Cybersecurity Tech Accord Submission to the Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime

January 2024

The Cybersecurity Tech Accord, representing over 170 cybersecurity companies on the frontlines of global efforts to counter cybercrime, is grateful for the opportunity to contribute to the UN cybercrime treaty negotiations. Leveraging the direct experience of our member companies, Tech Accord submitted detailed input throughout this process to assist states in developing an added value Convention by significantly addressing the rapidly growing menace of cybercrime.

The zero draft released ahead of the sixth negotiating session was described by the Tech Accord, the rest of the private sector, and civil society organizations as quite simply **not fit for purpose without extensive modification**. The Tech Accord provided multiple practical options for how that draft's many problems could be resolved. Unfortunately, our recommendations, which were remarkably aligned with the advice of the multistakeholder community – consisting of cybercrime experts, data protections specialists, cybersecurity professionals, and human rights lawyers – were largely ignored. In short, **the revised draft for the seventh and concluding negotiating session not only fails to address existing serious issues, but it has also made them significantly worse.** Among its many new flaws, the latest draft would:

- **Open the door for extraterritorial data exfiltration and real-time surveillance in secret and without safeguards:** Changes would allow any two states to secretly compel a service provider *"located or established"* therein to provide personal information stored in or of individuals domiciled in third states, compromising national security and international human rights obligations. Neither the targeted individual nor the third state would have knowledge of what data was exfiltrated or have any opportunity to appeal such disclosure.
- **Substantially increase conflict of laws:** Removal of key provisions limiting the treaty's scope to a few well-defined cyber-dependent crimes means that its intrusive surveillance and data access powers can be applied to any activity that leverages digital technology. This will lead to severe conflicts of laws problems – made worse by the new extraterritorial data access provisions – and data requests for prosecution of legitimate online activities, compelling service providers to break the law in one jurisdiction to comply with data access requests from another jurisdiction.
- **Weaken protections for cybercrime victims and witnesses:** The already weak provisions on witness and victim protection have been further watered down and made optional, leaving individuals with no recourse to seek protection and return of proceeds of cybercrime, particularly in countries where no domestic protections or guarantees to this effect exists.
- **Risk criminalization of a wide range of legitimate online activities:** The expansive scope of several criminalization articles, including those on fraud and child sexual abuse would subject many legitimate online activities to criminal prosecution. This would result in serious human rights violations, including the prosecution of children and broad liability of service providers for communications they cannot reasonably be expected to intercept and analyze for content infringement.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

The previous draft's problems included an unclear and overly broad scope, vague criminalization provisions, missing protections for cybersecurity researchers, unnecessarily expansive data access provisions, and intrusive surveillance powers with no meaningful safeguards to protect individuals and victims of cybercrime from arbitrary abuse of executive authority. As a result, **the latest draft reads more like a UN digital surveillance treaty than a targeted instrument to fight cybercrime.**

The Tech Accord is particularly concerned that after nearly three years of negotiations, and with only one negotiating session remaining, states have yet to reach consensus on some of the most fundamental issues. These include the definition of cybercrime and – very concerningly – the *purpose* and *scope* of the Convention itself. Failure to agree that cybercrime – and not the misuse of technology in general – is the objective of this treaty would inevitably create legal uncertainty and encourage abuse of its provisions. A misuse of this treaty will be a near certainty by governments that have a track-record of disregarding privacy in the digital space, engaging in state sponsored malicious criminal activity, or providing safe havens for cybercriminals. These abuses will undermine trust and fragment international law enforcement cooperation. For all these reasons **the Convention as currently drafted will ultimately make fighting cybercrime harder, not easier.**

We also fundamentally disagree with the notion that selectively copying and pasting provisions from other crime treaties, particularly the Budapest Convention, will produce a similar or even coherent result. The Budapest Convention was adopted amongst like-minded countries with a 60-page Explanatory Report, rule of law checks and balances, and a review mechanism which empowers its Secretariat to assess state parties' compliance. This Convention currently has neither, leaving the door wide open for abuse.

If adopted without the major changes we recommend below – changes we have advocated for throughout the negotiation process, and which are remarkably aligned with the positions of other industry and civil society stakeholders – the proposed draft is simply not fit for its intended purpose. It would harm, rather than foster, international cooperation on cybercrime prevention and prosecution, significantly weaken cybersecurity, erode data privacy, threaten national security of states, and undermine online rights and freedoms globally. It is the responsibility of industry stakeholders — those that often act as first responders in the event of cyber breaches and who find themselves at the frontlines of the global fight against cybercrime — to reiterate once again that such an outcome would benefit no one. **We could not recommend any state to sign or ratify a Convention with such profound negative impacts on the digital ecosystem.**

The Anticipated Negative Impacts of the Revised Draft Convention

What follows is a non-exhaustive summary of the most significant negative impacts this draft convention would have on global efforts to address cybercrime and the wider digital ecosystem. Each section also summarizes the minimum necessary changes needed to produce a fit-for-purpose instrument. **We want to be clear: addressing one or two of the issues below will not produce a Convention that is tenable for the private sector: *all* these problems must be addressed – as we have repeatedly urged.**

A full list of Tech Accord proposals with concrete text suggestions provided for the sixth session draft is available on the Ad Hoc Committee website. We stand ready to engage with interested delegations on any of those proposals.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

1. **The Convention will weaken global cybersecurity by compromising critical security measures and criminalizing practices that keep the digital ecosystem secure.**

The Tech Accord has consistently called on negotiators to ensure that the Convention does not undermine industry's ability to deliver cutting-edge cybersecurity to our clients. Today, cybersecurity solutions include sophisticated and closely guarded access control measures as well as 'ethical hacking' - a process whereby vulnerabilities are detected and reported directly to vendors for fixing. Such 'hacking' may involve authorized *or unauthorized access* to a computer system. These innovative cybersecurity practices represent a critical line of defense against constantly evolving cybercrime threats. In recognition of their growing importance, some states have recently legalized ethical hacking through dedicated legislation or prosecutorial guidance. **The current Convention must keep up with the times by building upon – rather than merely parroting – the 2003 Budapest Convention on Cybercrime and explicitly exempt individuals engaged in lawful cybersecurity from its scope.**

Despite our repeated warnings, the **draft Convention threatens to undermine cybersecurity in many ways.** For example, its outdated provisions criminalize *any unauthorized access* to a computer system. This will inevitably lead to prosecution of good faith cybersecurity researchers, particularly in jurisdictions that have in recent years aggressively targeted cybersecurity practitioners. Additionally, Article 28(4) is gravely concerning from a cybersecurity perspective. It allows any state – including states who have conducted cyberattacks against critical infrastructure – to compel a company or government agency employee with special knowledge of a computer system to hand over access credentials and encryption keys from vital systems to third states, all in secret. **A UN treaty that undermines cybersecurity for everyone, makes cybercriminals' jobs easier, and compromises online trust and safety, is unacceptable**.

Minimum Necessary Changes:

- Add a 'criminal intent' (*mens rea*) requirement to all relevant articles in the criminalization Chapter (i.e. Articles 6(1), 6(2), 7(1), 7(2), 9(1), 10(1), 11(2), 12(b).
- Exempt good-faith cybersecurity research from the scope of the Convention (including in Articles 3 and 35).
- Delete paragraph 4 of Article 28.
- Add El Salvador's text proposal (Article 53.3(k) *quinquies*) to promote an enabling environment for good-faith cybersecurity research in Chapter VI.

2. **The Convention will slow down cybercrime law enforcement response by preventing expedited sharing of electronic evidence (e-evidence) to prosecute cybercriminals.**

The Tech Accord has repeatedly stressed the need for strict dual criminality requirements to facilitate cooperation under the Convention. State parties need to **provide clarity to data custodians as to what constitutes an act of cybercrime and where to seek data from** to facilitate expeditious sharing of e-evidence. Without dual criminality, data custodians may be forced to comply with a data request from one jurisdiction while having to break the law in another jurisdiction. Data may also be sought from a service provider (such as a cloud service) who may have no means to locate and produce the evidence in question as opposed to the data's most proximate source or rights holder. To protect themselves from liability, service providers will have to use every legal avenue available to challenge many data requests in courts – which the draft Convention does not allow for. This outcome will benefit no one except cybercriminals and will only serve to frustrate cooperation and slow down exchange of electronic evidence.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

Unfortunately, the current draft Convention (Article 35.2 in particular) still does not establish explicit dual criminality requirements. In fact, **by removing language scoping the treaty's provisions to precisely defined crimes in Articles 6 to 16, the draft creates even greater uncertainty**. It also provides no clarity on where to direct data requests to ensure expedited disclosure. To facilitate data exchange under this treaty, offences should exist within the same or similar category of a crime, be punishable by a deprivation of liberty of at least four years and be defined in this Convention. Furthermore, to streamline requests for e-evidence, data should be sought from 'data custodians' - i.e. the data's most proximate source and rights holder. In many cases, this will not be the cloud or ICT service providers, who, unlike telecom service providers, often do not have a direct provider-customer relationship with natural persons that use services cloud providers merely host.

Minimum Necessary Changes:

- Add a strict dual criminality requirement in Article 35.2 as well as in Articles 40.21 and 42.4.
- Add Costa Rica's proposal in 40.21(c bis) allowing refusal of mutual legal assistance for political offences.
- Reintroduce scoping provisions referring to crimes in "*Articles 6 to 16*" in all relevant provisions.
- Clarify that data requests should go to the entity which controls the collection, holding, processing or access to personal information being requested.

3. <u>The Convention will generate conflict of laws problems leading to sovereignty violations, reduced trust, and fragmented international efforts to fight cybercrime.</u>

The Tech Accord has consistently warned that the mere **availability of ICT products or services in any given country cannot serve as the sole basis to establish jurisdiction over an offence, data, or individuals located elsewhere.** Given the lack of clarity on which crimes are covered by this Convention, the current text would allow any state – or multiple states simultaneously – to exercise jurisdiction in relation to virtually any online activity. As a result, any state could compel a service provider who has no legal nexus therein to undertake real-time digital surveillance on any individual, simply because a product or a service was accessed from within that state's territory. That would conflict with existing data protection and localization laws in many countries. It would also amount to a violation of state sovereignty and territorial integrity under the UN Charter. Severe conflict of laws and jurisdictional disputes would arise as a result, reducing trust among states, creating confusion for service providers, and fragmenting international efforts to counter cybercrime. Again, this will not help countries looking for the Convention to help them combat cybercrime. In this context, the industry has proposed several safeguards to expedite e-evidence sharing and address conflict of laws that in our experience frequently hinders international cooperation in this space.

Unfortunately, **the draft text does not contain any meaningful safeguards to reduce conflicts of laws situations**. At minimum, third parties should have the right to challenge data requests on conflict of laws grounds and data custodians should be exempted from liability for good-faith acts undertaken in connection with this Convention. Furthermore, **the latest changes significantly increase the potential for conflict of laws and jurisdictional disputes. This concerns most notably the expanded extraterritorial access to data "*in the possession or control of a service provider located or established in a given State Party*"** (i.e. Articles 42.1, 44.1, and 45.1). This would require service providers to hand over data irrespective of where it is located and without the knowledge of the state it is in, causing severe conflicts of laws, compliance issues, and direct conflict with Article 4 of the Convention.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

Minimum Necessary Changes:

- Add new paragraph 18.5 to exempt data custodians and service providers from liability for good-faith acts undertaken in connection with this Convention to ensure that third parties do not face sanctions in one jurisdiction for complying with data requests in another.
- Delete the newly inserted language authorizing requests for any data "*in the possession or control of a service provider located or established in the territory of a given state"* in Articles 42.1, 44.1 and 45.1.
- Add new paragraph 22.7 to ensure that the mere accessibility of an online service in one country may not be used as the sole basis to establish jurisdiction over that service provider or of data located elsewhere.
- Add an operative safeguard in Article 22.2 to enable third parties to challenge data access requests if they create conflicts of law.

4. <u>The Convention will encourage intrusions of digital privacy worldwide by allowing states to compel service providers to provide personal information, including real-time surveillance, in secret, without adequate safeguards or accountability.</u>

The current text of the **Convention enables any government to obtain the personal information of citizens of other countries without robust, explicit jurisdictional limitations or sufficient procedural safeguards, in perpetual secrecy,** without any accountability obligations, forcing private sector data custodians to cooperate with no ability to object even where requests are manifestly unlawful. This is simply not consistent with the rule of law or the Charter of the United Nations.

The Tech Accord reiterates that except in narrow circumstances, the **public has a right to know how, when, and why governments seek access to their data**. This is especially important in a law enforcement context where surveillance does not always lead to indictment, and where many persons of interest to investigations are not charged with an offense. Secrecy should be the exception rather than the rule.

Without transparency safeguards to hold law enforcement authorities accountable, the treaty's **intrusive data access and real-time surveillance powers will invite abuse and encourage widespread intrusions of online privacy** and abuse of individuals' rights. It is critical that states explicitly provide that data custodians may notify individuals whose data is being accessed whenever that would not prejudice an ongoing investigation or prosecution. Otherwise, individuals will be unable to assert their fundamental rights, including the right to appeal and remedy. This transparency is even more important when dealing with electronic evidence, where search and seizure often leaves no physical trace. To further protect individuals from abuse of executive authority it is also essential to ensure that data custodians can challenge government data requests, particularly where disclosure could put individual lives at risk.

Minimum Necessary Changes:

- Add the right of data custodians to notify impacted individuals when doing so will not prejudice an ongoing investigation or prosecution and to publish the number of requests they receive from each state on an annual basis. This provision can be inserted either in Article 24 or 36.
- Add in Article 24 the right of data custodians to challenge government demands for data where conflict of laws concerns and principles of proportionality, legality, and necessity are at stake.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

- Add New Zealand's proposed safeguard for Article 35.2*quater* exempting parties from an obligation to cooperate on requests that could lead to prosecution of individuals on the account of protected characteristics.

5. The Convention will lead to human rights backsliding in the digital space and will put individuals at greater risk of being prosecuted for exercising their rights online.

The Tech Accord continues to strongly oppose a Convention that would apply to an undefined and virtually unlimited list of activities that leverage digital technology in their commission. A Convention that leaves it completely in the hands of individual states to define the breadth and type of subject matter that comes under its scope would be unprecedented. We continue to note with grave concern that many states continue to push for this outcome by proposing to extend this Convention to other offences without defining what those offences are.

Doing so would effectively override the applicability of existing international human rights online, paving the way to online censorship, preventive content take-downs, and government surveillance without guardrails. The treaty's intrusive surveillance powers and lack of adequate safeguards would further amplify these risks. We again call on states to use the limited time available to produce a targeted instrument focused on core cybercrime offences where international consensus already exists. That would be a major achievement for the international community. It would also serve as a powerful deterrent for cybercriminals who often operate from jurisdictions that do not have the adequate legislation or resources to address transboundary cybercrime alone.

Failure to agree that cybercrime – and not a further undefined misuse of technology – is the objective of the treaty will inevitably lead to human rights violations. Individuals, including political dissidents, human rights defenders, regime critics, and minorities will be at risk of being extraterritorially spied on in secret, extradited, and prosecuted for exercising their fundamental human rights. Such an Orwellian outcome – made possible by a UN legal instrument – would have dire and long-lasting negative consequences.

Minimum Necessary Changes:

- Amend Article 3 to ensure the Convention applies only to offences established in accordance with articles 6 to 16 of this Convention.
- Add Canada's proposed safeguard in Article 3.3 to align the scope of the Convention with broader international obligations of UN member states.
- Amend Article 23 to limit the scope of procedural measures only to offences in articles 6 to 16.
- Amend Article 35 to limit the scope of international cooperation measures to Article 6 to 16 only (including by deleting references to other serious crimes, e-evidence gathering for any crime, and references to Article 17)
- Remove all references to "*the use of information and communications technologies for criminal purposes*" and un-bracket "*cybercrime*."

6. The draft Convention will undermine national security, including by threatening the unauthorized disclosure of sensitive data and classified information to third states.

The Tech Accord warns states in no uncertain terms that a treaty with practically limitless scope that allows for clandestine access to secured systems, extraterritorial exfiltration of data, secret real-time surveillance, and virtually

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

no safeguards will not just put individuals at risk. **A treaty containing such an unprecedented combination of powers will also present grave risks to the national security of states themselves**. Abuse of key provisions could lead to real-time surveillance being ordered on a travelling state official whose devices could contain sensitive or even classified information. Importantly, this would occur without the knowledge of the impacted state. Disclosure or real-time surveillance concerning traffic data of third-state nationals, such as an individual's location, could place government employees at risk. A forced disclosure of technical access control measures of secured systems by an IT professional employed by one state while travelling in a third state, made possible by Article 28(4), could open critical infrastructure of another state to cyberattacks or exfiltration of state secrets.

Alarmingly, the current draft leaves the door wide open for these abuses. It is critical that states reconsider secrecy and safeguards provisions. The **bar of transparency must be raised to protect both individuals and national security.** Apart from safeguards proposed elsewhere in this document, states must notify third states whenever e-evidence is requested on residents or data is located therein. Furthermore, states should delete the most intrusive provisions, such as those on real-time surveillance and access to ICT systems, where even ex-post facto notification alone cannot mitigate national security risks. In this context, we once again reiterate the importance of directing data requests to the data custodian (i.e. government agency for data requests concerning the content of email communications of state officials) rather than a service provider that hosts that government data (i.e. cloud provider merely hosting a government agency's services who is in no position to resist or disclose the request or assert protected communications privilege).

Minimum Necessary Changes:

- Delete Articles 29 and 30 on real-time surveillance and all related references as well as paragraph 4 of Article 28.
- Introduce an additional provision in Article 35 to require at least advance notification of a third-state party whenever data is requested on a person domiciled, or data located, in its territory.

The Way Forward

There is still time for states to negotiate a favorable outcome – but a fundamental change of course is needed. Given the many outstanding issues, we recommend that **states agree to a streamlined framework Convention at the seventh session, with robust provisions for protocols to be negotiated at a later stage**. This approach would allow states to score a major political victory now and make progress on other issues through subsequent negotiations based on the UNTOC precedent, which has proven successful.

The streamlined Convention should be limited to the following:

- Its scope and all cooperation and powers should be limited to articles 6-16 only.
- It should address cybercrime, rather than the various broader concepts that have been proposed related to ICTs more broadly.
- It should include provisions which are proven to facilitate trust between parties and accelerate cooperation between states and service providers to ensure cooperation is fostered rather than hindered, as we have recommended consistently throughout this process as well as in this submission.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com

- Provisions should ensure that states cannot demand access to data in third states without the third state's explicit consent.
- It should leave out provisions which are clearly and readily subject to abuse and conflicts of laws problems such as real-time interception and production of content and traffic data.
- It should specifically rule out cooperation of any kind where dual criminality does not exist.
- The proposal of Canada for Article 3 should be included, and the international cooperation and procedural measures and law enforcement chapters should be amended so it is explicitly clear those chapters' provisions do not apply to any offence related to the conditions in the Canadian proposal and neither states parties nor service providers shall cooperate in relation to them.

We understand that many states want to see other provisions and broader coverage and would be disappointed by a streamlined Convention. We have heard from many developing countries that they do not receive adequate international cooperation on major cybercrime offences and are looking for this Convention to address that problem. The outcome of this negotiation should prioritize the needs of those states and leave it to subsequent protocols to build international consensus around other issues.

We welcome further engagement with delegates on the issues raised above and stand ready to provide additional feedback and clarification as needed.

Contact: Nick Ashton-Hart, Head of Tech Accord Delegation, at nashtonhart@apcoworldwide.com