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

July 2024

The Cybersecurity Tech Accord, representing over 150 cybersecurity companies on the frontlines of global efforts to counter cybercrime, is grateful for the opportunity to once again contribute to the UN cybercrime treaty negotiations. Leveraging the direct experience of our member companies, Tech Accord has submitted detailed input to assist states in developing an added value Convention by significantly addressing the rapidly growing menace of cybercrime. **This document supplements our submission of January 2024 for the Concluding Session on the AHC website.** In this submission, we focus on issues related to the current draft supplemental to the previous statement, which continues to be relevant *mutatis mutandis*.

We welcome that the Canadian, New Zealand, and UK safeguard proposals have been included in the new draft, which we strongly support. We see these proposals as vitally important, along with the data protection article.

However, even if these, and all other safeguard provisions, were adopted the fact that state parties may choose to cooperate using the powers of the Convention and keep it secret in perpetuity dramatically undermines their value. It is not credible to believe that states who choose to operate in perpetual secrecy would feel bound to abide by any limitation the Convention contains. As we have stated consistently, we do not believe such secrecy is compatible with the rule of law or that a 21st century international agreement bearing the UN's name should allow for it.

Eight articles of the draft treaty require keeping aspects of cooperation 'confidential' even when this is no longer necessary for an investigation or prosecution. To make matters worse, while states are free to implement procedural law protections (such as those in Article 24.2) none would be obligated to do so.

It is important to recall that many individuals whose information is transferred will be persons of interest who are never charged with an offence. The Convention does not provide any mechanism for these innocent people or anyone else to ever know if governments have requested – and gained access to – their information, rendering them unable to defend their rights.

In its present form, the Convention will result in more individuals' private information being shared with more governments around the world, with no requirement that state parties allow legal challenges to problematic requests and without any transparency or accountability mechanisms.

The text still fails to protect cybersecurity researchers and penetration testers. While the language in Article 53(3)(e) is welcome, it is does not protect these professionals from criminal liability. This requires changes to the criminalization chapter, as we have consistently recommended in detail.

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

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

importance, some states have recently legalized ethical hacking through dedicated legislation or prosecutorial guidance.

Failure to protect such activities from attracting criminal liability will have a chilling effect on the work of these professionals, as a letter from the global security research community to AHC delegates in February made clear. A treaty that intends to reduce the instances of cybercrime should ensure that its provisions do not, either directly or indirectly, facilitate systems being less secure from criminals. Last but not least, the issues with the intent in the criminalization articles could also allow the activities of journalists, their sources and whistleblowers to be criminalized.

We call upon negotiators to address these critical issues by changing "may" to "shall" in Articles 7(2) and 8(2).

We are deeply troubled by the current state of the articles on Child Sexual Abuse Materials. As just one example of their problems, the wording of Article 14.4(a) allows for the criminalization of children for taking naked or sexually suggestive selfies (often referred to as 'sexting') due to the drafting of definitions in Article 14.2. Many delegations during the last session emphasized that the criminalization of children in this way is not consistent with the UN Convention on the Rights of the Child. At a minimum the phrase "may take steps to" in the chapeau of Article 14.4 should be replaced with "shall". **The adoption of provisions that facilitate the criminalization of children in articles which are supposed to protect them from harm should be unacceptable to everyone.**

The text still contains provisions that could be used to harm the national security of states as well as presenting serious risks to corporate IT systems relied upon by billions of people every day.

Article 28.4 allows law enforcement to force individuals to provide access to secure systems, turn over access credentials and otherwise compromise corporate or even government systems and networks and provide the details to law enforcement, even if they are simply travelling on holiday in a third country. This can all take place without the knowledge of affected states or individuals' employers. While this provision draws heavily from the Budapest Convention's Article 19.4, the scope of application has been significantly expanded by applying it to Article 28.3 (Article 19.3 in Budapest), covering the seizure of systems, copying of data or making data inaccessible. The Electronic Frontier Foundation explores the problems with this provision in its article of 14th June. Given the level of secrecy that this Convention allows this article creates such serious risks that we, and the stakeholder community very broadly, have consistently advocated for it to be deleted.

We recognize that the latest draft has made the articles on real-time interception of individuals' content and traffic metadata optional. This does not solve the problems with those articles. While we appreciate this attempt to resolve the impasse amongst the negotiators, our position throughout this negotiation is that making these articles optional does not solve the fundamental issues and that they must be deleted. We refer you to a detailed discussion of this in our previous submission from January 2024, and **we provide two illustrations of how these three articles endanger national security when combined with the ability to keep all the use of the powers of the Convention secret in the annex below.**

Further issues around safeguards

We appreciate the Chair's efforts in the revised Article 24. Unfortunately it remains seriously flawed. We recognize that it was copied over from Budapest's Article 15 but the changes then made have dramatically reduced its value. Clause 1 dropped an adequacy obligation for human rights safeguards as a whole and doesn't recognize specific international human rights treaties as the benchmark to use when forming legislation – even of those instruments

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

that are universally applicable. The second clause, containing an obligation to implement procedural law safeguards fundamental to protecting human rights in a law enforcement context, has been significantly weakened by making it "subject to domestic legislation." It is welcome that the right of effective remedy was added to clause 1 – an improvement over the Budapest original. Given that the Convention allows all its powers to be used in complete secrecy, this right is compromised for the citizens of any state which chooses to use the powers in this way, since individuals need to know they have been harmed in order to seek a remedy. **Resolving these flaws in this article is vital and the Convention should not be adopted unless they are.**

We find it deeply troubling that Article 33 in the new Convention was adopted *ad referendum* at the last session with text inserted into the UNTOC original allowing states very considerable latitude to adopt the level of witness protection they choose, where in UNTOC all the article's provisions are mandatory. Without amendment this would signal that the international community has gone significantly backwards in a fundamental aspect of human rights in a criminal justice context in less than 25 years. **While we understand the reluctance to revisit provisions adopted *ad referendum* we believe this is an example, along with Article 28.4, where doing so is essential for a Convention that is fit for purpose.**

We cannot support the proposed title of the Convention as it conflates "cybercrime" with "Crimes Committed through the Use of an Information and Communications Technology System." We acknowledge that the proposal reflects an attempt at a political compromise but the title should reflect objective reality. The current title would mean, for example, that two persons using a modern mobile device to exchange text messages whilst planning the commission of the robbery of a physical store were engaged in cybercrime – which is not the case. As we have said previously, the title should refer to cybercrime alone and not broader constructions which create confusion on the purpose and nature of the agreement.

The scope of the Convention continues to be overly broad and should be narrowed to address the crimes in the criminalization chapter only. We acknowledge that the Chair is attempting to thread a needle between differences amongst the member-states on the scope of the Convention. We have consistently said that this Convention's provisions should apply only to the offences it contains. We understand the desire of member-states to collaborate on crimes outside of those in the criminalization chapter and highlight once again that the UNTOC provides for doing so. **Relatedly, we believe Article 4 should be deleted,** as it would extend the scope of the Convention far beyond cybercrime. Moreover it is vague, as it is not clear whether "United Nations" means any treaty for which the UN Secretary-General is the depositary that contains "criminal offences" or only agreements adopted by the UN itself with such provisions.

Article 60, as presently drafted, could be used to undermine other international criminal law conventions

Given that this convention is largely based upon copying and pasting of provisions from the Budapest Convention, UNTOC and the United Nations Convention against Corruption (UNCAC), the phrasing of Article 60 is particularly important to ensure that the modified, generally watered down, provisions in the new Convention cannot be used by states to effectively replace the provisions in the source instrument with the new Convention's edited versions.

Unfortunately Article 60.1 creates problems rather than clarity. It was copied from the Budapest Convention's Article 39.1, and then the second sentence deleted as below:

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

> *"If two or more States Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly.* ~~*However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles."*~~

Without that sentence the clause is much less clear on which provision applies between parties to both the new and older agreements. Article 60 has another modified copy/paste of Budapest Article 39, clause 2:

> *"Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party* ***under international law****."*

The bolded element was added to the Budapest language. This added phrase compounds the uncertainty of 60.1 because there are many interpretations of the definition of "international law." While it is generally accepted that universally applicable treaties like the UN Charter would be covered by that phrase, what about those to which many, or even most, member-states are a party? Does it include any treaty between any two states on the basis that any agreement a state makes should be honored? Various different scenarios could be argued – it should be unambiguously clear.

Article 30 of the Vienna Convention on the Law of Treaties (VCLT) regulates how to interpret "successive treaties relating to the same subject matter." Without explicit clarity that the new convention does not impact the meaning or interpretation of other international agreements Article 30.3 and 30.4 would apply. While international legal experts might argue that the new convention isn't a successor to UNTOC and UNCAC, that argument is difficult to sustain given Article 4 alters the application of offences criminalized in all "applicable United Nations conventions and protocols."

Article 60 must be amended to make clear that the Convention operates without prejudice to any other agreement. Otherwise, at the point where there are states parties to Budapest, UNTOC and UNCAC that are also parties to the new Convention, those states can unilaterally decide to apply the weaker provisions of the new Convention to the older instrument per VCLT Article 30.4(a).

Here are two specific examples of what is at stake. The first is Article 24, where the safeguards article of Budapest has been copied but substantially weakened as described previously in this submission. Similarly, Article 33 in the new Convention made the UNTOC original text substantially weaker, also as described above.

Were states to apply VCLT Article 30 with respect to just these two examples, key human rights provisions in the Budapest Convention could be undermined between a growing number of its parties. The same is true for witness protection vis-à-vis joint UNTOC parties. A comparison of all the copied and pasted provisions in the new Convention to their originals would need to be done to find all problems of this nature. Given Article 4 of the new convention, this situation could be argued to extend much further than these three instruments.

Fixing this problem is more complicated given that 60.2 has been adopted *ad referendum*. The simplest fix is to amend 60.1 so it contains a clear statement of non-prejudice to other agreements and delete the additional phrase

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

from 60.2 or to otherwise make clear what "international law" means. Given the chair has proposed interpretative notes to the Convention that is an avenue to consider in order to address this issue.

So, on the one hand previous treaties' provisions could be overridden by this Convention thereby reducing human rights and other safeguards, and on the other, the offences in those same treaties (if Article 4 is retained) could apply in more circumstances. This is very imbalanced and should not be an acceptable result for any member-state.

Proposed extension of the AHC to negotiate a protocol to the new Convention

We understand the interest of many states in negotiating protocols to the current Convention were it to be adopted. We find the notion of starting to do so immediately, as is proposed in the draft UNGA Resolution, premature at best. A protocol negotiation tagged to the end of the cybercrime AHC process is not the appropriate way to try to reach compromise on the scope of the convention itself. We believe that the fundamental issues of the convention should be resolved before any Protocol can be considered. Any Protocol should help address specific issues or challenges addressed in the convention and should not broaden the scope of the convention.

Were member-states to agree to embark upon this, Protocols should be negotiated using the same modalities that are in place for the main Convention as the text currently provides, however, any text that is agreed by that body should be adopted by the UN General Assembly, and not the Conference of the Parties of the Convention, given that the new Convention won't have entered into force.

Explanatory Notes are a welcome development

We know from the Budapest Convention process how valuable its Explanatory Report has proven to be in providing clarity to states on the nature of the obligations in that Convention. We welcome the Chair's proposal of explanatory notes. For these to be meaningful they would need to be adopted along with the Convention and on the basis that parties seeking to ratify the Convention should consider them as integral guidance in the ratification process. The notes create a useful opportunity to explain, for example, that acts that were committed 'without right' but which are in the public interest, such as security research, whistleblowing and the reporting of current events, should be considered as having taken place with right – just as the Budapest Convention's Explanatory Report does. While this is not a replacement for relevant amendments in the Criminalization Chapter, to continue this example, they would add significant value.

In closing we thank the Committee for its attention and stand ready to discuss these issues, and those in our previous statements, at delegations' convenience, for which purpose our representatives will participate in person at the Resumed Session.

Annex: Examples of national security and other risks from abuse of the powers of the Convention

1. Example One: how Articles 29 and 30 would allow a senior officials' data and movements to be disclosed without the knowledge of the official or the state to which he belongs.

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

- Country Y = the "requesting state"
- Country Z = the "requested state"
- Country X = the state of nationality of a senior government official of that state - who is the target of the request from Y.

Country Y (the "requesting state") wants access to the secure communications and stored data of a senior official (a senior civil servant or minister) of country X who is travelling in country Z (the "requested state"). Country Y invents the details of a fictional offence that the unnamed official is alleged to be connected with which was committed in country Y. Y becomes aware that the official will be visiting country Z, and asks law enforcement officials in country Z to provide access to his real-time location information (using article 29) as well as real time interception of his digital communications (under article 30) without of course identifying the person as a government official of another state. To help obscure that the access relates to a senior official, the request does not mention a name, only a specific telephone number or IMEI number of a mobile device. Country Y also doesn't disclose that the senior official is travelling in, but not a resident of, country Z. Country Z receives this request and instructs Z's service providers to provide the access requested as it is unaware it relates to a government official of a third state – or even of a person who is only visiting Z's territory.

Those service providers quickly realize that the person is not a resident of country Z because the IMEI number is not registered with a local provider, it is roaming, which would raise questions since the request doesn't explain this and does not provide a rationale for the request for data of a third state national. This scenario is why we have consistently urged that in such instances, unless a persuasive argument for access to a third state travelling person's data has not been made by the requesting state, the third state should be notified that one of its residents or nationals' data is the subject of a request. If the Convention provided for such notifications it would be considerably more difficult for states to abuse the Convention to gain access to other states' officials movements and their data.

Because the convention draft does not require states parties to allow service providers to object to any request, and because country Z's legal framework does not allow for such objections, that service provider is forced to provide the data or potentially face civil or even criminal sanctions.

2. Example Two: How misuse of Article 28.4 would facilitate access to the defence ministry systems of a member-state

- Country Y = the "requesting state"
- Country Z = the "requested state"
- Country X = the state of nationality of a senior travelling IT specialist under contract to the defence ministry who is the target of the request

In this situation, country Y wants to gain access to highly secure networks of the defence ministry of country X. Similar to the previous example it invents the details of an offence involving a senior IT technician of country X who

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

is a private contractor to country X's defence ministry. The details of the offence – which is not related to the technician's work - requires access by the authorities of country Y to the laptop of the technician, as country Y believes that laptop has supervisory access to the networks it wants to infiltrate. Y finds out that the technician is going on holiday in country Z. Y sends a request for the seizure of this person (under Article 28.4 of the draft Convention) and his or her laptop and mobile device and demands that the authorities force the technician to provide access credentials for the mobile device and laptop and for the devices to be provided to representatives of country Y, and for the person to be held until the devices can be searched by Y's representatives. Y's representatives use their access to gain access to defence ministry systems and open clandestine access to those networks for country Y before giving the devices back to the representatives of country Z.

This example could as easily allow for access to secure networks of the private sector as well. Such abusive access could allow firm-level access to otherwise secure networks to steal trade secrets or other confidential data of those service providers for other purposes or to compromise the financial system of entire countries if secure systems of systemically important financial institutions were compromised. Abuse of this article as described could also make critical infrastructure of states vulnerable to attacks from other states or malicious actors as well, if the person in question had access to secure networks of such infrastructure.

The third-state notification regime we have recommended above, and in our most recent previous submission, would greatly reduce the likelihood that this type of abusive request would be successful.

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