# Cybersecurity Tech Accord Submission to the Sixth Session of the Ad Hoc Committee to Elaborate a Comprehensive International *Convention* on Countering the Use of Information and Communications Technologies for Criminal Purposes

*August 2023*

## Introduction

The Cybersecurity Tech Accord welcomes the opportunity to provide input into the Sixth Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. As a non-ECOSOC accredited member of the multi-stakeholder community, we would like to thank the AHC for establishing such a robust and inclusive process for multi-stakeholder participation in its work.

Since 2018, our coalition of over 155 technology companies has served as the voice of the tech industry on matters of peace and security online. Our signatories include small and medium-sized technology and cybersecurity enterprises, as well as global technology companies, allowing us to coordinate a range of input from private sector organizations across the globe. We represent those in the industry that can uniquely speak to the challenges posed by cybercrime and to how technology is expected to evolve in the coming years and the implications for crime online.

The Cybersecurity Tech Accord and our Signatories have collectively been an engaged partner and stakeholder in the deliberations of the Committee, and we welcome the publication of the Zero Draft.

## Major Issues and Opportunities

We want to reinforce our support for elaborating a Convention that reduces the scope, scale, intensity, and impact of cybercrime globally. Industry is on the front lines of this fight and we have a material stake in the AHC delivering a Convention that is fit for purpose.

We also know from direct experience that a collaborative multi-stakeholder approach – sharing actionable information and leveraging the combined capabilities of the private sector and the government – yields the best opportunity to disrupt cybercrime quickly and at scale. Our proposals and statements are based on that experience.

We thank the Chair and her team and the Secretariat for the Zero Draft, which is a good basis on which to work.

This Convention has a unique opportunity to address the very real obstacles to effective cooperation that exist. If it does, it will have a significant positive impact on global cybercrime cooperation and we believe that opportunity must be seized. However, for that to happen will require significant changes throughout the text.

Our submission is based on foundational concepts of the Convention which can be summarized as follows, based upon the private sector's global experience in responding to cybercrime.

**If this Convention fails to address major cybercrime incidents – which continue to grow in their number, extent, severity and visibility – it will be seen as a failure.** We know that existing international capacity for transboundary criminal cooperation is constrained even in major developed economies, and many UN member states do not yet have cybercrime legislation at all. This Convention should therefore focus on globally harmonizing serious cyber offenses against the confidentiality, integrity, and availability of computer data and systems (cyber-dependent crimes). Examples of such crimes include access, interception, data and systems interference, and misuse of devices. These make up the bulk of global criminal offences in cyberspace and need to be addressed as a matter of urgency to counter the rapidly growing global cybercrime economy.

**If the Convention fails to protect the activities of security researchers and penetration testers, it risks enabling cybercriminals' activities.** By design, these security professionals are frequently working "without right" and "without authorization" and depending upon the drafting of statutes they could also be inadvertently caught up if the threshold is "unlawful." Creating legal jeopardy as this Convention currently risks would mean systems will be less secure and more vulnerable to cyber criminals: exactly the opposite of the objective of the Convention. Arguably the lack of a criminal intent standard could also criminalize whistleblowing and journalism, as receiving information from computer systems without authorization is an offence as these articles are written.

**The Convention must ensure that its jurisdictional elements do not undermine its effectiveness.** Negotiators should carefully consider the implications of a Convention that could encourage one state to assert jurisdiction over a globally available online service provider to force disclosure of data associated with a third country's nationals merely because the provider's services were available to users in both countries without a request for cooperation to the third country. The Convention should encourage state parties to adopt laws - with robust human rights and due process protections - that establish jurisdiction over service providers with legal presence in *their* jurisdiction but which recognize that international cooperation is required to obtain data where the criminal acts, persons of interest, and/or service provider(s) are located in *other* jurisdictions. We propose specific changes in relevant chapters to address this to help ensure requests for cooperation are acted upon more swiftly and are more likely to be granted.

**Development and capacity building are fundamental to the success of the Convention.** As we have stressed in previous meetings, the Convention cannot be successful unless it ensures that all states who become a party to it are able to implement all its provisions, leveraging best practices on a voluntary *and* demand-driven basis. It should recognize that we are not in that place today and embed specific provisions to help ensure a step-change in capacity to respond as the Convention is implemented. Given that even the largest economies have backlogs in processing existing crime cooperation requests, the issue of technical assistance and capacity building should be approached as a shared challenge, rather than a source of conflict between groups of states.

**The Convention needs a mechanism for implementation that ensures all parties relevant to addressing cybercrime are a part of the process.** It is an objective reality that effective cybercrime investigation, prosecution, and redress for victims is impossible without public-private sector collaboration: most of the data necessary for cybercrime investigation and prosecution comes from the private sector. This argues for a step-change in the involvement of non-governmental stakeholders in the mechanism for implementation of this Convention

compared to previous crime treaties.

## Preamble

The Preamble should contain a strong statement that a key objective of the Convention is to foster socioeconomic development through effective cybercrime prevention and prosecution and to assist developing countries, particularly developing countries, as they seek to leverage this Convention to foster sustainable development.

Increased and more specific references to other international legal obligations is essential. This is particularly important with respect to human rights, the protection of which must be an integral obligation of the Convention, not a principle or recommendation limited to the Preamble. Where there is an obligation to comply with other principles of international law, we recommend the specific instruments are referenced to avoid different member-states implementing the obligations based on different sources of law which could create confusion or allow some states to exclude the source that is most appropriate.

The Preamble should highlight the benefits of technology generally and that information and communication technologies (ICT) and the Internet are global goods with profound socioeconomic benefits and foundational to achieving the Sustainable Development Goals. The Convention could therefore be framed as protecting these many benefits for all citizens, while protecting potential victims of cybercrime[3].

***Specific Provisions:***

1. We recommend that the list of specific offences in the last part of PP3 be deleted. While those are all serious crimes, they aren't cybercrimes, and a technologically-neutral approach would also argue for their deletion.
2. We recommend that the language of A/HRC/38/L.10/Rev.1 in *considering* 1 be added to the end of PP11[1]. This was adopted by consensus and will give specific clarity to the underlying objectives of the para.
3. Add, to the end of PP9, "*to protect the legitimate interests of users of information and communications technologies*." The Convention should seek to accomplish these objectives, and it should say so explicitly.

## 1. General Provisions [Articles 1-5]

As we and so many others have often said, we believe the proper object of the treaty is countering "cybercrime" and not the use of "Information and communications technologies for criminal purposes." Cybercrime is more focused and well understood in international criminal law; the broader term could allow the Convention to apply to any object that has integrated circuits and we submit that such a broad term would undermine the Convention's effectiveness and open the door for very large numbers of requests for cooperation on minor offences. All articles should be modified accordingly, in this chapter Articles 1 and 3. Further,

[1] "…that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights."

the Convention should avoid provisions which override or supersede other instruments, due to the inherent risk of conflicts of laws and of degrading the operation of those instruments.

***Recommendations by Article***

**Article 2 Use of Terms**:

Terms should be used consistently throughout the Convention and should be specific - avoiding terms such as 'lawful' or 'dishonest' where the meaning can be very different in different jurisdictions (and in the case of both of those terms, not even denote criminal conduct). Definitions of data, data subjects, or other terms relevant to these should be well-established, technically accurate, and leverage existing definitions already widely adopted across the member-states.

1. **The Convention should use the terms "computer system and "computer data" rather than inventing new terms.** More than 120 countries already use these terms as defined in the Budapest Convention. Creating new terms will result in confusion as to the scope of the defined terms and the likelihood that different definitions for the same objects may frustrate international cooperation.
2. **The definition of serious crimes should incorporate the entire text of UNTOC Article 2(b).** The current wording leaves out the last phrase and this defines serious crimes confusingly as "a maximum … of at least four years." It should also make clear that it refers to conduct with criminal intent.
3. **A new concept, that of the "data custodian" should be defined and used wherever the Convention addresses third parties and data instead of service providers.** Data custodians include service providers who control the collection, processing, or access to personal information. Using this term will help to ensure that states can direct requests for such data to the most proximate source of the data, rather than, for example, the cloud services, whose platforms are used by data custodians but who are not in control of that data and do not generally have access or means to identify specific subsets of data – delaying data access requests significantly. For further discussion of this concept please see the "International Cooperation" section below.
4. **The definition of "content data" is worded such that it could be misunderstood as overlapping with traffic data**. It should be modified accordingly by, at least, replacing the phrase "relating to" in respect of a communication, as traffic data does relate to the contents of a communication.

**Article 3 Scope of application:**

A new provision should be added to ensure that the Convention's provisions shall not apply to acts conducted in good faith undertaken to reduce the potential for harmful interference with computer systems. This ensures that acts done for legitimate purposes - such as penetration testing and security research - do not fall within the scope of the Convention whether they are done with or without consent. The Convention should do more than avoid criminalizing these activities, it should promote their work by protecting it.

**Article 5 Respect for Human Rights:**

The article should contain references to specific human rights instruments, including ICCPR and UDHR, among others. The protection of human rights must be an integral obligation of the Convention.

## 2. Criminalization [Articles 6-21]

The focus of this Convention should be addressing cyber dependent crime - defined as offences which cannot be committed without ICTs - and those which are serious - for which conviction carries a mandatory period of incarceration. According to estimates the global cost of cybercrime is expected to rise from $8.44 trillion in 2022 to a staggering $23.84 trillion by 2027, an amount larger than the GDP of the world's largest economy[2]. This Convention should have a meaningful impact on reducing the incidences of, and impact of, serious cybercrime. Subsequent protocols to the Convention can address additional offences as required.

The Convention won't be effective if the private sector doesn't have a clear understanding of what constitutes an act of cybercrime to respond to government requests for electronic evidence. At the same time states parties will have to mutually recognize offences as both criminal and substantially the same offence to satisfy requirements for dual criminality. Moreover, states should recognize that their widely diverging political, cultural, and legal systems will frustrate a finding of dual criminality if offenses are worded vaguely.

Domestic laws covering cyber-enabled crimes as well as complexities of jurisdiction over such crimes vary widely. This means the Convention should only criminalize offences that are cyber-dependent, and should not expand the scope of procedural and international cooperation measures to crimes that are not clearly defined, merely because a computing device was involved at some point.

All offences should require *mens rea* - criminal intent - and not intent alone. Thresholds such as "without authorization," "without right," and "unlawful" allow prosecution of behavior which did not intend or result in harm and may not even be criminal. This is of fundamental importance as otherwise acts which are critical to societies will be at increased risk of prosecution.

Because of the current lack of criminal intent most of the articles in this section could be used to criminalize the work of penetration testers and/or security researchers, as by definition their work can involve intentional penetration of networks, accessing them, reviewing and retrieving information, and interfering with systems and devices. Their activities, by design, are frequently "without right" and "without authorization" and depending upon the drafting of statutes, their activities could also be inadvertently caught up if the threshold is simply "unlawful." Failure to protect these functions means that systems will be less secure and more vulnerable to cyber criminals: exactly the opposite of the objective of the Convention. Arguably the articles could also criminalize whistleblowing and journalism, as receiving information from computer systems without authorization is an offence as these articles are presently written.

All crimes included should be the subject of consensus, not adopted by vote. This is important to ensure that the Convention is ratified, and implemented, by as many states as possible; it also ensures that the definitions of included crimes will be transposed to domestic laws so that

[2] Estimates from Statista's Cybersecurity Outlook.

they lend themselves to international cooperation in enforcement. Acts which are not already subject to criminal penalties in, at a minimum, a substantial majority of member-states should not be included in the Convention.

***Recommendations by Article***

**Articles 6-12**

Throughout these articles, the phrase "with criminal intent" should replace "intentionally and without right" *mutatis mutandis*.

A provision should be added at the end of all articles which do not yet have it to allow State Parties to require that the conduct of the offence must result in serious harm for it to be the subject of coverage in the Convention for them.

**Article 11 Computer related forgery, Article 12 Computer related theft or fraud, and Article 16 Laundering of proceeds of crime**

Where there is consensus to include cyber-enabled crimes, these should be strictly limited to those acts where the use of ICTs dramatically increases the scale, scope, and speed of the offence. The Convention should not include offences just because ICTs were used in their commission; criminals communicating online about the commission of theft, fraud, extortion, or other kinetic crimes does not justify special treatment as cybercrimes. Therefore the articles on forgery (11), fraud and theft (12), and money laundering (16), should be removed.

**Article 17 Offences relating to other international treaties**

We believe this article should be deleted. We question the validity of modifying the effects of other treaties through this Convention.

**Article 18 Liability of Legal Persons**

As has been said by the private sector at previous sessions of the Committee we do not see a persuasive reason to include an article on liability of legal persons. If it is not deleted, it should at least include a provision, which was in the consolidated negotiating document (CND) for the Fourth Session, that ensures legal persons will not be liable for acts done in good faith, or in relation to acts done in furtherance of the Convention's objectives. This is particularly important to deal with conflicts of laws situations.

**Article 19 Participation and Attempt**

We believe this article should be deleted. It is extremely broad and likely to result in criminalizing conduct which had no intent or knowledge of criminality. This article shows, better than most, the weakness of relying upon intent rather than "criminal" intent: a person might act intentionally to aid someone who is committing a crime but not knowing that a crime was being committed.

**Article 20 Statute of limitations**

We believe this article can be deleted as there is no cybercrime-specific elements to the article, and it is a sovereign matter.

**Article 21 Prosecution, adjudication and sanctions**

For the reasons previously mentioned we recommend 21.1 require a threshold of serious crimes. We recommend adding a right of appeal to 21.4, after the right to a fair trial, for obvious human rights reasons as well as for pragmatic purposes: many states will not provide

data for international cooperation if they don't see that the judicial system of the requesting state incorporates internationally recognized fundamental rights and those of their own legal system.

## 3. Jurisdiction [Article 22]

We have consistently noted two things about jurisdiction and its scope:

1. The jurisdiction elements of the Convention must ensure that it provides clarity as to what jurisdiction applies, and the extent of its application – and extraterritorial application must be avoided). Not doing so will create serious conflicts of laws problems for data custodians, who will be asked to violate the law in one jurisdiction to follow it in another;
2. The Convention's provisions should only relate to the offences in the Convention, and not extend to other crimes.

When requests are made from one jurisdiction to another, those requests must not force any entity to violate the law in any jurisdiction in which they have legal nexus. If requests have that effect, it will either block cooperation or cause considerable delays. This is especially important for disclosing personal information, extradition, and any seizure of property.

During the AHC we have warned that merely offering services in a given state must not provide sufficient ground for that state to establish jurisdiction and request data on suspected crimes committed in other states, or that providers must provide data held in third states just because they have technical access to it. If Article 22 retains its current form, it will create a serious risk of data being requested directly from service providers via procedural and law enforcement powers (including real-time surveillance) that are currently in the draft. Not only does this raise serious human rights concerns but it could gravely undermine national security as the third state would not even know if data in its territory, or of its nationals, had been handed over to another state. This is made worse by the absence of rights for service providers to give notice to impacted individuals and states given the secrecy with which the Convention treats cooperation.

***Recommendations for Article 22***

- 22.(2) the chapeau should be deleted, and articles 22.2 (a), (c), and (d) should be deleted as all of these allow or could allow extraterritorial application of the laws of one State Party in the territory of another. Article 22.2(c) would then become 22.1(c).
- 22.5 should be rephrased to the Budapest Convention language ("determining the most appropriate jurisdiction for prosecution" rather than on "coordinating their actions") as this is much clearer on the outcome required.
- A new clause should be added to make clear that no State Party can exercise jurisdiction over a service provider or data custodian simply because individuals use that service in their territory, absent any other element of legal nexus.

## 4. Procedural Measures and Law Enforcement [Articles 23-34]

One of the most important – and risky - aspects of this Convention is in how digital evidence is gathered by public authorities gaining access to data necessary to combat such crimes.

It is important to recognize that access to data by governments for law enforcement purposes has significant risks to human rights, as well as data protection and fundamental privacy rights. We recommend that the Convention explicitly protect whistleblowers, journalists, victims and witnesses in this section, reiterating and building upon the relevant provisions of UNTOC, particularly Articles 24 and 25. The draft in its current state, regrettably, creates the potential for extensive access to personal data, with secrecy of all requests by default, and extremely limited provisions for proportionality, necessity and legality that can very often be overridden by domestic law.

With respect to data access data the convention should embed principles of proportionality and necessity regarding data collection and retention provisions to ensure they do not (a) ignore the particularly intrusive nature of real-time surveillance if the articles relevant to real-time access and interception are not removed; and (b) represent a significant expansion of terms used in current mutual legal assistance treaties (MLATs). The Convention should also create a right of refusal to cooperate – particularly when the protection of human rights or national security might be at stake - and it should recognize that not all types of access are technically possible for all types of information or in all jurisdictions.

The Convention should provide for custodial requirements on states transmitting, or holding, personal data in compliance with domestic and international legal obligations particularly where it relates to natural persons who are neither nationals nor legally resident in the territory of the state that holds their information. While this introduces complexity, it is of fundamental importance to ensuring effective cooperation. Systematic failure by a party to effectively protect personal data that it has requested over time should be grounds for refusal of future requests as well.

The Convention should avoid establishing conflicting rules that raise barriers for international criminal cooperation, and explicitly recognize that conflicts of law will arise. Data flows are global, yet national rules vary considerably and are not always compatible across jurisdictions. Because compliance costs from conflicting rules are enormous and growing, governments should ensure that provisions reduce the risk of conflict. The private sector already deals with situations where one country's laws can create significant conflict when responding to lawful demands around the world. The Convention needs to recognize this explicitly and ensure that a request can be denied on such grounds, referring the requesting state to the jurisdiction where the legal problem has arisen and recognizing that third parties cannot be required to break the law in one jurisdiction to fulfil data access requests in another.

Additionally, we recommend that to expedite requests for data, governments should target their request at the most proximate source of the data – i.e. "data custodians" instead of "service providers." This recognizes a reality that data protection legislation is increasingly robust and a part of the legal systems of most member-states, none of which was true when the most recent international conventions on crime, or cybercrime, were developed – in fact this was a significant part of the negotiations of the Second Additional Protocol of the Budapest Convention.

It is essential that the Convention expedites data requests and addresses how states deal with conflicts of laws issues between themselves, instead of expecting data custodians to navigate the increasingly complex legal environment as is the case now. It must also recognize another

important reality: many states will not provide personal information to other states for law enforcement purposes unless the Convention provides assurances that the requesting and requested state's legal systems embody similar procedural safeguards to ensure that there is basic compatibility between legal systems and fundamental elements of international human rights law. Simply put: safeguards in the Convention will facilitate international cooperation on cybercrime, rather than frustrating it, to the benefit of all states.

There are also many instances where specific provisions defer to domestic legislation which will result in a very complex legal landscape for practitioners, almost certainly raising barriers to effective cooperation. We strongly recommend that negotiators use this legal convenience only when absolutely necessary.

Given the absence of robust safeguard provisions, the jurisdictional issues we have identified, the provisions extending the scope of these measures to all crimes, the requirement of secrecy by default for all requests for data, and the other issues we raise around necessity, proportionality, and legality we cannot support inclusion of provisions on real-time access to, or interception of, content and traffic data.

There are enormous practical obstacles to the use of these powers, which amount to real-time surveillance of individuals globally. For a request to use these powers to work lawfully across global jurisdictions simultaneously will alone create obstacles to effective collaboration of other kinds which is likely to be more effective. Conflicts of laws will certainly arise as a result, delaying or frustrating requests entirely. Last, but certainly not least, it is profoundly difficult to use surveillance powers globally without undermining internationally recognized human rights protections especially given that all of these powers are to be used in secret.

***Recommendations by Article***

**Article 23 Scope of procedural measures**

Article 23.2(b) should be deleted, and (c) should be limited to offences set forth in this Convention only.

**Article 24 Conditions and safeguards**:

In 24.1, necessity and legality should be added at the end of the sentence.

In 24.2 provisions should be added to:

- Facilitate third parties in challenging requests made by a state in relation to the powers and procedures of this Convention on the basis of legality, proportionality, or necessity, such challenges to be adjudicated by an organ of the State Party independent of the requesting agency;
- Allow third parties to initiate an independent review of data requests in relation to the immediately-previous point, also independent of the organ of the State responsible for adjudicating the decision;
- Allow third parties who are data custodians to disclose to the legal or natural persons the data, including traffic data, directly related to them that has been disclosed to a State Party, provided that doing so does not prejudice an ongoing investigation or prosecution;
- Ensure that states address requests for data to the data custodian of the data who is the proximate source and rights holder. This is consistent with the Trusted Cloud Principles and represents international best practices that are critical to maintain trust

in global data flows. This is also essential for expeditious replies to requests, as addressing requests to another entity will not be successful due to conflict of laws issues, or because they do not have means to locate the data, or both.

In Article 24.3: a provision should be added to the end to ensure that liability does not arise for third parties that do not act as requested or required by a State Party in relation to the powers and procedures in the Convention where doing so would require the third party or parties to act unlawfully in the jurisdiction of another State.

A new provision should be added to ensure that the data, including traffic data, of persons who are subject to the jurisdiction of another State Party or territory, which is acquired by a State Party through the powers and procedures of this Convention, are protected from modification or disclosure to unauthorized persons. Any such data should be expeditiously deleted when it is no longer required for an ongoing investigation or prosecution. The data should also not be used for any other purpose than that for which it was originally requested.

Last, but not least, a provision should be added to ensure that no obligation to cooperate exists if the requested party has reason to believe that the requesting state wants to prosecute or punish a natural person on the grounds of internationally protected characteristics like gender, race, language, sexual orientation, membership of a social group, or for their political beliefs, or that they would be tortured or subject to inhuman or degrading conditions by the requesting state.

**Article 25 Expedited preservation of stored computer data**

25.1 - the phrase "or similarly obtain" should be deleted as this article relates to preservation of data, not to disclosure of that data.

25.2 - the article should be modified such that data may be held for up to 90 days, renewable for a total of one year with relevant changes replacing "as long as is necessary".

25.3 – the last phrase should be deleted, as it will create an unharmonized legal landscape and indefinite retention would also create conflicts of laws problems in many states.

**Article 26 Expedited preservation and partial disclosure of traffic data**

1(a) should be amended to make clear that the provision is subject to technical feasibility and domestic legislation. The provision should be amended to allow for preservation for up to 90 days, renewable for a total of one year.

**Article 27 Production order**

27.1 should include a qualification that it is subject to a reasonable belief the offence committed is set forth in this Convention and where jurisdiction can reasonably be claimed over it.

27.2 should make clear that users can be notified of requests for their information by default except where doing so would prejudice an ongoing investigation or prosecution.

27.3 should make clear that:

- If a State Party wants information, or a request for it, to be secret it must make the case for doing so to an independent authority;
- A nondisclosure order should not be of unlimited duration, and;

- That the decisions made should be subject to challenge by the data custodian in question.

**Articles 29 and 30 should be deleted** as well as all references to them in other provisions for the reasons previously mentioned.

**Article 31 Search and seizure of stored computer data**

31.2, 31.3 and 31.4 should contain a qualification that the measures must be subject to States Parties' obligations under international human rights law and principles of legality, necessity and proportionality.

## 5. International Cooperation [Art. 35-52]

As previously noted, we strongly believe that the key to success for this Convention is to focus on major crimes, leveraging best practices in international cooperation in practical application. The rules in this chapter should ensure they solve the practical obstacles we already face today and do not create new obstacles or cause negative consequences in the future.

The scope of application of the chapter on International Cooperation should be limited to the offences defined in Articles 6 to 16 of the Convention. This is particularly important given there are objections to basic provisions for safeguards and that, overall, the safeguards elements are so limited that what is missing will hinder international cooperation rather than facilitate it. There is no value in increasing the scope of application of processes which will make cooperation more difficult.

Dual criminality is a key prerequisite for international cooperation and the Convention should make it a basic requirement. State Parties, as well as data custodians, must have a shared understanding of what constitutes a cybercrime across jurisdictions to be able to respond appropriately to government requests for information. Without such harmonization, conflicts of law will arise, frustrating effective cooperation and timely information-sharing.

Principles of legality, proportionality, necessity, and transparency should be better reflected throughout the chapter. There are many provisions which could be improved to better reflect these principles. As we have noted previously many states will refuse requests for access to data, especially data related to their own nationals, if they don't believe that the requesting state has sufficiently robust protections for human rights in place. This Convention will not change this. Ensuring that the Convention embodies the minimum protections that would allow all states to provide access to the data necessary for effective international cybercrime cooperation is therefore not just important, it is fundamental to whether this Convention will be successful.

We believe that all states have an interest in increasing transparency and restricting the use of data to the purposes it was originally requested for. In that regard, provisions should be improved in respect of transparency, to reflect that individuals have a right to know how,

when, and for what purpose their data is used by governments, subject to ensuring criminal investigations and prosecutions are not prejudiced. Data custodians should be able to disclose to persons (whether legal or natural) that their data has been disclosed to third parties - and in fact many jurisdictions require them to do so. Disclosure, and not secrecy as is the case with the text at present, should be the rule as otherwise end users are unable to challenge decisions that impact them.

Finally, as with the previous chapter, and for the same reasons, we do not support provisions on real-time access or interception, so we strongly recommend that articles 45 and 46, and all references thereto, be deleted.

***Recommendations by Article***

**Article 35 General principles of international cooperation**

35.1 – make clear that evidence-gathering relates to serious criminal offences defined in Articles 6 to 16 in the Convention.

35.2 – Make dual criminality a necessary requirement and make clear it will be fulfilled if the conduct relates to a serious criminal offence set forth in this Convention and in the laws of the cooperating states.

**Article 36 Protection of personal data**

Add two additional provisions:

1. That where the source of the data is a data custodian, that entity is entitled to inform the natural person concerned of the request where it does not prejudice an ongoing investigation, and that data custodians may publish the number of requests and the state parties who have made them periodically;
2. That the article is without prejudice to a State Party's domestic legal framework where it imposes conditions on the transfer of person data to other states. This is very important to ensure conflicts of laws problems do not frustrate cooperation; in such cases the relevant States Parties should consult one another to see if a resolution can be found.

**Article 37 – Extradition**

We recommend several changes.

37.1 – the threshold for deprivation of liberty should be a minimum, not a maximum, of four years, rather than one year. This would make this article congruent with the serious crime threshold of the rest of the Convention.

37.8 – "and safeguards" should be added after "conditions" and a specific reference to 37.15 should be added before domestic law.

37.9 and 10 should include existing international law before domestic law.

*37.15* should be modified as follows: "Nothing in this Convention shall be interpreted as imposing an obligation to ~~extradite~~ cooperate if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin, membership of a particular social group, or political opinions, or that compliance with

the request would cause prejudice to that person's position for any one of these reasons, or if there are substantial grounds for believing that the person would be in danger of being subjected to politically motivated persecution, torture, or inhuman and degrading treatment or punishment."

37.20 – at the end add a clause that makes clear States Parties may also take measures against states that intentionally harbor cybercriminals in their jurisdictions, whether or not they are States Parties to this Convention.

**Article 40 – General principles and procedures relating to mutual legal assistance**

40.1 – remove the ending phrase of the last sentence, after "Convention", so that the provisions only extend to offences in this Convention.

40.3 – make clear that assistance should not be contrary to existing international obligations or domestic law and delete (e) and (f).

40.6 – insert "existing international human rights instruments" between "under" and "any" to give emphasis to these instruments.

40.19 – make the existing second paragraph item a, and insert a new item b, to make clear that the accused will be notified unless secrecy is required as provided for in article 27(3).

40.20 – replace the existing text with a provision that the requesting state should inform the requested state in writing of the necessity for keeping the request confidential, and that such decisions should use the procedure we proposed to be added as Article 27(3) above.

40.21 – add a provision to make clear that the request may be refused if the requested state has reason to believe that dual criminality would not be fulfilled, or if the requested state has reasons to believe doing so would violate the human rights of the accused person.

40.30 – add a provision at the end making clear that such documents should be relevant to the investigation or prosecution of an offence defined in this Convention.

**Article 42 – Expedited preservation of stored [computer data] [digital information]**

42.2(g) – remove the presumption of secrecy and amend the provision to call for a rationale for confidentiality leveraging Article 27(3) as provided above.

42.3 – add "international obligations" in front of domestic law.

42.8 – provide for the requested state to notify the data custodian it should delete the preserved data at the end of the 60-day period.

**Article 43 - Expedited disclosure of preserved traffic data**

Add a new provision at the end that allows refusal if the requested state believes dual criminality could not be fulfilled.

**Article 44 – Mutual legal assistance in accessing stored [computer data] [digital information]**

Add a new (4) to make clear that the disclosure may be refused on the grounds provided in Article 40.21 or Article 24. This proposal aligns this Article with Article 43, where the same provision is in 43.2.

**Articles 45 and 46 should be deleted** as previously mentioned.

**Article 52 Return and disposal of confiscated proceeds of crime or property**

52.1 – add, at the end of the provision, an obligation that the proceeds of crime should be returned to its legitimate owners wherever possible, irrespective of what territory they are in. This should be the default, with the proceeds only going to other destinations as a last resort.

**Article 52 Return and disposal of confiscated proceeds of crime or property**

Returning proceeds of crime to its victims: Given that one of the most important objectives of the Convention is to protect victims and, wherever possible, recompense them for the damages suffered, we propose to amend Article 52 so that proceeds of crime confiscated by a State Party pursuant to article 31 or 50 can be returned to its prior legitimate owners whenever possible, and in accordance with its domestic law and administrative procedures.

## 6. Preventive measures [Art. 53]

This chapter, like the rest of the Convention, should focus on cybercrime and not the use of technology or general cybersecurity. States have typically focused on developing frameworks and legislative approaches that aim to increase the cybersecurity and cyber resilience of the online environment in non-criminal contexts and we believe this Convention should follow that pattern. The Convention should therefore remain focused on the public sector, given that governments have exclusive responsibility for criminal law and enforcement.

However, we would like to highlight the importance of Article 53.4 on anonymous reporting of ICT vulnerabilities. This covers, amongst others, penetration testers and security researchers (often known as "white hats"), when they do their work without authorization but with the intent to help service providers of all kinds learn of security vulnerabilities so they may be remediated before criminals exploit them. As we have repeatedly asserted, the Convention should proactively protect such activities from being criminalized. The criminalization chapter should address this deficiency, but this provision should be retained as well.

## 7. Technical assistance and information exchange [Art. 54-56]

The Convention cannot be successful unless all its States Parties are able to implement all its provisions leveraging best practices on a voluntary and demand-driven basis. That is why development and capacity building are fundamental to the success of the Convention.

We know that all states, irrespective of their level of development, have capacity constraints in their efforts to cooperate with other states on criminal matters to one extent or another. Ensuring states can cooperate more quickly and effectively ought to be a shared goal.

Last, but not least: stakeholders play an important role in technical assistance and capacity building both as recipients and as implementers: as we have noted elsewhere, most of the data and insights necessary to address cybercrime are in the hands of the private sector and the technical community. We welcome provisions that create a framework for training programs, as well as technical assistance to support the implementation of the Convention.

Existing cybersecurity capacity building principles, agreed in 2021 by consensus in the report of the Open-ended working group on cybersecurity (A/75/816) should be reflected in the provisions of this chapter. This includes, *inter alia*, states' commitments that cyber capacity building should respect human rights and fundamental freedoms, be gender sensitive, sustainable, results-focused, demand-driven, voluntary, and tailored to specific needs and contexts.

***Recommendations by Article***

**Article 54 Technical assistance and capacity building**

Insert references to voluntary collaboration with stakeholders, *mutatis mutandis*, in paragraphs 2 and 5; Furthermore, in our experience, conflicts of laws frequently present an obstacle to effective collaboration and ensuring that States Parties and stakeholders are better aware of them and how to they can be addressed will help everyone. Therefore, we propose to add two additional paragraphs at the bottom of the list in Article 54.3:

- *"(j) Methods for addressing, and training to address, conflicts of laws arising where requests made by one State Party to another would require a third party to infringe the law in one of the concerned States Parties;*
- *(k) Methods for addressing, and training to address, common issues in the formulation of requests for cooperation between States Parties that are refused because the request is overly broad or not sufficiently particular."*

**Article 55 Exchange of information**

Insert references to voluntary collaboration with stakeholders, *mutatis mutandis*, in paragraphs 1 and 2.

## 8. Mechanisms of implementation [Art. 57-58]

The Convention needs a mechanism for implementation that ensures all parties integral to fighting cybercrime are a part of the process.

It is an objective reality that effective cybercrime investigation, prosecution, and redress for victims is impossible without multi-stakeholder collaboration. This argues for a step-change in the involvement of non-governmental stakeholders without ECOSOC accreditation (such as the private sector) in the mechanism for implementation of this Convention compared to previous international instruments related to criminal matters.

We also believe that an expert forum of states, industry, and the technical community to exchange views on the evolving cybercrime threats and the practical application of the Convention would have real value, especially given the fast-paced nature of cybercrime across the globe. This could have modalities for participation of a more informal nature, allowing any member to bring up issues it sees as relevant to the broader group for discussion; any common views could then be taken up as appropriate in the Conference of the Parties.

***Recommendations by Article***

**Article 57 Conference of the States Parties to the Convention**

Improve the value of input from stakeholders by amending paragraph 6 so that it makes clear unambiguously that submissions from stakeholders will be considered.

Given how successful the modalities for stakeholder participation, adopted by consensus in (A/RES/75/282), have been in the work of the Ad-Hoc Committee we believe those should be embedded in Article 57.

**In closing we'd like to thank the Committee for their kind attention.** We are at the service of all concerned and can be reached as follows:

**During the AHC Session:** Mr. Nick Ashton-Hart, Head of Delegation, at nashtonhart@apcoworldwide.com and+1 202 779-1072

**All other times please email:** eravaioli@apcoworldwide.com