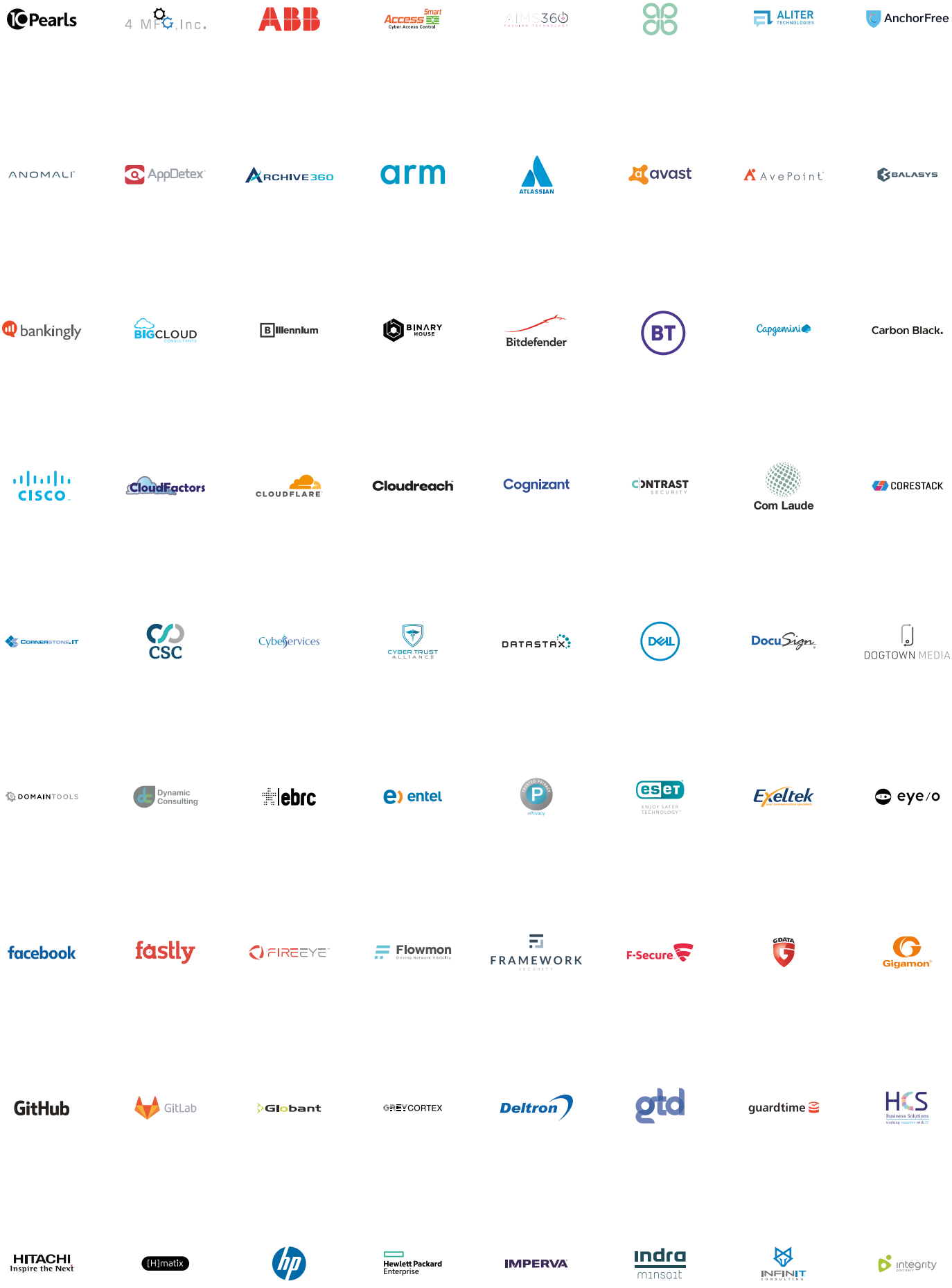
2019 IN REVIEW

Cybersecurity Tech Accord
The voice of technology industry on international cybersecurity


10Pearls
4 MF Inc.
ABB
Access Smart
AIMS360
ALITER TECHNOLOGIES
AnchorFree
ANOMALI
AppDetex
ARCHIVE360
arm
ATLASSIAN
avast
AvePoint
BALASYS
bankingly
BIGCLOUD
Illennium
BINARY HOUSE
Bitdefender
BT
Capgemini
Carbon Black.
CISCO
CloudFactors
CLOUDFLARE
Cloudreach
Cognizant
CONTRAST SECURITY
Com Laude
CORESTACK
CORNERSTONE.IT
CSC
Cybeservices
CYBER TRUST ALLIANCE
DATASTAX
DELL
DocuSign
DOGTOWN MEDIA
DOMAINTOOLS
Dynamic Consulting
ebrc
entel
ESET
Exeltek
eye/o
facebook
fastly
FIREEYE
Flowmon
FRAMEWORK SECURITY
F-Secure
Gigamon
GitHub
GitLab
Globant
GREYCORTEX
Deltron
gtd
guardtime
HCS
HITACHI
Inspire the Next
[H]matix
Hewlett Packard Enterprise
IMPERVA
indra
minsait
INFINIT
integrity


International
SOFTWARE SYSTEMS

intuit

JUNIPER
NETWORKS

KOOLSPAN

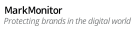
kpn

LaSalle Consulting Partners

LawToolBox

LinkedIn

LIREX.COM
IT INNOVATIONS

Madison Computer Works

MarkMonitor
Protecting brands in the digital world

MediaPRO

mercado
libre

Microsoft

nap
Solutions

NetApp

nielsen

NOKIA

NORTHWAVE

NTT

onShore
SECURITY

ORACLE

orange

PALADION

Panasonic

panda

pax8

perclpient.ai

predica.

PROFESSIONAL
OPTIONS

QOMPLX:

Associates

Resecurity

reveal

Rockwell
Automation

RSA

SAFE PC CLOUD

safetica

salesforce

SAP

Schneider
Electric

Scitum

secucloud

SecurityScorecard

SHARP

SILENT BREACH

SONDA

SSRD

STACKPATH

STRATA
Information Technology

stripe

StrongConnexions

swisscom

SWITCHFAST

Synack

TADGROUP

TANIUM

TIM

Telefónica

telelink

tenable

ThreatModeler

TREND
MICRO

UNISYS

US Licensing Group

US Medical IT

VALIDY

vmware

VU

TECHNOLOGIES

WIPFLI

WISeKey

144 COMPANIES COMMITTED TO PROTECTING CYBERSPACE

The online world has become a cornerstone of our global society, important to every aspect of our public infrastructure and our private lives.

As we look to the future, increased connectivity and new technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and even addressing environmental sustainability. In this process, virtually all entities are being digitally transformed, and much of our environment is becoming "smart" and connected.

However, malicious actors, with motives ranging from criminal to geopolitical, have taken advantage of this new digital ecosystem and inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. Attacks on the availability, confidentiality, and integrity of data, products, services, and networks have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity. Moreover, the vast connected network of entities and things across the globe today requires a new effort to ensure that good cybersecurity practices are integrated throughout the lifecycle of the products and services that underpin it.

In April 2018, 34 global technology and security companies signed the Cybersecurity Tech Accord, a watershed agreement and public commitment to protect and empower civilians online. Since then, this initiative has become the largest industry-led effort of its kind, with 144 signatory companies across the world pledging to improve the security, stability and resilience of cyberspace. This growth in numbers alone demonstrates the importance of this initiative, and the growing awareness across the technology industry that action is needed.

However, the Cybersecurity Tech Accord signatories have done much more than simply issuing a pledge.

Real change takes time and comes about as a result of many incremental steps. Over the past year, the group has sought to move the needle by working across 14 different initiatives – gathering input from other groups across government and civil society to ensure our focus is addressing needs, organizing events and workshops to further awareness of key cybersecurity initiatives, providing input on critical policy matters, and taking concrete steps to improve security. While each of these initiatives is described later in this report, we are especially proud of two, in particular.

Vulnerability Disclosure Policy Promotion

From the beginning, Cybersecurity Tech Accord signatories identified vulnerability disclosure policies and equity processes as key priorities.

In 2018, we called for governments to follow the United Kingdom and United States' examples in adopting vulnerability equities processes and put forward a set of principles to guide those efforts. We also endorsed the Global Forum on Cyber Expertise (GFCE)'s set of good practices for organizations on the adoption of vulnerability disclosure policies.

In 2019, we built on these efforts further.

Most significantly, all Cybersecurity Tech Accord signatories agreed to put a vulnerability disclosure policy in place. We have internally shared good practices for companies to consider in this effort and will share these through our webinar series in the future. To date, over 50% of signatories have now adopted a vulnerability disclosure policy.

These have been collected in a single area of the website, making it easier for anyone looking to understand how they can report a vulnerability to find the relevant data and contacts, as well as setting an example of what these policies can look like in different contexts across the technology industry.

The Cybersecurity Tech Accord signatories talked about the importance of vulnerability disclosure at events in Washington DC, and at the United Nations in Geneva. Several of our signatories also agreed to participate in the expert working group on the topic hosted by the Organization for Economic Cooperation and Development (OECD), which we hope will lead to a set of new guidelines in this space in the coming year.

Apps 4 Digital Peace Competition

The Cybersecurity Tech Accord signatories have been vocal proponents of continued dialogue at the United Nations on issues related to international peace and security online.

To this end, we welcomed the start of the discussions on these topics through the United Nations Group of Governmental Experts and the Open Ended Working Group, as we believe these issues are essential to the long-term stability of our online environment. As an international community, we need to agree upon a set of rules, laws, and norms of behavior for states in cyberspace, and ensure that these expectations are implemented and reinforced through investments in capacity building.

We have also repeatedly called for the multistakeholder community to be included in those discussions. This is why we were honored to be able to join not only governments, but also over 100 organizations from the private sector and civil society, in a consultative meeting at the United Nations this past December.

At this gathering, the Cybersecurity Tech Accord was able to share its signatories' understanding of the threat landscape we face, as well as put forward concrete proposals on confidence building measures to encourage restraint from offensive and provocative actions online.

However, in this challenging and ever-shifting issue space, fresh ideas and innovation are essential to further progress. This is why we were excited to partner with the United Nations Office of Disarmament Affairs and the United Nations Envoy on Youth to launch Apps 4 Digital Peace. This first-of-its-kind competition looks to young problem solvers the world over to help us think about cybersecurity challenges in new ways and propose new solutions. Launched in December, winners will be announced at the 75th UN General Assembly in September 2020.

OUR JOURNEY DOES NOT STOP HERE.

In our third year, the Cybersecurity Tech Accord signatories will continue to live up to our founding principles and strive to be active members of the diverse, global, and collaborative multistakeholder community that contributes to the stability of our shared online environment.

In our third year, the Cybersecurity Tech Accord signatories will continue to live up to our founding principles and strive to be active members of the diverse, global, and collaborative multistakeholder community that contributes to the stability of our shared online environment. We will honor our principles by investing in and innovating our cybersecurity practices and sharing the lessons we learn with others. We will especially focus on implementing the pledge for all of our signatories to have vulnerability disclosure policies in place – and on then ensuring that these are effectively managed and used.

We also hope to continue be an insightful partner for governments, especially as the United Nations discussions on international peace and security in cyberspace enter into their final phases of deliberation. We will continue to use every opportunity available to put forward suggestions that aim to halt and reverse what has been a persistent slide towards escalating cyberconflict, and will work with others in the industry, as well as civil society and governments, to identify concrete proposals to implement and uphold existing agreements.

Finally, in the next year we will deepen our investments in cybersecurity capacity building and awareness raising efforts, building on our partnership with the United Kingdom's Foreign and Commonwealth Office and the Global Forum on Cyber Expertise. We will also target new audiences and partner with those who know them best to ensure we are effective in our outreach. Even more importantly, we will seek to bring disparate efforts in this space together in order to amplify their impact. Whether by working to implement technical standards that improve cyber hygiene, or seeking to raise awareness of the importance of security in the Internet of Things, we will strive to be a true voice for the technology industry on international cybersecurity.

HOW THE CYBERSECURITY TECH ACCORD LIVES UP TO ITS PRINCIPLES

Protecting our online environment is in everyone's interest and we all have a part to play.

Cybersecurity Tech Accord signatories stand up for principles that reflect a future where enterprises that create and operate online technologies promise to defend and advance its benefits for society. Moreover, we commit to act responsibly, to protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace.

1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.
2. WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.
3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.
4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

1

Strong defense: We believe everyone deserves equal protection online irrespective of technical acumen, culture, location or motive for any malicious attack.

- The security and stability of our online environment needs fresh thinking and innovation. This is why the Cybersecurity Tech Accord is excited to partner with the United Nations Office of Disarmament Affairs and the United Nations Youth Envoy on Apps 4 Digital Peace. This first-of-its-kind competition looks to young problem solvers globally to help us think about cybersecurity challenges in new ways. Launched in December, winners will be announced at the UN General Assembly in September 2020.

- This commitment is as much about group action as it is about individual company actions. This is why we started an initiative that showcases how our signatories are implementing the Cybersecurity Tech Accord principles. You can already explore the first eleven case studies.

2

No offense: We are committed to not knowingly undermining the security of the online environment, and to protecting against efforts to tamper with our products and services.

- The Cybersecurity Tech Accord has been a vocal proponent of continued dialogue at the United Nations on issues to related international peace and security in online. Moreover, we repeatedly called for the multistakeholder community to be included in those discussions. Finally, we were able to have our voice heard when, in December, our representatives joined over 100 organizations and UN member states for a consultative meeting to advance expectations for responsible state behavior online.

- Cybersecurity Tech Accord signatories also engaged in other multistakeholder fora that deal with government action in cyberspace. We are an active participant in the Internet Governance Forum and have sought to focus their work on implementation of existing cybersecurity commitments.

- A year after we first endorsed the Paris Call for Trust and Security in Cyberspace, we were joined by over 1,000 other entities – including states, businesses, and NGOs – that share its values. We are excited to have been included in the Paris Call Community initiative and are committed to leading to help ensure two Paris Call principles - Principle 7 on advancing cyber hygiene and Principle 8 on preventing "hack back" – become a reality.

- Encryption continued to be a contested topic in the past year. The Cybersecurity Tech Accord joined nearly 50 other organizations in calling on the G7 governments to prioritize cybersecurity and not to require technology companies to "modify their products or services or delay patching a bug or security vulnerability to provide exceptional access to encrypted content; turn off 'encryption-on-by-default'; cease offering end-to-end encrypted services; or otherwise undermine the security of encrypted services."

3

Capacity building: We see cybersecurity as a shared responsibility and work to improve both the ability of everyone to act securely and safely online as well as the diversity of the security practitioner community.

- October has been designated Cybersecurity Awareness Month by a growing number of countries around the world. This year, the Cybersecurity Tech Accord joined the in effort and used this designation to promote cybersecurity good practices, collating a set of helpful resources to support individuals, businesses and governments alike.

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

- Our capacity building webinar series is now in its second year. Whether the audience wanted to learn about ransomware, email protection, network forensics, or another cutting edge cybersecurity innovation, our signatories were able to provide an overview across ten webinars, which remain available to view through our website.

4

Collective response: We believe we can achieve more together and will partner within the group and more broadly to address critical cybersecurity challenges.

- The impact of vulnerability disclosure policies on our security posture has been top of mind this past year. We began implementing our pledge to ensure all our signatories have vulnerability disclosure policies in place, with 54% already having reached that goal. The group also sought to promote greater awareness of this important topic at events in Washington, DC and Geneva.

- The Cybersecurity Tech Accord signatories engaged with the Organisation for Economic Co-operation and Development to find path a forward that would heighten awareness of the effective management of product vulnerabilities, as well as improve the security of all products and services.

- In 2019, Internet of Things (IoT) security emerged priority area for providers, manufacturers, and governments to work on collectively. To this end, our signatories partnered on and endorsed the collaborative process that the UK National Cybersecurity Center employed to develop an IoT "code of conduct," and which is now also being considered at the European level.

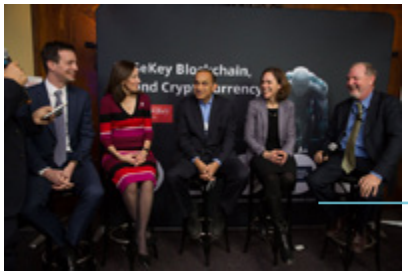
- A key mission for the group has always been to leverage its signatories' expertise to identify and promote good practices that will help us address today's cybersecurity challenges, as well as tomorrow's. Indeed, we think this is our unique value add – no other group brings together hardware security experts from the United States, platform providers from Latin America, and cybersecurity vendors from Europe. To this end we announced a blog series, "a view from the front lines of cybersecurity," that gives voice to signatories to share their unique views on what are the most pressing challenges.

- Finally, we know that we can and must continue to do better. To help improve our collective understanding of existing concerns and identify new areas of focus, the Cybersecurity Tech Accord consulted with civil society groups at RightsCon and the Internet Governance Forum and continue to welcome feedback on our work and priorities.

CONTRIBUTING TO THE GLOBAL MULTI-STAKEHOLDER DIALOGUE ON CYBERSECURITY

The Importance of dialogue across industries and sectors cannot be overstated, and no field is this more true than in cybersecurity.

This is why the Cybersecurity Tech Accord is proud to be the leading technology industry voice on issues related to international peace and security in cyberspace, engaging with governments, civil society, and other private sector players on topics that will determine our future as a global community in cyberspace.



Cybersecurity Tech Accord returned to the World Economic Forum in Davos in 2020, engaging with global business leaders to discuss the future of cybersecurity.

Cybersecurity Tech Accord was honored to deliver remarks to the first United Nations Intersessional Meeting on Cybersecurity in December 2019.

CISA Cybersecurity Summit in Washington DC brought together policy makers and the technology industry in a dialogue around securing critical infrastructures. Cybersecurity Tech Accord representatives stressed the importance of vulnerability disclosure policies.

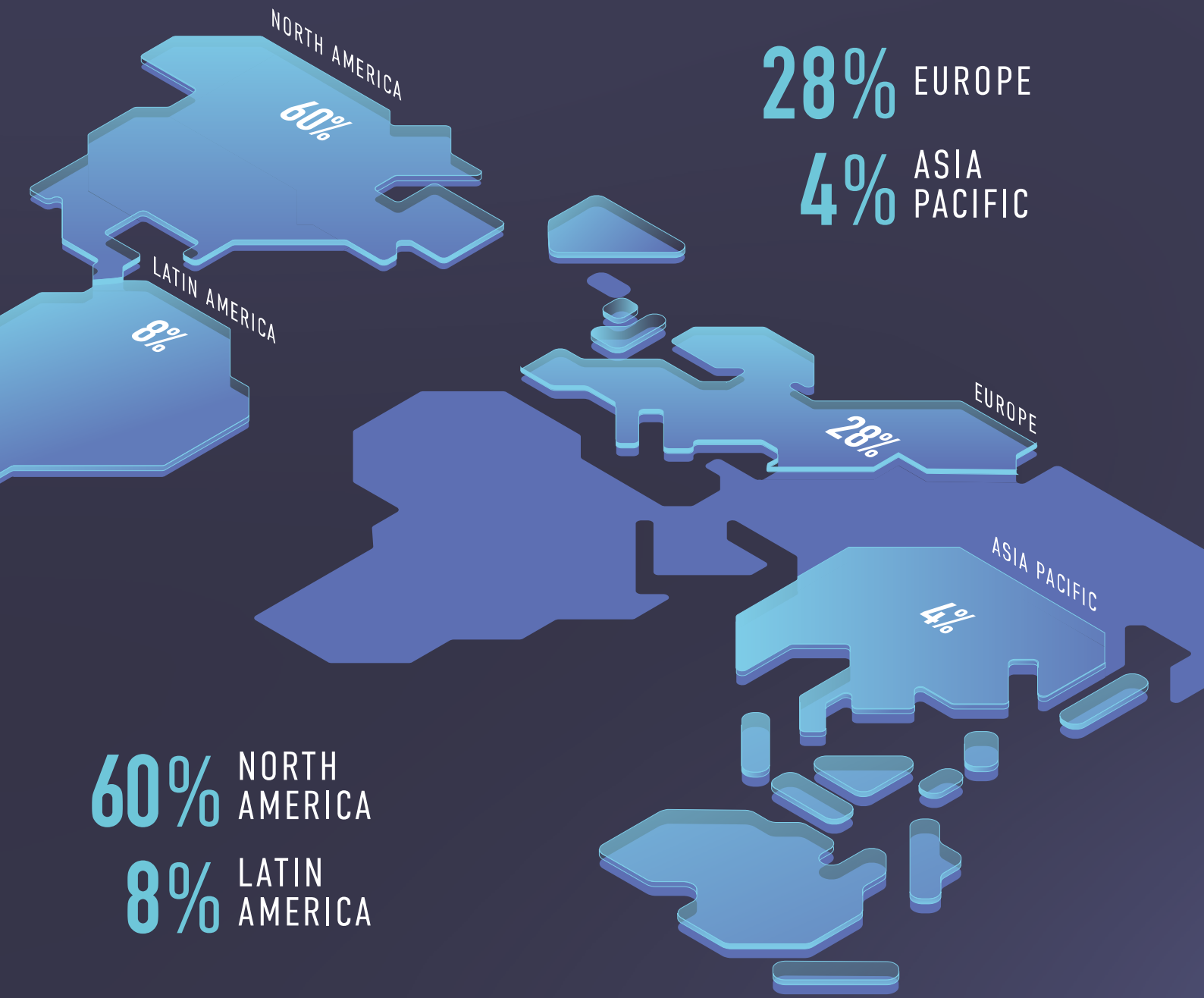
Active engagement with Tech Accord partners has informed Australia's engagement in two processes at the United Nations discussing responsible state behaviour in cyberspace (the Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG)). It is important to ensure that these discussions take into account the views and suggestions of the multi-stakeholder community, including industry. Thanks to Tech Accord for facilitating this thoughtful engagement

Johanna Weaver
Head of Australian Delegation to OEWG and GGE, Special Adviser to Australian Ambassador for Cyber Affairs

Stable and peaceful cyberspace can only be achieved and maintained through a meaningful and coordinated effort of all actors involved. The Cybersecurity Tech Accord demonstrates the value that industry-led initiatives can add to the operationalization of international cybersecurity norms, providing a baseline for its signatories that aims at achieving the best available solution and prevents the 'race to the bottom'. We are particularly grateful to the Cybersecurity Tech Accord for how it has supported UNIDIR's research on cyber by facilitating the engagement and dialogue between the research community and industry that is key to understand and address complex issues such as vulnerability identification and management, and supply chain security

Dr Giacomo Persi Paoli
Programme Lead for Security and Technology at the United Nations Institute for Disarmament Research (UNIDIR)

2019 BY THE NUMBERS



28% EUROPE

4% ASIA PACIFIC

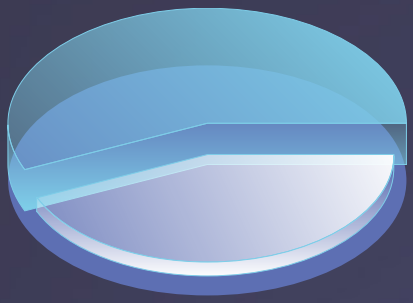
60% NORTH AMERICA

8% LATIN AMERICA

14 INITIATIVES SUPPORTED

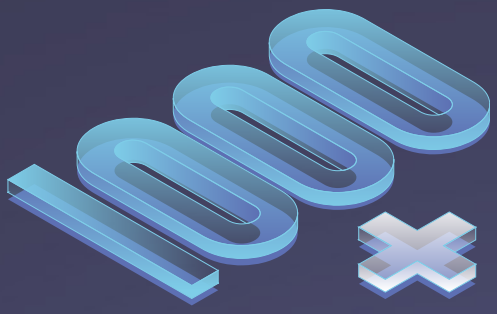
7 EVENTS ORGANIZED

5 CONSULTATION RESPONSES PROVIDED



54%

of signatory companies with vulnerability disclosure policies in place



1000+

registrants for capacity-building webinars and in person events

ELECTRICAL EQUIPMENT | CLOUD-BASED SERVICES | CYBERSECURITY SERVICES
SEMICONDUCTORS | TELECOMMUNICATIONS | INFRASTRUCTURE PROVIDERS
SOCIAL MEDIA | SOFTWARE DEVELOPERS | HOSTING SERVICES | BUSINESS CONSULTING
AUTHENTIFICATION SERVICES | HARDWARE MANUFACTURERS | ARTIFICIAL INTELLIGENCE
INFORMATION SECURITY & TECHNOLOGY | ONLINE MARKETPLACES | AUDIOVISUAL
DATA MANAGEMENT | ELECTRICAL EQUIPMENT | CLOUD-BASED SERVICES
CYBERSECURITY SERVICES | SEMICONDUCTORS | TELECOMMUNICATIONS
INFRASTRUCTURE PROVIDERS | SOCIAL MEDIA | SOFTWARE DEVELOPERS | HOSTING SERVICES
BUSINESS CONSULTING | AUTHENTIFICATION SERVICES | HARDWARE MANUFACTURERS
ARTIFICIAL INTELLIGENCE | INFORMATION SECURITY & TECHNOLOGY | ONLINE MARKETPLACES
AUDIOVISUAL | DATA MANAGEMENT

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