Human Rights Assessment of the Draft United Nations Cybercrime Convention

Statement by the United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, Ben Saul

25 July 2024

Introduction

1. The Special Rapporteur on the promotion and protection of human rights while countering terrorism is pleased to offer this brief assessment of selected human rights implications of the third revised draft United Nations Convention against Cybercrime,[1] with suggestions to improve its compatibility with international human rights law. Due to its subject matter and scope, the Convention poses distinctive human rights risks that require heightened scrutiny and safeguards. The Special Rapporteur broadly endorses the Submission of the Office of the United Nations High Commissioner for Human Rights dated 22 July 2024.

Offences Committed through the Use of an Information and Communications Technology System: Article 4

2. Article 4 requires states parties to criminalize offences under "other applicable United Nations conventions and protocols… when committed through the use of an information and communications technology system". The provision has the practical effect of extending ending the scope of the offences under other conventions to encompass cyber means, without formally amending each of those conventions. In principle there may be legitimate reasons for so extending some offences under some conventions, to "update" earlier conventions in the light of the potential for the criminal use of cyber technologies.

3. However, Article 4 is objectionable for two reasons. First, it is inherently vague and uncertain in scope because it does not identify the specific conventions or their offences. There are dozens of such instruments and many more offences within them. Each of the offences under those conventions was carefully negotiated with due legal scrutiny given to the particular elements of each substantive and inchoate offence under each convention. Article 4 requires the wholescale and indiscriminate potential extension of every offence under every convention, without close drafting scrutiny of whether it is appropriate, or even possible, to so extend each individual offence and of the human rights implications or other adverse consequences of doing so. Such haphazard extension of a wide range of criminal offences serving a variety of different purposes is not consistent with good practice in the drafting of criminal instruments and could result in inconsistencies with human rights law.

[1] United Nations Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System), A/AC.291/22/Rev.3.

4. Secondly, the criminalization of offences "committed *through the use of* an information and communications technology system" is ambiguous and does not indicate with sufficient precision the circumstances in which cyber means should be unlawful. Commission "through the use of" information and communications technology could encompass a wide range of conduct and interactions with such systems, from intentional and direct deployment of cyber means through to inadvertent, unconscious, incidental, indirect or offline connections with an information and communications system. The indeterminacy of the conduct and fault elements is of concern for two reasons. First, it violates the fundamental principle in international human rights law of legal certainty, whereby offences must be sufficiently clearly defined so as to enable individuals to prospectively regulate their conduct. Secondly, it is likely to produce considerable variations in national implementation and fail to satisfy the double criminality rule in extradition and mutual assistance, thus weakening prospects for international cooperation.

5. **It is recommended** to delete Article 4, unless: (a) an assessment is made of each offence under each of the United Nations conventions and protocols to which Article 4 could apply, to determine the appropriateness of applying Article 4 to them; (b) the Convention specifically lists the specific offences under each United Nations convention and protocol to which Article 4 appropriately applies; and (c) the conduct and fault elements of the expression "committed through the use of an information and communications technology system" are clarified to limit the offences to only acts that intend to produce criminally harmful consequences.

Cybercrime Offences: Articles 7 to 12

6. Articles 7 to 12 of the Convention generally criminalize "intentional" conduct "without right", while some of these offences offer states parties the option to qualify the fault element with more restrictive intent requirements (e.g. intent to obtain data; dishonest or criminal intent; or intent to defraud) and/or to include additional objective elements (e.g. infringing security measures; or a result of serious harm). The very existence of the optional elements recognizes that the offences are otherwise over-broad and capture conduct that not only may not be sufficiently serious or harmful to warrant criminalization, but that may be positively beneficial or in the public interest. Thus, the baseline offences risk criminalizing "whistleblower" disclosure of information to expose illegality or fraud;[2] action to prevent crime; the activities of ethical hackers, cybersecurity researchers, and pen-testers who keep the digital ecosystem secure from genuinely criminal interferences;[3] or acts of protest that that constitute protected freedom of expression. The optional elements will also produce divergence in the offences between national laws, which in turn will increase cases where the double criminality rule cannot be satisfied in extradition and mutual assistance, thus weakening prospects for international cooperation.

7. **It is recommended** that the optional elements be made mandatory in order to ensure that the offences are confined to sufficiently serious and harmful conduct that warrants transnational criminalization and cooperation. An alternative would be to establish mandatory exceptions to the scope of otherwise over-broad offences, as is the position under Article 11(2) (carving out authorized testing or protection of an information and communications technology system).

[2] https://www.ohchr.org/sites/default/files/2024-05/Human-Rights-Draft-Cybercrime-Convention.pdf.
[3] https://cyberpeaceinstitute.org/news/proposed-cybercrime-convention-risks-making-cyberspace-less-secure/#4169daa5-7691-4a3b-8f52-44302bc0ea45-link.

Requiring an Explicit Intention for Inchoate Offences

8. It is welcome that the fault element of intention is explicitly required for the offences of participation and attempt under Article 19. **It is recommended** that the inchoate offences that currently lack an express intention requirement under Article 17(1)(b)(ii) be amended to similarly include it, namely "[p]articipation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article".

Scope of the Convention: Articles 3, 23, and 35

9. While the express purpose of the Convention is the prevention and combating of cybercrime (see Article 1), the Convention covers collection and so forth of electronic evidence for criminal investigations and proceedings not only in relation to cybercrimes but also for "any criminal offence" (Article 23(2)(c)). It further provides for international cooperation on electronic evidence relating to "any serious crime" (Article 35(1)(c)).[4] These expansions beyond the original and core purpose of the Convention in combating cybercrimes proper are not desirable and **it is recommended** that they be deleted from the Convention. Article 23(c) enables the application of highly invasive measures in relation to data connected to even trivial or minor offences under national law, as well as to innocent or legitimate conduct that is abusively criminalized in particular jurisdictions, where such restrictions on rights would not be necessary or proportionate in pursuit of a legitimate law enforcement aim. Article 35(1)(c) limits international cooperation to serious crimes, defined as those punishable by a maximum of four years imprisonment or a more serious penalty (Article 2(h)). Even so, such offences may not be sufficiently serious to warrant transnational cooperation where they do not involve death or injury to persons or other grave harms,[5] given the wide divergence in criminal penalties between states and the excessive penalization of minor or legitimate conduct in states that misuse the criminal law.

Respect for Human Rights: Article 6

10. Article 6(1) commendably affirms that states parties must implement their obligations consistently with their international human rights law obligations, thus responding to the significant risks of rights violations when criminally regulating cyber activities.[6] Article 6(2) provides that the Convention is without prejudice to specified human rights. **It is recommended** to add to this list other rights particularly affected by the Convention, namely the rights to: (a) liberty and security of person; (b) fair trial; (c) privacy; (d) non-discrimination; (e) participate in public affairs; (f) humane conditions of detention and freedom from torture or cruel, inhuman or degrading treatment or punishment; and (g) non-refoulement. **It is also recommended** that Article 6(1) additionally refer to international refugee law and non-exhaustively highlight the International Covenant on Civil and Political Rights 1966 as a particularly relevant instrument.

[4] See relatedly Article 3(b), indicating the scope of application of the Convention to "[t]he collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention".
[5] OHCHR Submission dated 22 July 2024, p. 5.
[6] See e.g. A/RES/76/174 (10 January 2022).

Conditions and Safeguards: Article 24

11. Article 24(1) contains a welcome obligation on states parties to ensure that the procedural measures and law enforcement under Chapter IV of the Convention protect human rights, including "the principle of proportionality".[7] The selective reference to proportionality is, however, plainly under-inclusive of the range of core rights affected by Chapter IV. **It is recommended that** other fundamental principles related to the limitation or restriction of rights be explicitly mentioned, including lawful authority, legitimate aim, necessity and non-discrimination. **It is further recommended** that the list of specific human rights protections in Article 24(2)[8] be reformulated as binding – reflecting their legal status under international law – rather than being presented as subject to discretionary qualifications ("[i]n accordance with and pursuant to the domestic law of each State Party", and "as appropriate in view of the nature of the procedure or the power concerned").[9] These should also be strengthened to reflect their full scope under international law, such not only judicial review but prior judicial authorization of certain intrusive measures such as surveillance.

General Human Rights Safeguards in Chapters II, V, VI and VII

12. The inclusion of the human rights clause (Article 24(1)) in Chapter IV invites reflection on why similar clauses are not included in other relevant chapters, notwithstanding the applicability of the Article 4 human rights clause to the whole Convention. Other chapters each raise distinctive human rights risks, including Chapter II on criminalization, Chapter V on international cooperation, Chapter VI on preventive measures and Chapter VII on technical assistance and capacity building. Chapter V, for example, includes Article 35 on "general principles of international cooperation" but there is no mention of human rights. The inclusion of a safeguard clause in Chapter IV but not the other chapters may imply that human rights are less important in those chapters, despite the inclusion of specific human rights in particular articles of the chapters. The omission is heightened because some of these chapters make a state party's obligations subject to "domestic law"[10] or "fundamental principles of its legal system",[11] but there is no comparable reference to international law. **It is accordingly recommended** that safeguards similar to those in Article 24(1), albeit strengthened as indicated earlier, be applied and tailored to these other chapters.

Prosecution, Adjudication and Sanctions: Article 21

13. **It is recommended** that:

    (a) In Article 21(4), the human rights safeguards in relation to prosecutions, including for fair trial and defence rights, be expanded to include other fundamental rights specially affected, namely the right to liberty and security of person, humane conditions of detention, and freedom from torture or cruel, inhumane or degrading treatment.

---

[7] Article 24(2) further requires "judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure."

[8] Namely, "judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure".

[9] See also the drafting suggestion in the OHCHR Submission, p. 6.

[10] Article 35 on international cooperation under Chapter V; Article 54(3) on technical assistance and capacity building under Chapter VII.

[11] Article 53 regarding prevention under Chapter VI.

(b) In Article 21(2), the discretion for states parties to take into account aggravating circumstances in relation to offences should be balanced with equal provision for states to consider mitigating factors (e.g. severity of the offence and harm caused, age, character, criminal history, personal circumstances, admission of guilt, cooperation with police, blameworthiness, detention as a last resort etc.), in accordance with general principles of criminal law and proportionality in sentencing

(c) In Article 21(3), the direction to exercise any prosecutorial discretion to maximize the effectiveness of law enforcement and deterrence should be balanced by the recognition of other equally relevant public interest factors (e.g. the seriousness/triviality of the offence, the passage of time, the degree of culpability, factors and characteristics personal to the accused and any victims, the interests of justice, other remedies, public confidence, fair trial and other human rights risks etc.).

Extradition and Mutual Assistance: Articles 37 and 40

14. **It is recommended** that:

(a) In Article 37(14), the guarantee of "fair treatment" in extradition should refer not only to rights under "domestic law" but also under "international human rights law".

(b) In Article 37(15), the welcome inclusion of a savings clause for non-discrimination as a basis for refusing extradition should be strengthened and supplemented:

(i) Discrimination should be a mandatory ground of refusal under the Convention;

(ii) Other human rights-based grounds of mandatory refusal should be included, namely *non-refoulement* generally (i.e. not limited to discrimination), including protection against return to: arbitrary deprivation of life, including the death penalty where it is not consistent with international law; torture or cruel, inhuman or degrading treatment or punishment; persecution; flagrant denial of justice or unfair trial; or other serious violations of international law.

(iii) The political offence exception to an extradition request should also be expressly recognized as a permissible ground of refusal.

(c) In Article 40(21), the same considerations pertaining to the refusal of an extradition request in the preceding point of this Statement should apply to mutual assistance. In addition, lack of "double criminality" should be recognized as a ground of refusal, as it already is in relation to extradition (Article 37(1)).

Assistance to and Protection of Victims: Article 34

15. **It is recommended** that the positive measures for victims of crime in Article 34 be strengthened by encouraging states parties to pay due regard to the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power 1985.[12]

[12] A/RES/40/34 (29 November 1985).

Personal Data Protection: Article 36

16. While Article 36 requires personal data sharing to be consistent with international law, implicitly including the right to privacy and other relevant human rights, **it is recommended** to include more explicit and detailed data protection safeguards. In this respect the Special Rapporteur endorses the substance of the drafting proposal of Privacy International.[13]

Preventive Measures: Chapter VI

17. Chapter VI contains numerous potentially positive measures of prevention from a human rights standpoint, including in relation to civil society participation, reintegration of offenders into society, addressing gender-based violence and child safety, enhancing transparency and public participation in decision making and public access to information, respecting freedom to seek, receive and impart public information, and supporting victims of crime. **It is recommended** that Chapter VI also include as a preventive measure the need to address the conditions conducive to cybercrime, which may include state violations of human rights committed whether committed by cyber or other means.

Technical Assistance and Capacity Building: Chapter VII

18. Chapter VI refers in detail to capacity building, training, exchange of information and best practices, technical assistance and technology transfer as means of facilitating the prevention and suppression of Convention offences. Strikingly, there is no reference at all to human rights in the context of any of these activities, including both the importance of mainstreaming human rights in all such activities where relevant and conducting human rights impact assessments in advance of and after such activities. Given the well-recognized potential for abuse of law enforcement powers and data collection in relation to cybercrimes and other crimes covered by the Convention, **it is recommended** that human rights should be incorporated as a mandatory component of Chapter VII activities.

Mechanism of Implementation: Chapter VII

19. **It is recommended** that the periodic conferences of states parties to the Convention charged with reviewing its implementation (Articles 57(1) and (5)(e)) and making recommendations for its improvement (Article 57(5)(f)) be explicitly mandated to review the consistency of implementation with international human rights law and to recommend necessary improvements.

***

[13] Privacy International's Comments on the Updated Draft Text of the UN Cybercrime Convention, May 2024.