NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Fourth Session

9-20 January 2023

Submission of the Office of the United Nations High Commissioner for Human Rights

10 January 2023

1. Introduction

The Office of the United Nations High Commissioner for Human Rights (OHCHR) welcomes the opportunity to provide comments to the Consolidated Negotiating Document (CND) and to continue our participation in the process towards a new Convention. In advance of the fourth round of negotiations in January 2023, OHCHR reiterates the importance of an inclusive process and the need to put human rights protection at the centre of the future Convention. We welcome the availability of the CND, which provides the opportunity to ground our comments on concrete textual proposals, building on our previous observations and recommendations.

As a general point, we would like to emphasise that development of a future Convention on cybercrime takes place is an environment which is dominated by expansive cybercrime laws across various jurisdictions which are unjustifiably used to target legitimate exercise of human rights and that undermine the rule of law. It is also a context where there are considerable variations not just between States but also between existing regional instruments, including in the definition of "cybercrime". A future Convention that is rooted in the international human rights framework would play a significant role in curbing this trend by helping to ensure that measures to prevent and combat cybercrime, understood primarily as cyber-dependent crimes, do violate human rights or run counter to States' legal obligations.

OHCHR is particularly concerned regarding two features of the current text which may stand in the way of achieving this aim. The first is the broad scope of the future Convention which currently includes a very wide range of cyber-enabled criminal offences, including acts that under international human rights law cannot be subject to criminalization. The second is the broad manner in which criminal offences and procedural measures are drafted and which would violate international human rights standards that require such measures meet criteria of legality, legitimate aim, necessity and proportionality. The comments provided here are not intended to be exhaustive nor to offer a detailed analysis of each article. Rather, through these comments, OHCHR wishes to highlight some cross-cutting issues where we believe our observations and recommendations can have an added value and help strengthen the Convention's grounding in human rights.

2. Chapter I: General Provisions

(a) Article 1. Statement of purpose

As raised by several States and other stakeholders since this treaty process began, efforts to combat cybercrime need to be solidly grounded in human rights, both because cybercrime can endanger the enjoyment of rights and because the measures taken to combat cybercrime must themselves be human rights compliant. The current draft addresses the second point in article 5 through a general human rights clause, and we believe this point can be further strengthened in each of the specific provisions on procedural measures. However, the draft's statement of purpose is silent on the first point, and could benefit from making this link explicit by underlining the strengthening of human rights and the State duty to respect, protect and promote human rights, as a key element of its purpose.

By stating clearly that the protection of human rights is a reason why cybercrime needs to be prevented and combatted, the draft will achieve a more meaningful statement of purpose that is grounded in human rights law. Examples of regional treaties that directly ground the statement of purpose in human rights can be found in the African Union Convention on Preventing and Combatting Corruption[1], article 2; and the African Union Convention on Cybersecurity and Personal Data Protection[2], article 8.

(b) Article 3. Scope of application

It is not immediately clear what role article 3(1) and (2) are envisaged to perform and what added value these paragraphs may have beyond what is provided in article 41 (see comments below to article 41). For this reason, OHCHR recommends deleting article 3(1) and (2) altogether to avoid duplication. As discussed below, OHCHR also recommends that the scope of application for the procedural measures and law enforcement as set out in Chapter III of the CND be narrow.

Concerns also arise with regard to article 3(3), determining that criminal offences under the Convention by default do not need to result in damage or harm to persons, legal persons, property and the State. This may lead to criminalization of legitimate behaviour and would further provide an overbroad scope for initiating procedural/law enforcement measures, including in cases where it would not meet the criteria of necessity and proportionality. Moreover, in view of the CND's general provisions on criminalization of attempt, preparation and participation in article 36, and together with the lack of a clear (criminal) intent requirement for several of the criminal offences under the Convention, this could lead to far-reaching criminalization as well as far-reaching procedural and law enforcement measures, beyond what is necessary and proportionate. For example, the current text could lead to the criminalization of research or journalistic activities, or of the mere possession of an electronic device. While situations can be envisioned where the *potential* for harm can justify law enforcement measures, this is something that should be added to those provisions that are relevant. For this reason, it is recommended to avoid a general (default) provision precluding the

[1] https://au.int/sites/default/files/treaties/36382-treaty-0028_-_african_union_convention_on_preventing_and_combating_corruption_e.pdf.
[2] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

need for harm or damage. Instead, lack of harm/damage can be added to only those specific provisions where lack of harm or potential for harm can justify criminalization and initiation of procedural/law enforcement measures.

(c) Article 5. Respect for human rights

OHCHR supports a general clause requiring that the implementation of the treaty be in line with international human rights law. As noted in OHCHR's submission to the Ad Hoc Committee of 17 January 2022, national cybercrime laws are frequently drafted in overly broad fashion and used to silence political opponents, oppress peaceful protests, prosecute human rights defenders and hamper the work of journalists. A general human rights clause serves the function of articulating the overall frame within which the provisions of the future Convention are to be interpreted, and signal that this international instrument is not to be interpreted in a way that can justify such steps. This general human rights clause also sets the overall frame for ensuring that the interpretation of both the criminalization provisions and the procedural/ law enforcement measures do not go beyond what is necessary, proportionate and in pursuit of a legitimate objective.

As the Convention has concrete implications for the right to privacy and other rights through the powers given to investigation and law enforcement authorities, the general clause also gives the opportunity to articulate more explicitly some of the elements of the human rights framework that are particularly relevant to prevent arbitrary infringement of individual rights. One such element is the principle of due process of law.[3] Elements of this principle are already incorporated into some of the specific provisions of the CND, for example provisions that refer to the necessity and proportionality of specific law enforcement measures, but this approach is not taken consistently throughout the document. In addition to being explicitly included in the general human rights clause, guarantees of due process of law should be incorporated into each procedural and law enforcement provision.

Applied to the measures within the scope of the Convention at hand, including due process guarantees would invite an evaluation of the predictability of the application of procedural and law enforcement measures, the competence and independence of the authorities authorizing various measures, the fairness of the measures governing their application, the potential for excessive use of such powers and the availability of safeguards against abuse.

It is recommended that article 5 is enhanced to make explicit reference to international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), as well as an explicit acknowledgement of the rights particularly affected by the future Convention (including the right to privacy, the right to freedom of

[3] As a general principle of law, due process of law encapsulates the idea that the exercise of the powers of government, including in law enforcement, must be accompanied by recognizing safeguards for the protection of individual rights. Notions of due process are further reflected in several articles of the International Covenant on Civil and Political Rights, including article 14, and due process is also interpreted as a condition to prevent arbitrary interference with rights.[3] The Human Rights Committee has called for a broad interpretation of "arbitrariness" which includes "elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality". See https://undocs.org/CCPR/C/GC/35.

expression, the prohibition against discrimination) as well as the principles that any modern Convention on crime prevention and investigation should seek to strengthen, such as rule of law, due process and minimum standards in the administration of justice, and the respect for democratic principles and institutions. Examples of general human rights clauses with enhanced language can for example be found in the African Union Convention on Preventing and Combatting Corruption, which in addition to including the promotion of human rights in its objectives under article 2, includes a set of principles in article 3. As a further safeguard, OHCHR would also recommend the addition of language providing that "*nothing in this treaty should be interpreted in a way that would constitute a violation of or weaken States' obligations under international human rights law".*

In this context, we would like to reiterate that, while a general human rights provision would be an important element of basing the Convention on human rights, each provision of the Convention, needs in addition to be written in a fully human rights compliant way.

3. Chapter II: Criminalization

Before commenting on specific provisions in Chapter II, we would like to make a few general observations. First of all, we would like to reiterate that in OHCHR's view, the Convention should focus on offences that are specific to computer data and systems and therefore require explicit criminal law provisions due to the lack of protection provided by existing criminal law. On that basis, only a narrow set of offences inherent to cyberspace should be criminalized, such as crimes against integrity, confidentiality and availability of data and systems, misuse of devices for the purpose of committing these crimes, and, where appropriate, a limited number of specific computer-related offences, such as computer fraud and forgery.

In addition, the Convention should avoid including offences based on the content of online expression ("content offences"). As noted, cybercrime laws have been used to impose overly broad restrictions on free expression, for example by criminalizing various online content related to extremism, terrorism, public morals, or hate speech. The current text's inclusion of a number of content offences and the scope of these offences would stand in direct conflict with States' international human rights obligations. A future Cybercrime Convention should expressly ensure that its provisions neither improperly restrict conduct protected under human rights standards or allow for interpretations that would do so, nor legitimize already existing uses of cybercrime law as an instrument for oppression.

Moreover, the provisions criminalizing particular conduct should be clear and focused, rather than open to broad interpretations. The principles of legality and legal certainty require criminal law provisions to be publicly accessible, clear, and precise in scope, so that individuals can reasonably ascertain which conduct is prohibited and adjust their behaviour accordingly. Vague and imprecise definitions of offences leave room for arbitrary interpretations and risk infringement of human rights. To reduce these risks and to avoid over-criminalization, any international instrument should define criminalized conduct in a clear and narrow manner.

Against this background, we are particularly concerned at the possibility that provisions on incitement to subversive or armed activities (article 26), extremism-related offences (article 27), denial, approval, justification or rehabilitation of genocide or crimes against peace and humanity (article 28), terrorism-related offences (article 29) could be included in the Convention.

Furthermore, the Convention should ensure that it cannot be instrumentalized to restrict the legitimate work of civil society organizations, journalists, security researchers, whistle-blowers and other actors pursuing the public interest. Apart from narrowly and precisely drafting provisions establishing criminal offences, we recommend that States consider introducing a public interest exception into the Convention.

OHCHR further notes that while several of the provisions in this chapter require an act to be committed "intentionally", this is not a consistent requirement throughout. Several provisions on criminalization lack the requirement of intent altogether (see articles 13, 14, 22, 23, 26, 27, 29). The Convention should ensure that intent is included as a minimum for all acts subject to criminalization. The absence of such a requirement would easily lead to abuse of the Convention to target legitimate activities. As highlighted by our previous submission, cybercrime provisions without a requirement of intent have proven problematic in the past. OHCHR also notes that for those articles that already include the requirement of intent there appears to be some inconsistency as to those that require intentionality *and* unlawfulness, and those that fail to do so, as well as those that make "criminal intent" discretionary and those that do not.

(a) Cluster 1

Several provisions in Cluster 1 are phrased in a way that could enable the criminalization of legitimate acts, done without any criminal intent or causing any harm. For example, article 16 is worded in a very broad fashion and could be read as criminalizing very common practices, such as the sharing of passwords for online services among family and friends. Furthermore, articles 6 and 10, as currently drafted, could impose criminal penalties on independent security researchers and whistle-blowers. This raises the risk of chilling crucial cybersecurity work and access to public interest information. In this context, the aggravation of penalties made possible by article 6(3) is concerning, in particular since it would cover any confidential government information. Such a broad clause risks introducing overly strict punishments even when the information concerned is not particularly sensitive.

To address these concerns, OHCHR recommends elevating criminal intent, as referred to in article 6(2) to be a requirement of criminalization rather than an option open the States parties to the Convention. Moreover, article 6(3)(b) should at least be limited to highly classified government information, understood as information where the unauthorized disclosure reasonably could be expected to compromise the security of the population, the national economic supply, the security of infrastructure, the fulfilment of the duties of the government and the armed forces, international relations and the protection of sources or individuals in the operation of intelligence services.

(b) Cluster 4

The inclusion of provisions on infringements of copyrights and related rights raises concerns. Copyright enforcement is a matter where interests and rights of rightsholders, users and the public compete. It therefore requires a carefully calibrated approach using a variety of enforcement measures from civil proceedings to administrative actions and, in the most serious cases, criminal sanctions. Existing copyright treaties have undertaken to employ such a nuanced lens and to leave States parties sufficient flexibility to adopt measures that suit their legal systems and avoid over-enforcement of copyright to the detriment of free expression, access to information and innovation. By imposing criminal sanctions for infringements of copyrights and related rights under any applicable copyright treaties, including those that do not require or do not even mention criminal sanctions, the Cybercrime Convention would risk fundamentally changing the balance struck in existing international frameworks and domestic laws.

(c) Cluster 5

Combatting and preventing child sexual abuse and exploitation is a matter of the utmost importance. If provisions addressing crimes in that regard are included in the Convention, the rights of children and their best interest should be the key considerations guiding the drafting. OHCHR recommends in this regard to align the language in articles 18-22 with the Convention on the Rights of the Child, the widely ratified Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, as well as the Committee of the Rights of the Child's General Comment 25 on "Children's Rights in Relation to the Digital Environment".[4]

The current text falls short by potentially encroaching upon children's rights and failing to properly protect the legitimate experience and expression of sexuality of adolescents. For example, article 18 could be interpreted in a way that would criminalize the production or possession of intimate images made within a consensual relationship between adolescents. Similarly, article 21 could be read as criminalizing the sharing and saving of any contact information between adolescents. Also, article 20 could result in making certain consensual sexual relations between adolescents a criminal offence. Such outcomes contravene the recommendation of the Committee on the Rights of the Child to "avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity."[5] While article 18(4) appears to address this, the current wording "take due account of avoiding the criminalization of children that have self-generated material as described in paragraph 2 (…)" does not offer sufficient guarantee for the rights of adolescents and would need to be significantly strengthened to avoid that the provision is used to target consensual relationships between adolescents. In this connection, article 18(4) should be expanded to cover the offences set out in articles 20 and 21 as well.

Article 20 has additional shortcomings. Some of the language, such as "grooming" is vague and could encompass a vast range of actions. This is particularly concerning since the term "grooming" has in some parts of the world been misappropriated and is being used in an abusive manner against LGBTI people. Furthermore, by linking grooming to

[4] https://undocs.org/CRC/C/GC/25.
[5] https://undocs.org/CRC/C/GC/20, para. 40.

"unlawful" sexual conduct, while apparently leaving the determination of unlawfulness to domestic law, article 20 could become the basis for further criminalizing same sex relations and trans people, and exposing LGBT people to arrest, in countries with laws that run counter to protection of LGBTI rights.

(d) Clusters 8 and 9

All of the articles in cluster 8, which deals solely with speech-related crimes, are currently formulated in a way that directly contravenes international human rights law, raising substantial concerns. The overbroad wording of these provisions does not meet the threshold of advocacy to incitement to violence, hatred or discrimination under article 20(2) of the ICCPR and the language lacks the necessary clarity and precision required under article 19(3) of the ICCPR. Given these serious shortcomings and concerns that the future Cybercrime Convention is not the appropriate place for defining criminal offences relating to terrorism, violent extremism conducive to terrorism and incitement to violence, OHCHR recommends the removal of Clusters 8 and 9. For more detailed analysis of the range of problems raised by Clusters 8 and 9, see the following paragraphs.

At the outset, OHCHR reiterates that article 19 of the ICCPR protects everyone's right to maintain an opinion without interference and to seek, receive and impart information and ideas of all kinds. Under article 19(3) of the ICCPR, restrictions on the right to freedom of expression must be "provided by law", and necessary for "the rights or reputations of others" or "for the protection of national security or of public order (ordre public), or of public health and morals". Under the article 19(3) requirement of legality, it is not sufficient that restrictions on freedom of expression are formally enacted as domestic laws or regulations. Instead, restrictions must also be sufficiently clear, accessible and predictable.[6] In this context, the United Nations High Commissioner for Human Rights and regional bodies have criticized laws that criminalize "extremism" for targeting non-violent conduct and using broad and imprecise definitions.

OHCHR notes that while the title of article 26 speaks of "incitement", the actual description of the criminalized speech ("*call issued by means of information and communications technologies for subversive or armed activities directed towards the violent overthrow*…") does not align with the requirements of incitement as defined under international human rights law. Each of the terms in this provision should be narrowly and clearly defined, and a requirement of intent should be explicit. Absent those changes, OHCHR recommends deletion of this provision.

The current language in article 27 provides excessive discretion to the authorities, which could be used to target legitimate expression, and risks leading to disproportionate suppression of a wide range of expressive conduct that may not be suppressed or penalized in a democratic society, including criticism of the government, news reporting, political campaigning and the expression of unpopular, controversial or minority opinions. The language of article 27 ("distribution of materials" and "provision of access to such materials") may also impose third party liability on platforms in ways that could undermine freedom of expression. In view of the above, OHCHR recommends the removal of this provision.

[6] Human Rights Committee, General Comment 34 (https://undocs.org/CCPR/C/GC/34), para. 25.

Article 28 criminalizes freedom of expression on grounds that are incompatible with international human rights law. As held by the Human Rights Committee, laws that penalize the expression of opinions about historical facts are incompatible with the obligations that the ICCPR imposes on States parties in relation to the respect for freedom of opinion and expression.[7] According to the Committee, the ICCPR does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events. In view of this, OHCHR recommends the deletion of this provision.

Concerning article 29, OHCHR notes that it lacks the necessary requirement of intent. Moreover, the language in this provision both lacks precision and includes a wide range of acts, including types of speech that under international human rights law cannot be subject to criminalization. The lack of a universal definition of terrorism or a definition in the Convention itself, together with the vagueness and ambiguity of article 29, would in effect grant State authorities wide discretion in its application for purposes that would not be considered legitimate under international human rights law.

Any counter-terrorism provision should be sufficiently precise to comply with the principle of legality, so as to prevent the possibility that it may be used to target civil society and the legitimate exercise of rights. The principle of legal certainty under international law, enshrined in article 11 of the UDHR, requires that criminal laws are sufficiently precise so it is clear what types of behaviour and conduct constitute a criminal offence and what would be the consequence of committing such an offence. A failure to restrict counter-terrorism provisions and implementing measures to the countering of conduct which is truly terrorist in nature poses a risk of unnecessary and disproportionate interferences with a vast range of rights, such as freedom of expression, movement, family life, religious belief, education and health. OHCHR recommends the removal of this provision. Should the Convention contain a terrorism-related offence, the provision should refrain from using the vague notion of "terrorist offences", or "terrorism-related offences", and define the offences covered by the provision clearly. OHCHR furthermore would like to stress that the provisions' language on "facilitation of communication", "use of website", and "collection or provision of funds" are overbroad and should be avoided, as they would not comply with international human rights standards. Moreover, "use of website" and "facilitation of communication" could create criminal offences for service providers or individuals who merely visit a website, in violation of the right to freedom of expression under international human rights law.

In the absence of a universal and comprehensive definition of terrorism, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted that the counter-terrorism conventions provide the proper starting point for determining what conduct is to be proscribed in the fight against terrorism. This includes the International Convention for the Suppression of the Financing of Terrorism, Security Council resolution 1566 (2004), as well as the report of the Secretary-General's High-level Panel on Threats, Challenges and Change. The definition of terrorism and terrorism activity must be confined to acts that are 'genuinely' terrorist in nature in accordance with the three cumulative elements identified by the Security Council in its resolution 1566 (2004), paragraph 3 and the

[7] Human Rights Committee, General Comment 34 (https://undocs.org/CCPR/C/GC/34), para. 49.

model of definition of terrorism developed by this mandate and recommended as best practice.[8]

OHCHR further notes that several elements in the language of article 29 also concern speech crimes, and that the broad umbrella of "terrorism" is used to cover a range of different forms of expression, including expression that do not meet the threshold of articles 19(3) and 20 of the ICCPR. Moreover, some of the forms of expression listed in article 29 would already be covered by article 27 on extremism-related offences. OHCHR would therefore recommend to remove these elements from article 29. OHCHR notes that "advocacy and justification of terrorism" as well as "spreading of strife, sedition, hatred or racism" do not meet the threshold of incitement under article 20(2) of the ICCPR, nor do they offer the sufficient clarity or precision as required under article 19(3) of the ICCPR. For this reason, OHCHR recommends that the speech related provisions under article 29 should be deleted.

(e) Cluster 11

Some provisions in Cluster 11 raise concerns given their vagueness and overbreadth. Article 38 lacks the necessary clarity by demanding a "long statute of limitations" without specifying what would constitute such a long period. Moreover, as the provision does not require differentiating between the gravity of the criminal offences concerned, measures taken under it could fail the proportionality requirement imposed under international human rights law.

Article 39 is also problematic. Paragraph 4, which requires to parties to "maximize the effectiveness of law enforcement measures" inappropriately requires states to pursue that objective without taking account of the human rights affected by such measures. Similar concerns can be brought forward concerning paragraphs 6 and 7, which seem to give greater weight to prosecution of offenses than to the full range of rights of the defendants and convicted persons.

Article 39(5) should be strengthened to expressly recognize that prosecution and adjudication powers under the Convention should be subject to international human rights standards on due process and fair trial, to avoid situations where domestic law offers weaker guarantees than those provided under international human rights law. As to the second paragraph of article 39, we refer to the concerns raised above with regard to article 6(3).

---

[8] A/HRC/16/51. According to the model definition, terrorism means an action or an attempted action where the action

a) including against civilians, is committed with the intention of causing death or serious bodily injury, or the taking of hostages;
b) irrespective of whether motivated by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, is committed for the purpose of provoking a state of terror in the general public or in a group of persons or particular persons, intimidating a population, or compelling a Government or an international organization to do or to abstain from doing any act, and
c) it constitutes an offence within the scope of and as defined in the international conventions and protocols relating to terrorism.

This cumulative approach acts as a safety threshold to ensure that it is only conduct of a truly terrorist nature that is identified as terrorist conduct under law.

.

4. Chapter III: Procedural measures and law enforcement

Effective procedural frameworks that enable access to electronic evidence in a timely manner are crucial for tackling the problem of cybercrime. It is key that human rights are baked into those frameworks, by establishing adequate conditions and safeguards. A global treaty failing in this regard could affect the integrity of and public confidence in criminal justice globally, enabling human rights violations and abuses both at the national level and across borders.

(a) Cluster 1

OHCHR welcomes therefore the inclusion of article 42 with clear references to human rights, the principles of proportionality, necessity and legality, the protection of privacy and personal data, as well as a number of conditions and safeguards. The provisions in Cluster 1 could be further strengthened to ensure that the procedural frameworks set out in the Convention are aligned with human rights requirements.

First, in order to comply with the principle of proportionality, the language of the Convention should acknowledge that intrusive procedural measures should only be adopted in response of criminal offences of sufficient weight. In other words, any wording that would suggest that the procedural measures outlined in Chapter III could be adopted to investigate all crimes that are in some way connected to a computer or evidence stored in electronic form, even petty crimes (as currently in article 41), should be avoided since it would entail disproportionate restrictions of human rights. In this context, OHCHR notes with concern the vast scope of offenses potentially within article 41(2). The consideration of a proper democratic consultation process is a further reason for the need to limit the scope. While OHCHR acknowledges that criminal offences beyond those defined in the future Convention often leaves digital traces and that there is a legitimate demand to enable e-evidence collection, regulation with such deep and multifaceted impact on the enjoyment of human rights requires in each country an open national debate involving all stakeholders and taking into account the criminal law features of each jurisdiction and the complexity of the questions involved. Making key decisions in that regard within a treaty negotiation process that is followed only by a few hundred experts risks undercutting the crucial democratic processes needed for establishing new investigatory powers of the authorities.

Moreover, the current text operates with a general list of procedural measures (articles 43-50), including measures of a particularly privacy-intrusive character, which could in principle be employed in connection with the suspicion of any crime, regardless of the degree of the severity of the criminal offence. The Convention even allows for procedural measures in the absence of suspicion of any criminal offence (see article 43, which only requires reasonable belief that data may be deleted, lost, etc.). In view of the wide range of criminal offences established under the Convention itself, and in particular of the scope of procedural measures in article 2(1) b and 2(1) c extends to any criminal offence, such an approach would easily come in conflict with the principles of necessity and proportionality and could therefore allow arbitrary interferences with individual rights rather than justified law enforcement measures. Instead of the current approach, OHCHR would recommend a nuanced/scaled approach, whereby the type of procedural measure allowed would depend on the gravity of the criminal offence in

question, and where the intrusiveness of the measure (again subject to proportionality) would correspond to the gravity of the criminal offence for which it is employed.

Second, while it is positive that article 42(1) requires that domestic law provide for fundamental rights under international human rights law, this element could be further strengthened, including by replacing "adequate protection" with "full protection". As with article 39(5), this article should be formulated in a way that guards against a lower standard of rights than those guaranteed under international human rights standards.

Third, although article 42(2) mentions limitations of the scope and duration of procedural measures as possible safeguards, the current text of the CND fails to make such limitations mandatory. This risks running afoul of the principles of necessity and proportionality. Therefore, the Convention should incorporate language—either in article 42 or in the provisions of Cluster 2—that sets out an obligation of State parties to limit both the scope and duration of procedural measures to what is necessary and proportionate to the investigation of a particular criminal offence.

Fourth, article 42(2) could be enhanced by expressly mentioning prior authorization of procedural measures by an independent body, ideally a judicial one. As outlined in OHCHR reports to the Human Rights Council as well as in OHCHR's previous submissions to the Ad Hoc Committee, such prior authorization is a key safeguard for privacy-intrusive procedural measures. Consequently, we recommend making such authorization a mandatory safeguard at least for covert procedural measures (where the suspect is not aware of the measure), with exceptions only allowed in acute time-sensitive circumstances and in any event requiring subsequent independent review within strict timeframes.

Fifth, the text should be strengthened by including clear commitments to transparency and accountability measures and requiring access to remedies, in line with article 2(3) of the ICCPR. One key step towards that goal would be to make the notification of targets of procedural measures mandatory, once such notification would not imperil the success of the investigation in question.

Sixth, the Convention should provide robust safeguards for the confidentiality of legitimate attorney-client and other privileged communications, in accordance with international human rights law and standards. Furthermore, additional safeguards should also be in place to protect communications of specific professions commonly regarded as appropriately attracting additional legal protection through privilege rules, such as medical professionals and journalists.

(b) Cluster 2

Further improvements should be made by clarifying or adding conditions and safeguards to the provisions determining the specific measures State parties are expected to adopt. The discussion of Cluster 2 below outlines suggestions that would significantly help bringing the text of the Convention in line with human rights law. We start with three observations that apply to several provisions across Cluster 2 before addressing specific provisions.

First, only some of the procedural measures delineated in the CND expressly require a reasonable belief that a criminal offence has been or is being committed. This requirement should apply to all procedural measures, as lacking such a belief, no procedural measures could be necessary for achieving a legitimate goal, as required by international human rights law. Moreover, we recommend that the text should clarify that there must be a case-specific factual basis for the belief that a crime has occurred or is happening to avoid authorities acting on mere hunches or guesses.

Secondly, the provisions in Cluster 2 fail to expressly require that the information sought through the specific procedural measures is believed to be relevant for the investigation or prevention of a suspected criminal offence. While this may merely be an editorial inaccuracy, it leaves room for expansive interpretations of the provisions that would not comply with necessity and proportionality requirements. We suggest adding language clarifying for each measure that the data sought was necessary only for the purposes of investigating or preventing a specific crime.

Thirdly, articles 43(3), 47(3) and 48(3) would enable States parties to oblige third parties to keep information about the procedural measures in question confidential. While maintaining confidentiality can without question be key to successful investigations, such obligations cannot be limitless. The principle of transparency requires mandatory disclosure of information on personal data. As mentioned before, transparency is a prerequisite for access to remedy; moreover, it is needed for accountability and building public confidence on law enforcement measures. Consequently, confidentiality obligations should be limited to the extent necessary to protect legitimate criminal investigations. Once disclosure of the measures cannot interfere with such investigations, confidentiality should not be required anymore.

Article 46. Search and seizure of [information stored or processed electronically/digitally] [stored computer data]

As noted in OHCHR's submission to the AHC of 17 January 2022, personal electronic devices frequently contain highly sensitive personal information not only about their user/owner, but also many third parties. Search and seizure measures regarding such devices therefore can carry even greater risk to human rights, including the right to privacy, than covert access to data on a particular individual. It is thus essential that the future Convention ensures that these measures are subject to sufficient independent oversight and control. We therefore recommend adding language to that effect to either article 46 or article 42.

Moreover, article 46(4) raises concerns regarding its possible security and privacy implications. The current wording of this paragraph could be read as to impose an obligation on third parties to facilitate the weakening or circumvention of essential security and confidentiality measures, such as end-to-end encryption. It could also be understood as enabling authorities to request the disclosure of security vulnerabilities in ICT systems that could be exploited beyond the specific case. Such measures can severely undermine the right to privacy of individuals and, moreover, hamper security of the ICT for all users globally".

Article 47. Real-time collection of traffic data

It is widely recognized that the collection of traffic data itself reveals sensitive information about individuals, including information which may be unrelated to the criminal offence for which they are authorized, making such approaches at times as intrusive as access to the content of communications themselves.[9] For that reason, OHCHR recommends limiting the application of measures set out in article 47 to serious crimes. The retention of traffic data is a serious measure, irrespective of the length of the retention period and of the amount or nature of the data retained and requires safeguards to protect the data stored against risks of misuse and against any un-authorized access. It should be noted that retention of data and access to them constitute separate interferences with the fundamental rights of the data subjects which require separate justification.

Article 49. Admission of electronic/digital evidence

Article 49 appears to be written in an overly permissive way, failing to provide for any safeguards to ensure that digital evidence has been obtained, stored, and is used in a human rights-compliant way. It fails to mention even fundamental requirements, such as the need to maintain the integrity and accuracy of electronic data and the need to properly and lawfully obtain and handle evidence. In addition, it seems not to limit its applicability to data obtained through measures set out in articles 43-48 but is written in a way that could include data extraction methods that are deeply intrusive and could facilitate evidence tampering. We recommend rewriting the provision so as to include robust limitations and safeguards or deleting the provision altogether.

In concluding, OHCHR refers to its previous submissions and oral statements during the negotiation process[10] and its reports on the right to privacy in the digital age[11] for more details on human rights considerations relevant for drafting a new cybercrime treaty. We stand ready to assist all interested stakeholders in elaborating human rights respecting and promoting responses to cybercrime.

[9] See https://undocs.org/A/HRC/27/37, paras 14 and 19; https://undocs.org/A/HRC/39/29, para. 6.
[10] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/2nd_session_item_4.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Statements/Item4/3rd_session_item_4.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_1_OHCHR.pdf.
[11] https://undocs.org/A/HRC/27/37; https://undocs.org/A/HRC/39/29; https://undocs.org/A/HRC/48/31; https://undocs.org/A/HRC/51/17.