoperable. Such shared commitment is key to reinforcing international cybersecurity resilience in an increasingly interconnected digital environment.

Through this call to action, the Cybersecurity Tech Accord reaffirmed its commitment to promoting responsible cybersecurity practices and to supporting global mechanisms that underpin trust, transparency, and coordinated response in the digital ecosystem.

CYBERSECURITY TECH ACCORD STATEMENT ON THE NEED TO ADVANCE INTERNATIONAL REGULATORY ALIGNMENT IN CYBERSECURITY

In March 2026, the Cybersecurity Tech Accord issued a statement calling for stronger international alignment in cybersecurity regulation directed at OECD member-states, warning that growing fragmentation across national and regional regimes risks undermining global cyber resilience. As cyber threats increasingly transcend borders the statement highlighted that divergent regulatory approaches could drain scarce cybersecurity expertise into duplicative compliance efforts at the expense of threat prevention and incident response. This challenge is particularly important given an already constrained global cybersecurity workforce and an escalating threat environment.

The statement emphasized that regulatory alignment is not about lowering standards or curbing national sovereignty, but improving security outcomes through coherence and interoperability. The Tech Accord, building on growing momentum from industry and governments alike, urged OECD member states to make alignment a core policy objective. This includes a 2025 joint call from more than 50 global Chief Information Security Officers for greater regulatory convergence, a public commitment from the Chair of the OECD Working Party, as well as the launch of Business at OECD's initiative to address fragmentation.

To enable progress the Cybersecurity Tech Accord outlined five priority actions for policymakers:

1. Anchoring cybersecurity regulation in international standards;
2. Developing a common baseline for cyber incident reporting;

3. Enabling mutual recognition of equivalent cybersecurity requirements;
4. Strengthening domestic coordination among regulators; and
5. Institutionalizing meaningful multistakeholder engagement.

Effective regulatory alignment would allow both governments and industry to focus resources on defending networks, responding to incidents, and building long term resilience, strengthening collective cybersecurity across jurisdictions and sectors.

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.

CYBERSECURITY TECH ACCORD ENGAGEMENT TO ADVANCE GLOBAL CYBERSECURITY COOPERATION

Authoritarian states like Russia, China, North Korea, and Iran, widely recognized as among the most active sponsors of cyberattacks, have advanced a proposal for a new UN treaty on ICT security **that would grant governments sweeping powers over the Internet, data flows, and digital infrastructure. Framed as necessary to tackle the escalating threat landscape, proponents argue that only binding international legal obligations can effectively address cyber risks.**

At the same time, democratic governments have not articulated an agenda for international cybersecurity cooperation that can effectively counter such initiatives. There remains a lack of operational clarity on how the eleven UN norms of responsible state behavior should be implemented. Likewise, the broader business and security community has so far failed to articulate a holistic, common positive agenda for global cooperation on cybersecurity to address the growing volume and sophistication of cyberattacks.

To help close these gaps the Cybersecurity Tech Accord has been exploring options for enhanced industry cooperation, through a Blueprint for Global Cyber Stability, currently under development. This initiative will aim

to define a set of practical priorities to pursue through international public-private partnerships that can deliver real action in reducing global cyberattacks and hold those that engage in them accountable.

High-priority areas being explored include:

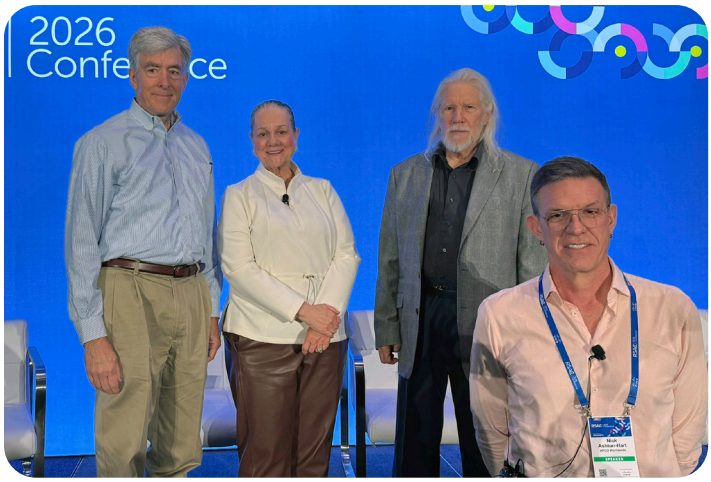
- **Protecting critical infrastructure**, such as through identifying a minimum list of critical infrastructure sectors, defining baseline protection standards, and enabling cross-border assistance.
- **Securing ICT supply chains**, through agreed international mechanisms on comprehensive risk assess¬ments, transparency, and international best practices for supply chain security.
- **Strengthening vulnerability disclosure frameworks**, ensuring protection for good-faith researchers, developing interoperable processes for cross-border vulnerability disclosure, and encouraging the use of the existing global CVE database.
- **Building and increasing capacity for national CERTs, and ensuring all states have at least one**, to improve global incident response capacity.
- **Developing international incident response protocols**, enabling coordinated, real-time action across jurisdictions, and increasing threat intelligence sharing.

Now more than ever, governments, industry and civil society must come together to advance a credible, inclusive, and positive agenda for global cybersecurity cooperation capable of addressing the growing scale and complexity of cyber threats through common action. The Cybersecurity Tech Accord and its signatories are uniquely positioned to help drive this effort. By aligning around a clear set of priorities and actively shaping this Blueprint for Global Cyber Stability, signatories can help catalyze the global cooperation needed to secure a stable, open, and rights respecting digital future. **The Cybersecurity Tech Accord invites all industry partners to contact us to hear more about the Blueprint for Global Cyber Stability and contribute their expertise, provide feedback, and actively support the development and implementation of this agenda.**

SHAPING THE FUTURE OF GLOBAL CYBERSECURITY COOPERATION: INSIGHTS FROM THE CYBERSECURITY TECH ACCORD EVENT AT RSA

Ahead of RSA, the Cybersecurity Tech Accord had already been developing options for greater industry co-operation and impact in pushing back against authoritarian visions for cyberspace. The discussion at RSA helped reinforce several of these priorities, particularly the need for clearer definitions around critical infrastructure, stronger public-private coordination, greater operational clarity in international policy, and a more active role for industry in shaping the future of cybersecurity governance.

On 26 March at the RSAC Conference, the Cybersecurity Tech Accord organized a panel discussion on how the private sector and open societies can work together on a positive, holistic international agenda for reducing cyber insecurity. The session, moderated by **Nick Ashton-Hart**, Head of the Cybersecurity Tech Accord, opened with a video message from Vint Cerf, one of the fathers of the Internet, Vice-President and Chief Internet Evangelist at Google. Mr. Cerf emphasized the central challenge facing today's Internet governance: how to make the Internet a safer place while preserving the freedoms that have defined it for more than fifty years. To meet this challenge, Mr. Cerf stressed the importance of developing a shared understanding of what a "safer Internet" should look like, including the principles and safeguards required.



Cybersecurity Tech Accord Event at RSA Conference: "Trick or Treaty: How Authoritarians Are Hacking Global Cyber Rules". *From left to right:* Chris Inglis*, the first National Cyber Director of the United States and current board member of MITRE, AIG, Huntington National Bank, and Andesite;* Edna Conway*, former Chief Security and Risk Officer at Microsoft and Cisco, and current Board Director, CEO, Non-Resident Scholar, Carnegie Endowment for International Peace, and Chief Operating & Risk Officer, TPO Group;* Whitfield Diffie*, one of the fathers of public key encryption and current Honorary Fellow at Gonville & Caius College at Cambridge; and* Nick Ashton-Hart*, Head of the Cybersecurity Tech Accord and moderator.*

"We need to articulate collectively what the desirable properties are for a safer Internet, what practices need to be obtained, and how we do this in an internationally collaborative way" – Vint Cert

The discussion then turned to **Chris Inglis**, the first U.S. National Cyber Director, who highlighted a core divide in how democratic and autocratic systems understand "information security." In democracies, it is generally about using governance to protect a free and open society; in autocracies, it is often framed as protecting the state. He argued that the private sector is well placed to help reduce the ambiguity that still shapes cyberspace and pointed to areas where industry can have real impact: clarifying what counts as critical infrastructure, reducing ambiguity in policy language, grounding change in real-world practice, and strengthening proven mechanisms such as shared CERT responses and cross-border cooperation.

"Here's my recommendation: do your homework and take a position. You don't need to align with a geopolitical coalition, but you should take a position on behalf of your customers." – Chris Inglis

The panel also addressed the topic of encryption, as authoritarian states' push for a UN treaty on "ICT security" raises questions about backdoors in encryption technologies. **Whitfield Diffie**, one of the fathers of public key encryption and current Honorary Fellow at Gonville & Caius College at Cambridge, explained that the debate has shifted over time towards calls for regulatory action, with governments arguing that they should also regulate encrypted communications and tools including messaging platforms. To support this shift, arguments increasingly rely on emotionally charged scenarios, including terrorism, online radicalization, or child protection.

"[The encryption debate] has evolved into something that [governments] are much more likely to win [by picking up issues that people find frightening or revolting]" – Whitfield Diffie

Edna Conway, former Chief Security and Risk Officer at Cisco, and VP, Chief Security and Risk Officer of Microsoft's Azure Infrastructure, current Board Director, CEO, Non-Resident Scholar, Carnegie Endowment

for International Peace, and Chief Operating & Risk Officer, TPO Group, encouraged the private sector, and particularly CISOs, to speak out in both public and private forums. She urged them to coordinate internally, engage directly with governments, and strengthen public-private partnerships, which are more essential than ever.

"I believe the private sector has an opportunity—and a responsibility—to step up again and say: we want these allies with us. More importantly, we want to hear the voices that differ from our own." – Edna Conway

Ms. Conway concluded by encouraging industry representatives from the security community to contribute to the **positive agenda** for cybersecurity and to **join the Cybersecurity Tech Accord**. Now is the time to coordinate efforts and be ready when the next treaty proposal is tabled, a process which is already underway.

WISEKEY EVENT AT THE WORLD ECONOMIC FORUM IN DAVOS

On 21 January 2026, WISeKey and the Cybersecurity Tech Accord hosted a roundtable and reception at the World Economic Forum WEF on quantum security with the theme "Age of Convergence". The roundtable was marked by strong participation and active engagement throughout. Discussions highlighted the rapid convergence of key technologies, such as AI, cybersecurity, semiconductors, and space infrastructure, and how they are already reshaping global digital ecosystems. Participants emphasized the importance of ensuring security and trust as foundational elements, especially as interconnected systems increase complexity and potential vulnerabilities.

Another important conclusion from the roundtable was the need for enhanced cross-sector collaboration. As these technologies converge, no single industry can address the challenges alone. Public-private partnerships and international cooperation were highlighted as essential to building resilient and interoperable systems. Finally, there was a strong consensus on maintaining a human-centric approach to innovation. As technological capabilities expand, ensuring alignment with ethical principles, privacy, and human dignity remains critical.

Building on these themes, the roundtable also identified several actions governments can take to accelerate quantum readiness:

- **Establish quantum safety as a national cybersecurity priority:** Position quantum-safe cryptography as a strategic imperative and embed it into national cybersecurity frameworks.
- **Align quantum-safe strategies across jurisdictions:** Harmonize public policies, standards, and transition timelines. The G7 should lead by expanding its financial sector post-quantum cryptography workstream to align G7 members' broader quantum-safe strategies.
- **Adopt international standards:** Support global standards development and avoid fragmented, region-specific approaches that hinder interoperability, innovation, and security.
- **Set early and progressive timelines:** Drive action well before 2030. For instance, the U.S. CNSS Policy 15 mandates quantum-safe algorithms in all new products and services for national security systems by January 2027.
- **Lead by example with transparent transition plans:** Publish and regularly update government transition roadmaps—including timelines, milestones, and budgets—to foster knowledge sharing and best practices.
- **Raise awareness and build workforce capacity:** Educate the public and critical infrastructure sectors on quantum risks and readiness. Invest in skilling programs to equip the workforce for a quantum-safe transition.

Speakers included:

- **Carlos Creus Moreira**, Founder, Chairman, and CEO, WISeKey
- **Grant Bourzikas**, Chief Security Officer, Cloudflare
- **María Pía Aqueveque Jabbaz**, Technologist & Systems Architect in AI Governance
- **Mark Hughes**, Global Managing Partner of IBM Consulting Cybersecurity Services
- **Guillem Martinez Roura**, AI and Robotics Program Officer, International Telecommunications Union

OUR PARTNERS

PERMANENT MISSION OF EL SALVADOR TO THE UNITED NATIONS

"Last year, El Salvador had the privilege of partnering with the Cybersecurity Tech Accord on the event 'Breaking Barriers in Tech Careers,' held on the sidelines of the 69th Commission on the Status of Women. Together, we helped create a space that brought visibility to one of the defining challenges of our time: ensuring that women are not only included in the digital future, but empowered to lead it.

Our partnership reflected a shared belief that cybersecurity and digital governance cannot be effective, legitimate or truly global if half of humanity remains underrepresented in shaping them. Through this collaboration, we elevated the voices of women in cyber diplomacy, highlighted pathways for women and girls in STEM, and reinforced the importance of investing in capacity-building initiatives that open doors for the next generation of female leaders.

For countries like El Salvador, these partnerships matter. They demonstrate how governments, industry and international organizations can work together to turn commitments into action and create real opportunities for inclusion.

Initiatives like the Cybersecurity Tech Accord play an essential role in international cyber governance. In an increasingly interconnected world, governments cannot address digital challenges alone. Industry brings innovation, expertise and global reach. By engaging constructively with Member States and other stakeholders, the Tech Accord helps build a more inclusive, resilient and collaborative digital ecosystem, one where women's leadership is not the exception, but the norm".

Egriselda Aracely González López
Ambassador
Permanent Representative of El Salvador to the United Nations

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/

YEAR 7 REPORT (2024)

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

OUR SIGNATORIES


FRAMEWORK
SECURITY


G DATA


Gigamon


GitHub


GitLab


Globant


GREENLIGHT
CYBER


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

ON
Empresas

ORACLE

orange

PABLOSEC

Panasonic

panda

pango

pax8

PayPal

PECB

percipient.ai

predica.

privacybee

PROFESSIONAL
OPTIONS

QOMPLX:

Associates

REDSEAL


Resecurity

reveal

Rockwell
Automation

RSA

SAFE 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

TECH
mahindra

TIM

Telefónica

telelink

tenable

ThreatModeler

TRACER

TREND
MICRO

UNISYS

USLicensing Group

US Medical IT

VALIDY

vmware

VU

WCA
TECHNOLOGIES

WIPFLI

WISeKey

WITH
secure

ZENDATA
CYBERSECURITY