Human Rights Watch's Comments on the Updated Draft Text of the UN Cybercrime Convention (Rev 3)

July 2024

Introduction

Human Rights Watch remains concerned that Rev. 3 of the UN cybercrime treaty (A/AC.291/22/Rev.3) continues to be fundamentally flawed due to a) its ill-defined and exceedingly broad scope and b) its lack of adequate human rights safeguards.

The draft treaty is not in fact about cybercrime, at all. Instead, the convention requires states to establish expansive electronic surveillance powers to investigate and cooperate on a wide range of crimes, even offenses where no information and communication (ICT) system is involved in the commission of the crime.[1] Some elements of the convention call for even physical investigative techniques in relation to all serious crimes, including those with no ICT system implicated at all, such as cross-border requests for physical evidence or in-person testimony.[2]

As a practical matter, the treaty's broad scope would overwhelm an already overstretched mutual legal assistance system, leading to even more delays and backlogs. Opening mutual legal assistance to such a wide range of offenses instead of focusing resources on genuine cybercrime will increase already significant delays.

Furthermore, while the convention attempts to address child sexual abuse material, it does so in a way that risks violating childrens's rights. It is poised to criminalize the consensual conduct of children of similar ages in consensual relationships, contrary to guidance by the UN Committee on the Rights of the Child, and puts at risk the work of human rights organizations that investigate abuses of children's rights.

With greater surveillance powers should come more robust human rights safeguards to protect against abuse. However, this could not be further from the case with the UN cybercrime treaty. Rev 3. continues to defer to domestic law to provide for human rights safeguards and fails to enumerate key human rights standards.

---

[1] See, for example, the contrast between Art. 23(2)(b), which applies the convention's national surveillance powers to "criminal offences committed by means of an ICT system" with Art. 23(2)(c), which applies those same powers to the collection of evidence in electronic form "of any criminal offence". See also Art. 35(1)(c), which similarly applies to evidence in electronic form "of any serious crime" regardless of whether these crimes were committed "through the use of an ICT system" or not. The convention's surveillance powers would for example apply to data captured by "smart" devices, like internet connected home security systems or AI-enabled assistants, even if these devices were not used to commit any crime.

[2] For example, Art. 40(3)(c) allows states to request searches of physical locations for physical evidence of any serious crime; Art. 40(4) allows proactive disclosure of any information (including sensitive personal information) obtained by any means in relation to any serious crime; Art. 41(3)(c) authorizes the locating of suspects of any serious crime by any investigative means.

The draft UN cybercrime treaty resembles a global surveillance treaty to address all crime, which is poised to facilitate cross-border human rights abuses, and far exceeds the most expansive possible interpretation of the Ad Hoc Committee's mandate.[3] The analysis below outlines Human Rights Watch's key concerns with Rev. 3 and should not be considered exhaustive.[4]

1. **Scope** (Title, UNGA resolution, Articles 2, 3, 23, and 35, and Information Note 7)

Title and UNGA resolution

- The new title equates cybercrime with any crime committed through the use of ICT systems, which is harmful from both a conceptual and practical standpoint. Cybercrime traditionally encompasses criminal acts against computer systems, networks, and data. Efforts to expand its definition in recent years have gone hand in hand with criminalization of expression and human rights advocacy.[5] On a practical level, where there are grey areas with respect to application of the treaty, the equation of cybercrime with any crime committed through ICTs will encourage an expansive interpretation.
- The title also signals that the treaty can be expanded to any/all offenses through future protocols. Draft UNGA resolution A/AC.291/25/Rev.1 already provides that the Ad Hoc Committee shall continue its work to elaborate a draft protocol supplementary to the Convention, addressing additional criminal offenses as appropriate.[6] This problematic approach creates specific problems for Art. 4 as elaborated below.
- **HRW recommends the following as the title for the treaty: "United Nations Convention against Cybercrime" and to delete OP5 of A/AC.291/25/Rev.1. If this paragraph is retained, it should be revised so that it reads "Also decides to examine at a future session the question of continuing the work of the Ad Hoc Committee, mutatis mutandis, in accordance with General Assembly resolutions 74/247 and 75/282, to consider the drafting of any protocol supplementary to the Convention**

Article 2 – Definition of Serious Crimes

[3] UN General Assembly, "Countering the use of information and communications technologies for criminal purposes", Resolution 74/247, https://undocs.org/A/RES/74/247 OP2: "Decides to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime."

[4] For more comprehensive analysis of the full treaty see Human Rights Watch and ARTICLE 19, "Comments on the Draft Text of the UN Cybercrime Convention, August 2023, https://www.hrw.org/news/2023/08/30/article-19-and-human-rights-watchs-comments-draft-text-un-cybercrime-convention and Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session, January 23, 2024, https://www.hrw.org/sites/default/files/media_2024/02/Joint_Advocacy_Statement-UN_Cybercrime_Treaty-Jan24.pdf

[5] Many governments are putting into place cybercrime laws with provisions that directly violate freedom of expression, or that are overbroad and vague, lending themselves to crackdowns on freedom of expression. Such laws unduly restrict rights and are being used to persecute journalists, human rights defenders, technologists, opposition politicians, lawyers, religious reformers, and artists. In a 2019 report, the UN special rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, observed, "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world." See: "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch news release, May 5, 2021, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

[6] UN General Assembly, "Revised draft resolution for consideration by the General Assembly", Draft resolution, A/AC.291/25/Rev.1, https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FAC.291%2F25%2FRev.1&Language=E&DeviceType=Desktop&LangRequested=False

- Elements of the draft convention apply to all serious crimes, but the definition of serious crimes does not include any substantive parameters, leaving wide discretion to each state to decide what offenses qualify simply by applying a four-year or greater sentence. Governments around the world criminalize the ability to speak freely, to express non-conforming sexual orientation or gender identity, or protest peacefully, in blatant violation of human rights standards and attach significant jail terms or even death sentences for such acts. In requiring mutual legal assistance for these and other "crimes," the proposed treaty invites governments to facilitate human rights abuses around the world by making highly intrusive surveillance powers available for cross-border investigations through an unprecedented multilateral tool.
- **HRW supports OHCHR's proposal to define "serious crimes" as acts "involving death or bodily harm , significant financial crimes or coercive acts" to limit the potential inclusion of conduct that is protected under international human rights.**[7]

Article 3

- HRW remains concerned by the draft treaty's wide scope for investigations and prosecutions of offenses and even wider scope for collection of evidence.
- Article 3 also continues to apply to the "prevention" of crimes (explicitly mentioned in Art. 3(a) and incorporated by reference to Articles 23 and 35). Inclusion of 'prevention' is acceptable in relation to some parts of the convention (e.g. its capacity-building provisions) but is problematic when applied to specific policing powers (see concerns regarding Interpretive Note 7 on Arts 23 and 35, below).

HRW's position is that Art. 3 should be limited to specific investigations and prosecutions of offenses established in accordance with Articles 7-17 and delete para (b) altogether. If para (b) is retained, HRW recommends amending it as follows:

> 3(b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, **where there are reasonable grounds to believe that a criminal offence established in accordance with Arts 7-17 of the convention has been or is about be committed** as provided for in articles 23 and 35 of this Convention.

Article 23

Overview: Article 23 on the scope of Chapter IV on domestic investigative powers is now helpfully limited to "specific" investigations and proceedings (in line with its counterpart in Budapest) and now includes Article 23(4), which confirms that specific safeguards in limitations found in Chapter IV continue to apply when specific investigative powers set out in Chapter IV are invoked via requests for cross-border legal assistance further to Chapter V of the convention. These developments do not address ongoing core problems with Article 23 and the lack of human rights safeguards in Chapter V cross-border requests (for reasons set out below). Interpretive Note 7 on

[7] UN Office of the High Commissioner for Human Rights, "Information Note: Human rights and the draft Cybercrime Convention", May 2024, https://www.ohchr.org/sites/default/files/2024-05/Human-Rights-Draft-Cybercrime-Convention.pdf

Articles 23 and 35 introduces additional problems and should also be amended. Article 23 also continues to problematically apply to investigations of all crimes, including those with no nexus to the use of ICT systems.

HRW recommends the following amendments to Art. 23(2) and IN7:

23(2) Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences established in accordance with this Convention;
(b) **The collection of evidence in electronic form where there is reasonable suspicion to believe that a serious crime ~~Other criminal offences~~ has been or is about to be** committed by means of an information and communications technology system; and
(**b Alte**) The collection of evidence in electronic form **~~of any crimninal offence~~ where there is reasonable suspicion to believe that a serious crime established in accordance with this Convention has been or is about to be committed**.

Interpretive Note 7. Criminal investigations **~~may~~ shall** include situations where there are reasonable grounds to believe, on the basis of factual circumstances, that a crime has been **or is about to be** committed and **that ~~where~~** the investigation **will** lead**~~s~~** to **evidence of that crime ~~stopping or impeding subsequent crimes from being committed~~**.

Rationale:

- **IN7**: Article 23 was helpfully limited in scope to "specific" investigations and proceedings in Rev.2 (in line with its counterpart provision in Budapest). This inclusion is important because it ensures that law enforcement investigative powers are applied in a case-by-case manner (in line with human rights standards) rather than on a generalized basis.[8] However, Interpretive Note 7 problematically states that investigative powers can be used "where the investigation leads to stopping or impeding subsequent crimes from being committed" even in the absence of reasonable grounds. Investigative powers may only be used when necessary and proportionate, in a specific case, to pursue a legitimate aim. To ensure proportionality and necessity, there should be an individualized determination of reasonable suspicion that someone has engaged, is engaging in, or is about to engage in activity that is appropriately criminalized in a manner consistent with international human rights law. Therefore, reasonable grounds should be a required (not optional) precondition to the exercise of powers in Chapter IV and the use of investigative powers when there is reasonable suspicion that a crime is about to be committed must be assessed on a case-by-case basis. We therefore recommend the above amendments to IN7. We also propose incorporating the reasonable grounds mechanism directly into the text of Art. 23(2)(b), as above.

[8] Human Rights Watch and ARTICLE 19, "Comments on the Draft Text of the UN Cybercrime Convention, August 2023, https://www.hrw.org/news/2023/08/30/article-19-and-human-rights-watchs-comments-draft-text-un-cybercrime-convention. See paragraph 41 and footnote 59.

- **Limit to Cybercrimes or, alternatively, to ICT Crimes:** While UNGA Res 74/247 established the AHC to comprehensively counter the use of ICT technologies to commit crimes, Chapter IV instead continues to authorize the use of ICT systems to investigate any crime including crimes with no nexus to ICT Systems.[9] This would include, for example, the use of production or intercept powers to identify individuals attending a political protest where some property damage occurred on the basis of the mobile phones in the protesters' pockets. The sole nexus to ICT systems is that protesters brought their cell phones with them to the protest. To avoid this overbreadth, HRW would therefore remove paragraph (c) altogether and replace paragraph (b) with (b alt) to limit evidence gathering of crimes established in accordance with the convention, as above.
- **Ensure limits and safeguards apply to Chapter V:** Article 23(4) now indicates that states should use the powers and procedures set out in Chapter IV (including any applicable conditions, limitations and safeguards) when replying to requests for legal assistance further to Chapter V. This is helpful to the degree that it prevents states from using even more intrusive powers when responding to cross-border requests and confirms that Article 24 continues to apply to those powers when invoked through Chapter V. However, Chapter V explicitly authorizes a broader range of international cooperation including many investigative tasks that have no relation to the powers in Chapter IV.[10] Chapter V also encodes specific mechanisms that modify the specific powers set out in Chapter IV,[11] and explicitly supersede their Chapter IV counterparts in relation to collecting, obtaining, preserving and sharing of evidence in electronic form by virtue of Art. 35(2).[12] Art. 24 would not apply to the exercise of any of these powers by virtue of Art. 23(4). We would therefore recommend, as set out below, amending Art. 24 so that it applies to the convention as a whole by replacing "chapter" with "convention" in Art. 24(1) and by adding "and Article 24" to Article 35(2), which lists elements of the convention applicable to evidence gathering provisions included in Chapter V.

Article 35

Overview: Chapter V continues to authorize a problematically wide scope for international cooperation well beyond cooperation on offenses established in accordance with the convention (Arts. 7-17). Art. 35(1)(c) specifically applies Chapter V to the collecting, obtaining, preserving

[9] This is most evident when contrasting Art. 23(2)(b), which applies the powers in Chapter IV to any criminal offence "committed by means of an [ICT] system" with Art. 23(2)(c), which applies the powers in Chapter IV to the "collection of evidence in electronic form of any criminal offence" whatsoever). As noted above, Art. 3, which establishes scope for the entire convention, provides no additional limitation since it incorporates the full breadth of Art. 23 by reference (See Art. 3(b)).

[10] For example, Art. 40(4), which applies with respect of any serious crime, authorizes states to proactively disclose information (including sensitive personal information) to other state parties "where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings", a disclosure power that places human rights at heightened risk and is not tied to any investigative powers itemized in Chapter IV; Art. 40(3)(a) authorizes "taking evidence or statements from persons"; Art. 40(3)(c) authorizes "executing searches and seizures, and freezing" of physical premises and objects ,while Art. 40(3)(g) further authorizes "Examining objects and sites"; Art. 40(3)(m) authorizes "any other type of assistance that is not contrary to the domestic law of the requested State Party."

[11] For example, Art. 41(3)(d) authorizes the provision of electronic data in an emergency whereas Chapter IV does not address any emergency use of the encoded powers it includes while many legal regimes will codify distinct exigent powers for production, preservation, wiretapping, etc.

[12] Art. 35(2) "For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, and articles 41 to 46 of this Convention shall apply."

and sharing of evidence in electronic form "for any serious crime." Elements of Chapter V extend well beyond the AHC's mandate of countering the use of ICT systems in crime and encompass the use of ICT systems to investigate crimes as well as the gathering of physical evidence to investigate any serious crime including crimes with no nexus to the use of ICT systems.

HRW recommends deleting Art. 35(1)(c) or, if retained, amending it as follows.

> 35(1) States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of:
>
> (a) ~~**The**~~ **Specific** investigation**s** and prosecution**s** of, and **specific** judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;
>
> (b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention;
>
> (c) The collecting, obtaining, preserving and sharing of evidence in electronic form **where there are reasonable suspicion to believe that a** ~~**of any**~~ serious crime **has been or is about to be committed by means of an information and communications technology system**~~**,**~~ **and that the offense is legitimately criminalized under international human rights law**~~**. including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention**~~.

2. Human Rights Safeguards (Articles 6, 24, and 35)

Article 6

Article 6(2) is a welcome improvement in the text. While it does not address the draft Convention's wide scope or lack of specific human rights safeguards, it is the only reference to fundamental rights like freedom of expression, association, and assembly, and deleting it would signal states' intention to use this treaty to suppress human rights

HRW's position is that Article 6(2) should be retained.

Article 24

Overview: Article 24 still defers too much to domestic law and does not spell out some important human rights safeguards (principles of necessity and legality, the need for individual notification) while others are left optional (the need for prior judicial authorization premised on robust factual grounds prior to any interference with the right to privacy, including the right to data protection). As noted above, despite the addition of Article 23(4), its application remains limited to the powers and procedures set out in Chapter IV including when they are used to respond to requests for legal assistance further to Chapter V. This piecemeal approach leaves gaps. Article 24 should apply to the full Convention.

HRW makes the following proposals for Article 24:

24(1). Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this ~~chapter~~ **Convention** are subject to conditions and safeguards ~~provided for under~~ **defined by** its domestic law, which shall provide for the protection of human rights in accordance with its obligations under international human rights law, ~~and which shall~~ **including by incorporating** ~~incorporate~~ the principle**s** of **legality, necessity, and** proportionality**, and require a factual basis justifying the use of such powers and procedures**.

(2) ~~In accordance with and pursuant to the domestic law of each State Party, s~~ **S**uch conditions and safeguards shall, ~~as appropriate in view of the nature of the procedure or power concerned~~, inter alia, include **prior** judicial or other independent **authorization and** review, the right to an effective remedy, **demonstrable** grounds justifying application, ~~and~~ limitation of the scope and the duration of such power or procedure, **publication of statistical information periodically detailing the use of powers and procedures, remedial actions taken, adequate notification, and reasonable retention limitations.**

Article 35

Article 35 urgently requires a dual criminality requirement, an explicit human rights safeguards provision, and a prohibition on mutual legal assistance in cases where there are credible reasons to believe that the request is politically motivated or arbitrary. Human Rights Watch supports a dual criminality requirement because of the significant risk of this treaty being used to provide mutual legal assistance for "serious crimes" that overcriminalize protected expression and behavior in a manner inconsistent with international human rights law. These obligations should not be optional and states should be obligated to explicitly incorporate these limitations in their national law as a condition of ratification.[13] Art. 40(22) and 37(15) should be added to Art. 35. These should also be amended to constitute a prohibition set out in national law rather than a discretionary exclusion, as currently formulated, and should adopt a more permissive evidentiary burden. Further, many of the safeguards in Chapter V remain contingent on a state "request" for some form of international cooperation while a number of powers in this Chapter operate without any "request" being issued and, as a result, remain wholly unprotected.[14] Cross-border legal assistance places human rights at heightened risk and requires commensurately robust safeguards.

HRW therefore recommends the following amendments to Article 35:

35(2) For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, ~~and~~ articles 41 to 46**, and article 24** of this Convention shall apply.

35(3) In matters of international cooperation, ~~whenever~~ dual criminality is considered a requirement~~, it~~ **and** shall be ~~deemed~~ fulfilled ~~irrespective of whether the laws of the~~

[13] US ''Clarifying Lawful Overseas Use of Data Act'' (CLOUD Act) , 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf See: Section "Executive agreements on access to data by foreign governments".

[14] See, for example, Art. 40(4)-(5) authorizing proactive disclosure including of sensitive personal information in relation to any serious crime "without prior request"; Art. 47 authorizing direct law enforcement cooperation in relation to offences established in accordance with that Convention; Art. 48 authorizing joint investigations in relation to offences established in accordance with the Convention.

~~requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party,~~ **only** if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

~~40(22)~~ **35(3*bis*) Each State Party shall adopt such legislative and other measures as may be necessary to ensure that** ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ mutual legal assistance**, extradition or any other form of international cooperation shall not occur**

(a) if ~~the requested State Party has substantial~~ **there are** grounds for believing that the ~~request has been made~~ **cooperation is** for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or ~~that compliance with the request~~ would cause prejudice to that person's position for any one of these reasons;

(b) if the offence in question is politically motivated; or

(c) with any state that does not demonstrate respect for the rule of law and adherence to international human rights law including the principle of non-discrimination.

3) Criminalization

Overview: Article 14 on offenses related to online child sexual abuse or child sexual exploitation material continues to criminalize or risk criminalizing content and conduct that has evidentiary, scientific, or artistic value, and does not sufficiently decriminalize the consensual conduct of older children in consensual relationships.

Article 14

Criminal liability for service providers acting as mere conduits: Article 14 (1)(c) still criminalizes "possessing" and "controlling" child sexual abuse material, which could lead to criminal liability for service providers acting as mere conduits. Though the Article 14(1) stipulates that the conduct should be "committed intentionally and without right," "without right" remains novel in international law (with the exception of the regional Budapest convention). To avoid the risk of prosecution under this clause, intermediaries or controllers may implement preventative measures, like general monitoring of users or device-side scanning, which are disproportionate and undermine the human rights to freedom of expression and privacy.

HRW recommends amending Article 14(1)(c) to read "knowingly possessing and controlling" to address this concern.

Criminalization of material that has evidentiary, scientific, or artistic value: Article 14(2) still risks criminalizing material that has evidentiary, scientific, or artistic value. Sub para (d) is of particular concern for human rights organizations that intentionally possess, collect, and publish based on material depicting children being "subjected to torture or cruel, inhumane or degrading treatment or punishment" including cases where "such material is sexual in nature" in order to investigate abuses of children's rights. Human rights organizations would therefore need

to rely on the "without right" exception. But "without right" is not clearly defined in international law and is not sufficiently precise to require exclusion of legitimate activity. States would have significant latitude to define what this means in national law, including whether to exclude attempts by survivors to report CSAM activity to law enforcement or platforms, documentation or trend analysis of CSAM distribution chains, preservation of evidence by platforms, and other activity. There should be no latitude in this provision for states parties to, for example, weaponize this provision in order to persecute survivors who are attempting to document and report their own abuse or by human rights organizations document abuses and assist survivors in accessing justice. Finally, the "without right" exception grants states parties too much latitude when pursuing their own respective objectives, especially in cases where the government is the perpetrator of abuses. The resulting crime will be "established in accordance with the Convention," qualifying for cross-border extradition, investigative powers, and other international cooperation, including in situations where the state in question is the perpetrator of the human rights abuses being documented. This is particularly a problem as Article 22 allows a state to assert jurisdiction over any offense committed against a national of that state.

HRW recommends addressing the above concerns by adding:

14(5)(bis) States Parties shall exclude the following from criminalization:

a) **Material identified in paragraph 2 of this article that is of manifestly artistic, educational or scientific value, and does not include digitally manipulated representations of real persons under the age of 18; and**
b) **Conduct set forth in paragraph 1 of this article that is carried out for a manifestly legitimate purpose related to medicine, the administration of justice, or the documentation of human rights abuses.**

Criminalization of self-generated material by older children in consensual relationships: Article 14 para 4 still does not go far enough to decriminalize self-generated content by children (sub paragraph a) or material produced in a consensual relationship (sub paragraph b). Article 14 establishes that "states parties may take steps to exclude the criminalization" of such conduct. By making decriminalization optional, qualifying material (e.g. consensual sexting between children of similar ages) may constitute an "offence established in accordance with the convention," subject to the convention's extradition and cross-border investigative provisions. The Committee on the Rights of the Child has advised that "States should avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity."[15]

HRW recommends amending the opening line of Article 14(4) as follows:

14(4) States parties ~~**may take steps to**~~ **shall** exclude the criminalization of:

[15] UN Committee on the Rights of the Child, General Comment No. 20, The implementation of the rights of the child during adolescence, CRC/C/GC/20 (2016), https://undocs.org/en/CRC/C/GC/20 (accessed August 20, 2023), para 40.

Summary of proposed amendments

Title
United Nations Convention against Cybercrime ~~(Crimes Committed through the Use of an Information and Communications Technology System)~~

Article 2
(h) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty and **involving death or bodily harm, significant financial crimes or coercive acts"**

Article 3
This Convention shall apply, except as otherwise stated herein, to:

(a) The ~~prevention,~~ investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

Delete Article 3(b). If retained, amend as follows:
(b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, **where there are reasonable grounds to believe that a criminal offence established in accordance with Arts 7-17 of the convention has been or is about be committed** as provided for in articles 23 and 35 of this Convention.

Article 14

14(1)
(c) **Knowingly p~~P~~**ossessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;

14(4) States parties ~~**may take steps to**~~ **shall** exclude the criminalization of:

14(5)(bis) States Parties shall exclude the following from criminalization:

c) Material identified in paragraph 2 of this article that is of manifestly artistic, educational or scientific value, and does not include digitally manipulated representations of real persons under the age of 18; and
d) Conduct set forth in paragraph 1 of this article that is carried out for a manifestly legitimate purpose related to medicine, the administration of justice, or the documentation of human rights abuses.

Article 23

23(2) Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences established in accordance with this Convention;
(b) **The collection of evidence in electronic form where there are reasonable grounds to believe that a serious crime ~~Other criminal offences~~ has been or is about to be** committed by means of an information and communications technology system; and
(**b Alte**) The collection of evidence in electronic form **~~of any crimninal offence~~ where there is reasonable suspicion to believe that a serious crime established in accordance with this Convention has been or is about to be committed**.

Article 24

24(1). Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this **~~chapter~~ Convention** are subject to conditions and safeguards **~~provided for under~~ defined by** its domestic law, which shall provide for the protection of human rights in accordance with its obligations under international human rights law, **~~and which shall~~ including by incorporating ~~incorporate~~** the principle**s** of **legality, necessity, and** proportionality**, and require a factual basis justifying the use of such powers and procedures**.

(2) **~~In accordance with and pursuant to the domestic law of each State Party, s~~ S**uch conditions and safeguards shall, **~~as appropriate in view of the nature of the procedure or power concerned~~**, inter alia, include **prior** judicial or other independent **authorization and** review, the right to an effective remedy, **demonstrable** grounds justifying application, **~~and~~** limitation of the scope and the duration of such power or procedure, **publication of statistical information periodically detailing the use of powers and procedures, remedial actions taken, adequate notification, and reasonable retention limitations.**

Article 35

(1) States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of:

(a) **~~The~~ Specific** investigation**s** and prosecution**s** of, and **specific** judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

(b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention;

HRW recommends deleting Art35(1)(c) or, if retained, amending it as follows.

(c) The collecting, obtaining, preserving and sharing of evidence in electronic form **where there are reasonable suspicion to believe that a ~~of any~~** serious crime **has been or is about to be committed by means of an information and communications technology system~~,~~ and that the offense is legitimately criminalized under international human rights law~~. including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention~~**.

(2) For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, ~~and~~ articles 41 to 46**, and article 24** of this Convention shall apply.

(3) In matters of international cooperation, ~~whenever~~ dual criminality is considered a requirement~~, it~~ **and** shall be ~~deemed~~ fulfilled ~~irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party,~~ **only** if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

~~40(22)~~ **35(3*bis*) Each State Party shall adopt such legislative and other measures as may be necessary to ensure that** ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ mutual legal assistance**, extradition or any other form of international cooperation shall not occur**

(d) if ~~the requested State Party has substantial~~ **there are** grounds for believing that the ~~request has been made~~ **cooperation is** for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or ~~that compliance with the request~~ would cause prejudice to that person's position for any one of these reasons;

(e) if the offence in question is politically motivated; or

(f) with any state that does not demonstrate respect for the rule of law and adherence to international human rights law including the principle of non-discrimination.

Resolution A/AC.291/25/Rev.1

~~**5. Also decides that the Ad Hoc Committee shall continue its work, mutatis mutandis, in accordance with General Assembly resolutions 74/247 and 75/282, with a view to elaborating a draft protocol supplementary to the Convention, addressing, inter alia, additional criminal offences as appropriate, and that, for that purpose, two sessions of a duration of 10 days each, with the first session taking place no later than one year after the adoption of the Convention by the General Assembly and the second session in the following calendar year, in Vienna and New York, respectively, shall be convened for the purpose of submitting its outcomes to the Conference of the States Parties to the Convention at its first session, for its consideration and further action, in accordance with the relevant articles of the Convention;**~~

Interpretive Note 7

Interpretive Note 7. Criminal investigations ~~may~~ **shall** include situations where there are reasonable grounds to believe, on the basis of factual circumstances, that a crime has been **or will be** committed and **that** ~~where~~ the investigation **will** lead~~s~~ to **evidence of that crime** ~~stopping or impeding subsequent crimes from being committed~~.