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

1. These submissions are made on behalf of ARTICLE 19, an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and information. Our submissions draw on ARTICLE 19 experience and expertise advocating for the implementation of the highest standards of freedom of expression, nationally and globally. These submissions provide recommendations for the content of a) the Preamble, b) criminal offences and c) procedural measures and law enforcement

Preamble

2. At the outset, ARTICLE 19 reiterates that we are not persuaded there is a need for a convention on cybercrime. On the contrary, we believe that without a narrow approach and strong human rights safeguards, this treaty is highly likely to be abused and would perpetuate many of the current problems in existing national 'cybercrime' laws around the world. Therefore, ARTICLE 19 warns against the feasibility to replicate several problems concerning broad provisions and illegitimate restrictions on the rights to freedom of expression, privacy, freedom of assembly and due process. In order to prevent this occurring, ARTICLE 19 urges the Ad Hoc Committee (AHC) to ensure that the protection of human rights is not diminished by the new treaty.

3. Hence, the new treaty should put the protection of human rights as one of the founding principles of addressing cybercrime and security concerns on the Internet. In particular, the Preamble should specifically acknowledge the principle that the rights that people have offline must also be protected online,[1] including the right to freedom of expression and privacy.[2]

4. For the purposes of ensuring the protection of the right to freedom of expression in this treaty, the Preamble could also acknowledge that the use of encryption and anonymity are vital to exercising freedom of expression online as well as to the work of civil society, human rights defenders, and journalists. For the avoidance of doubt, restrictions on the use of encryption of anonymity tools constitute restrictions on freedom of expression and must be avoided at all costs. This is consistent with international human rights standards in this area.[3] Both the UN Special Rapporteur on Freedom of Expression and the European Court of Human Rights uphold that the anonymity of users help promote the free exchange of ideas and information and these tools provide robust rights to privacy.[4]

---

[1] *See* e.g. UN Human Rights Council (HRC), The promotion, protection and enjoyment of human rights in the Internet, A/HRC/38/L.10/Rev.1, 4 July 2018; HRC, The right to privacy in the digital age, A/HRC/RES/42/15, 7 October 2019, para 4.
[2] *Ibid*, UN HRC, The promotion, protection and enjoyment of human rights in the Internet, para 8.
[3] *See* Recommendation no. 6 of ARTICLE 19's recommendations for the UN Cybercrime Convention, March 2022.
[4] *See* European Court of Human Rights, Standard Verlagsgesellschaft v. Austria, App. no. 39378/15, 7 December 2021; UN Special Rapporteur on Freedom of Expression, Report on encryption, anonymity and the human rights framework, 22 May 2015.

Criminal offences

Speech related offences

5. From a human rights perspective, the scope of the convention should be narrow and should not include speech-related offences. Just because a crime might involve technology does not mean it needs to be included in the proposed convention.

6. ARTICLE 19 recalls that assurance of respect and safeguarding of human rights must exist in any human rights instrument, particularly where Member States are parties to the International Covenant on Civil and Political Rights (ICCPR) or regional treaties. Under international law, restrictions on freedom of expression must satisfy a three-part test. They must be defined in law, satisfy a legitimate aim, and be necessary and proportionate. If expressive activities are criminalised as part of a cybercrime proposal, those measures constitute restrictions under international law and must satisfy the tripartite test. Measures that broadly restrict any form of content in a cybercrime law are unlikely to advance a legitimate aim, nor be necessary or proportionate.

1. Further, all prohibitions of 'hate speech' and incitement to violence should not fall under the scope of a criminal cybercrime treaty. Instead, States should implement recommendations outlined in the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[5] and in the reports of the UN Special Rapporteur on freedom of expression and other standards in this area. [6]

2. In ARTICLE 19's experience the cybercrime laws have been **used to criminalise ordinary activities**, including legitimate expressive activities involving computers. Many of these laws include overly broad terms such as 'hate speech', 'cyberbullying', 'disinformation', 'incitement', terrorism and extremism, morality, among others. The use of vague and broad terms in cybercrime laws and "cyber" related criminal provisions is often accompanied with a clear focus on making the use of a computer, device or technology an aggravating circumstance. This is problematic from the point of proportionality of sanctions. There is no evidence that justifies the need to criminalise the use of technology -and therefore the means of expression- based on broad and vague expressive terms. For these reasons we strongly object inclusion of speech related offences among the crimes in the Conventions.

'Core' cyber crimes

3. In our experience, criminalising a large number of offences is counterproductive for freedom of expression and unnecessary to effectively deter cyber-related threats. We observe that the Council of Europe Cybercrime Convention of 2003 contains five offences (Articles 2 - 6) that have been replicated elsewhere. While we point out that the Cybercrime Convention suffers from its own issues from a human rights perspective — particularly a lack of procedural human rights protections and integration with European human rights and data protection instruments — it nevertheless may serve as a reference point as a limit on the number of offences as well as requiring that any offences, at a minimum, serve legitimate aims and be necessary and proportionate. Duplicative offences raise the risk of prosecution for the same conduct as multiple different crimes, as well as increase the risk of over-interpretation and abuse.

---

[5] OHCHR, Rabat Plan of Action, Report of Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred, A/HRC/22/17/Add.4, adopted 5 October 2012, published on 11 January 2013.

[6] *See* Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report on online hate speech, A/74/486, 9 October 2019.

4. We also recommend that criminal offences require "serious" harm and specific "dishonest"/"malicious" intent to commit the offence, rather than mere possession or use of certain technologies. They **must hinge on state of mind, rather than the specific technologies used.**

5. For instance, ARTICLE 19 is concerned that provisions punishing based on technology may be used to prosecute individuals or companies producing, distributing, selling or otherwise circulating software used to break Digital Management Rights systems. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use."

6. Further, **a public interest defence must be provided to ensure the protection of legitimate expressive activities.** A public interest defence entails providing an opportunity for an accused to establish that there was no harm or risk of harm to a legitimate interest in engaging in the proscribed activity, and that the public benefit in the activity outweighed any harm. Such a defence is crucial to prevent the abuse of provisions that criminalise simply accessing computer systems and data without the technical infringement of security measures.

Procedural and investigative Criminal Measures

7. ARTICLE 19 is concerned about the use of criminal procedural measures that may undermine human rights protections for privacy and due process. For instance, extraterritorial application, compulsory mutual legal assistance, and data-sharing obligations may undermine and override the rights to national and regional judicial oversight and remedies, as well as protections under regional human rights and data protection instruments.

8. The treaty **must ensure that information and technology providers are not forced to become extensions of public authorities.** Judicial warrant requirements should not be circumvented on the basis of provisions that mandate the assistance of ICT companies. Any procedural and law enforcement measures should ensure that "assisting" related activities are not implemented in a way that force disclosure of records, to commandeering service providers to become extensions of law enforcement, or to engage in active surveillance of users.

9. **Mutual legal assistance and extradition obligations must preserve international, regional, and national due process safeguards**. The implementation of global investigatory and mutual legal assistance obligations without simultaneously universalising regional human rights and data protection measures could likely lead to lopsided availability of remedies, as well as undermine the scope of protection of existing measures like the EU's General Data Protection Regulation (GDPR), or regional instruments and courts -i.e. European Court of Human Rights, the Inter-American Court of Human Rights, or the African Court on Human and Peoples' Rights-.

10. The treaty should clearly connect to the protection of human rights instruments on due process and privacy. The availability of strong procedural human rights protections must be weighed in any grant of investigatory powers or mutual legal assistance obligations.[7]

For more details on the recommendations outlined in these submissions, please see ARTICLE 19's briefing.[8]

[7] *See* Recommendation no. 8 of ARTICLE 19's Recommendations for the UN Cybercrime Convention, op. Cit.
[8] ARTICLE 19, ARTICLE 19's Recommendations for the UN Cybercrime Convention, March 2022.