ARTICLE 19's Comments on the Consolidated Negotiating Document on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Ahead of the fourth session of the Ad Hoc Committee drafting the international convention on cybercrime, starting on 9 January 2023, ARTICLE 19 raises its concerns about the latest draft of the Convention. In particular, we warn that numerous content-based provisions do not comply with international standards on freedom of expression. Further, the draft instrument conflates "cybercrime" with data protection and personal privacy issues, muddying frameworks that historically have been deliberately separated at the national and regional levels. We urge the Ad Hoc Committee to seriously reconsider its efforts and make sure the draft provisions do not violate international human rights standards which the instrument explicitly requires adherence to and claims to prioritise.

Background

In December 2022, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (the Ad Hoc Committee), released the Consolidated Negotiating Document on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (the Negotiating Document).[1] The Negotiating Document is scheduled to be discussed at the forthcoming forth session of the Ad Hoc committee, commencing on 9 January 2023 in Vienna.

This draft of the Negotiating Document is structured into three chapters, starting with a statement of purpose and ending with provisions dealing with procedural and law enforcement issues.[2] The second chapter deals with criminal measures to be taken at the national level, and is divided into eleven sections titled "clusters" for the purposes of structuring discussions during formal session.[3]

[1] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/16, 7 November 2022.

[2] These are Cluster 1 (jurisdictional issues), Cluster 2 (preservation of data, production orders, searches and seizures, and real-time collection and interception of traffic data) and Cluster 3 (freezing and confiscation of criminal proceeds, compensation, and witness protection).

[3] These are Cluster 1 (offences enumerated in the Council of Europe Convention on Cybercrime - illegal access, illegal interception, data interference, system interference, misuse of devices), Cluster 2 (further offences enumerated in the Budapest Convention – computer-related forgery and fraud), Cluster 3 (privacy-related offences), Cluster 4 (copyright), Cluster 5 (offences pertaining to child exploitation), Cluster 6 (offences involving minors in criminal acts

Overall, ARTICLE 19 is concerned that the Negotiating Document fits into what the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association identified in 2019 as a growing trend[4] of expansive cybercrime laws being utilized as a pretext to stifling freedom of expression and dissent. ARTICLE 19 typically witnesses cyber-legislation contain a large number of criminal provisions when there is 'mission creep' beyond cyberspace, and the legislation punishes conduct merely because it peripherally involves a computer or digital technology. For example, a criminal defamation law that punishes defamation on the Internet should not be codified as a 'cyber offence' as it is essentially a criminal defamation offence (that should be abolished in line with international freedom of expression standards).[5]

As ARTICLE 19 has already provided guiding principles on the first clusters of substantive offences in Chapter Two of the Negotiating Document,[6] in these comments we focus on the freedom of expression issues raised by the content-based offences of the latter clusters (i.e. Cluster 6 onward).

Importantly, we also maintain that the drafting process of should be revisited entirely when there is greater harmony and consensus on the scope and necessity of an international cybercrime convention. The effectiveness of an international convention on cybercrime is already unclear, given that the handful of existing attempts at regional instruments already suffer from deeply conflicting standards. Our comments on substantive provisions are made with these considerations in mind.

Last but not least, we note that civil society must be given meaningful participation in a drafting process for this unprecedented criminal treaty.

Our key concerns with the Negotiating Document are as follows.

1. Unacceptable scale and scope of content- based offences

ARTICLE 19 notes that the Negotiating Document contains an unprecedented scale of offences - over thirty offences and half a dozen content-based offences. This goes beyond what States have

---

or coercion to suicide), Cluster 7 (sexual extortion and "revenge porn"), Cluster 8 (incitement, extremism), Cluster 9 (terrorism-related offences, narcotics distribution, and arms trafficking), Cluster 10 (money laundering and obstruction of justice) and Cluster 11 (agency and aiding/abetting provisions, and statutes of limitations).

[4] The Special Rapporteur on the rights to freedom of peaceful assembly and of association, Report on the rights to freedom of peaceful assembly and of association, A/HRC/41/41, 19 May 2019.

[5] The UN Global Programme on Cybercrime distinguishes between "cyber-dependent" crimes and "cyber-enabled" crimes. "Cyber-dependent" offenses require ICT infrastructure for them to be committed, while "cyber-enabled" offenses are traditional offenses that may be facilitated or aided by a computer, such as illicit drug purchases online or online money laundering.

[6] These guiding principles are threefold: cybercrime offences must require dishonest intent, serious harm, and be cyber dependent rather than cyber-enabled.

an obligation to prohibit under international treaties and extends well beyond any regional instrument. Moreover, the content-based offences, which are **cyber-enabled rather than cyber-dependent**, contain a number of problematic features for freedom of expression. These include offences that have not been previously implemented at an international level, and would create conflicts with international human rights obligations even without the use of a computer/digital technology. The offences do not leave room for other mechanisms for redress such as civil or non-legal remedies.

ARTICLE 19 recall that the Special Rapporteur on freedom of expression has clarified that the only exceptional types of expression that States are required to prohibit under international law are child pornography, direct and public incitement to commit genocide, hate speech; and incitement to terrorism.[7] While this is the case, there is no requirement that this be done in a *cybercrime* treaty; States have had ample opportunities to do so and have declined to adopt widespread prohibitions on most of these categories of information, due to the complex issues they raise.

As a starting point, criminal laws prohibiting dissemination of content are, by definition, restriction on freedom of expression, and therefore must be analyzed according to the tripartite test of restrictions enumerated under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). In framing future negotiations surrounding the Negotiating Document, ARTICLE 19 calls attention to the September 2011 report of the UN Special Rapporteur on the Right to Freedom of Opinion and Expression, which clarified the scope of legitimate restrictions on different types of expression online.[8] In that report, he identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;

- expression that is not criminally punishable but may justify a restriction and a civil suit; and

- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[9]

ARTICLE 19 notes that the bulk of the offences featured in the Negotiating Document fall under the third category; i.e., they might raise concerns for society or respect for others, but a broadly-worded, binding international criminal instrument is not the appropriate venue to address them. Instead, States should consider civil and non-legal instruments to properly balance the complex privacy and freedom of expression questions.

The provisions in question under the Negotiating Document include (in order in which they appear in the Negotiating Document):

[7] Report of the Special Rapporteur on FOE, A/66/290, 10 August 2011, para 18.
[8] *Ibid*.
[9] *Ibid.*

Copyright (Article 17)

ARTICLE 19 questions the need to include copyright-related criminal offences in a cybercrime instrument, as well as the compatibility of criminal sanctions for non-commercial copyright infringement with freedom of expression. Such sanctions have a chilling effect on the free flow of information and are a disproportionate interference with the right to freedom of expression.

In *The Right to Share Principles on Freedom of Expression and Copyright in the Digital Age*,[10] international experts recommend that criminal laws related to copyright infringement at a minimum conform to the following:

- Offences for copyright infringement may only be compatible with the right to freedom of expression and information if they have a clear legal basis, each element of the offence is clearly defined and the range of sentences available are proportionate to the seriousness of the offence.

- There is no public interest in bringing a prosecution in non-commercial copyright infringement cases. Therefore, law enforcement authorities should not initiate such prosecutions

- Prison sentences, suspended prison sentences, excessive fines and other harsh criminal penalties should never be available as a sanction for non-commercial copyright infringement.

We are concerned that no analogous protections apply or are even recommended in the Council of Europe Convention on Cybercrime (the Budapest Convention),[11] thus encouraging parties to this new instrument to adopt disproportionate restrictions criminalizing copyright infringement.

Child exploitation offences (Articles 18-21)

ARTICLE 19 notes that the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography[12] defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."

As 176 States are already parties to the Protocol, which provides for mutual investigative assistance, ARTICLE 19 questions whether a cybercrime treaty is a necessary place to impose additional content-based obligations.

[10] ARTICLE 19, The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age, 2013.
[11] The Council of Europe Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001.
[12] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, adopted on 25 May 2000 by Resolution A/RES/54/263 at the fifty-fourth session of the General Assembly of the UN.

Encouragement of or coercion to suicide (Article 23)
Article 23 of the Negotiating Document requires the prohibition of the "encouragement of or coercion to suicide, including of children, through psychological or other forms of pressure" using a computer system.

ARTICLE 19 is aware that there are numerous Internet websites, forums and chatrooms devoted to suicide-related information and discussions, as well as a number of reported case studies or articles linking individual suicides to this content. We also recognize that this content is causing an alarm, especially in relation to adolescents and young adults.

At the same time, we point out that the vague terminology and lack of intent requirement of this article raise serious freedom of expression concerns. It is not clear what "psychological or other forms of pressure" even means, and this could be potentially limitless. A number of distinct legal frameworks at the national level already exist; States apply varied standards on both the legality of suicide and the scope of counseling or aiding suicide.

It is unclear that it is even possible to harmonize the range of views on this issue, or that cybercrime legislation is the proper venue to do it.

Sexual extortion and non-consensual sharing of intimate images (Articles 24-25)
While non-consensual sharing of images is an extremely problematic phenomenon, ARTICLE 19 believes that addressing it in an international criminal instrument raises serious and complex issues in balancing freedom of expression and privacy rights. The types of issues presented in Articles 24-25 are ones of personal privacy, fundamentally distinguishing them from the core computer crime offences named in the first Clusters, and featured in existing regional instruments such as the Budapest Convention. The subtext for these prohibitions is protecting the privacy rights of victims; privacy rights are outlined in human rights instruments and data protection mechanisms. Thus, it follows that these provisions must be analyzed under these frameworks.

Existing terminology is vague and open to subjective interpretation, exposing it to abuse. As drafted, we are concerned that these provisions may inadvertently create problematic violations or be misused through provisions that are subject to widely varying interpretations. For instance, Article 25(3) vaguely provides that "No criminal liability is established if the non-consensual sharing has a legitimate purpose." It is unclear how far liability would extend and how individuals who simply re-post content would have reason to know (and thus be able to be "reckless") as to whether the person depicted gave consent. These questions are highly context-dependent and potentially subjective.

Definitions as to what is considered "intimate" or "explicit" may vary greatly, depending on the area and customs. Worse, these terms could be interpreted to discriminate against same-sex interactions, which have historically been targeted under obscenity and pornography laws.

Further, Article 25 would punish distribution or sharing of intimate images where one is "reckless" as to whether the person depicted gave consent; however, this question is often highly context-dependent. Some States do or have attempted to prohibit pornography, or discriminate against depictions of same-sex relationships under obscenity laws.

Existing human rights instruments and data protection mechanisms already address questions of personal privacy, and a cybercrime treaty where these conversations are not taking place is not the proper venue to consider them. We also believe that civil mechanisms, national oversight bodies, as well as regional instruments, could be more appropriate venues to consider.

This issue is compounded in jurisdictions where there has already been a push to criminalize pornography generally. For example, regional instruments such as problematic Arab Convention on Cybercrime broadly call for punishment of pornography; where this is the case, terminology like "explicit sexual activity" may be interpreted in sweeping manners.

Incitement to subversive or armed activities, extremism-related offences (Articles 26-27)

Articles 26 and 27 of the Negotiating Document provide for offences of incitement and justification of subversion and a number of hate categories.

ARTICLE 19 notes, for context, that Article 20(2) of the ICCPR provides that any advocacy of national racial or religious hatred that constitutes incitement to discrimination, hostility or violence is to be prohibited by law. However, it does not call for criminalization, and States are not obligated to criminalize such expression. The provisions as outlined do not meet, or even appear to consider, the high standards 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 (the Rabat Plan).[13]

The only regional cybercrime instrument that contains hate speech prohibitions is the Malabo Convention,[14] whose provisions do not reflect the Budapest Convention. The Malabo Convention does not appropriately consider or adhere to the Rabat Plan recommendations.

[13] The UN Rabat Plan of Action (2012) is authoritative guidance on interpreting Article 20(2) based on conclusions and recommendations emanating from four regional expert workshops organised by the OHCHR and adopted by experts in Rabat, Morocco, in 2012. The Rabat Plan outlines a six-part threshold test, taking into account (1) context, (2) status of the speaker, (3) intent to incite the audience against a target group, (4) content and form of speech, (5) extent of dissemination and (6) likelihood of harm.

[14] The provisions of Article 29(3)(1)(e) make it a criminal offence to: "Create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system." Article 29(3)(1)(f) states: "Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics." Article 29(3)(1)(g) states: "Insult, through a computer system, persons for the reason that they belong to a group distinguished by race,

It is not clear why a different standard from Article 20(2) of the ICCPR and from standards developed by regional courts[15] is proposed in the Negotiating Document. Further, these provisions only appear in a cybercrime instrument because they are merely cyber-enabled, i.e. done "by means of information and communications technology." It is unclear why they need to even be considered in this cybercrime context.

ARTICLE 19 recommends striking this provision. It merely requires calls for "illegal acts" motivated by broad terms such as "political" or "ideological." This is not narrowly limited to calls for serious violence, and thus does not comply with international standards.

Denial, approval, justification or rehabilitation of genocide or crimes against peace and humanity (Article 28)

Article 28 punishes dissemination of materials denying genocide or crimes against peace and humanity, using computer or information technology. Such restrictions are not justified whether or not they are cyber-enabled. The Human Rights Committee has observed that opinions which are "erroneous" and "an incorrect interpretation of past events" may not be subject to general prohibition. Any restrictions on the expression of such opinion "should not go beyond what is permitted" under Article 19(3) or "required under article 20" of the Covenant. The Special Rapporteur for freedom of expression also recently articulated the questionability of laws that criminalize the denial of the Holocaust and other atrocities.[16]

As a result, ARTICLE 19 recommends that this provision be stricken entirely.

Incitement, advocacy and justification of terrorism (Article 29)

Article 29 broadly includes various overly vague and problematic provisions under the umbrella of "terrorism" that ultimately restrict freedom of expression without articulating a legitimate aim, or being necessary to achieve that aim. For instance, it punishes "advocacy and justification" as well as "spreading of strife, sedition, hatred or racism," among other prohibitions that depend wholly on the highly subjective term "terrorism."

ARTICLE 19 is surprised and deeply concerned to even see a prohibition on "sedition" appearing in serious negotiations for a treaty imposing mandatory criminal sanctions. We observe that, generally speaking, sedition laws—which include laws that proscribe subversive activities—are undemocratic and infringe on the right to freedom of expression. They go beyond what is

colour, descent, national or ethnic origin, or religion or political opinion, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics."

[15] For information about regional standards on incitement, see for instance ARTICLE 19, Prohibiting incitement to discrimination, hostility or violence, 2012.

[16] 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.

strictly required to protect an interest, *even if* a legitimate interest exists and is provided by law. In most democracies sedition laws have been formally been rescinded.

We also observe that there is no universally agreed definition of terrorism under international law, which States have often leveraged to implement repressive measures.[17] The only instrument where a similar prohibition appears is in the Arab Convention on Combating Information Technology Offences. The Arab Convention does not articulate why that prohibition is necessary to achieve a legitimate aim, and ARTICLE 19 therefore does not endorse it. We also observe that States have declined to follow that Convention.

- At the same time, UN human rights bodies have highlighted the tension between freedom of expression and counter-terrorism measures.[18] *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security. Principle 2 states that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions, or to entrench a particular ideology.

- Further, the *Tschwane Principles on National Security and the Right to Information* also consider extensively the types of restrictions that can be imposed on access to information.

These principles articulate standards for the legitimacy and necessity of restrictions on freedom of expression on national security grounds. ARTICLE 19 is concerned that the current provision in the Negotiating Document leaves ample room for precisely what the Johannesburg and Tschwane Principles caution against - becoming a tool for illegitimate and unnecessary restrictions of expressive activity, ideologies, and dissent.

Comparison with other regional instruments

As noted above, the scale and scope of the proposed content-based offences is excessive. For comparison, the Council of Europe Cybercrime Convention (Budapest Convention) contains only nine offences, and only two content-based offences (related to copyright and child exploitation materials).

[17] See e.g. UNODC, Frequently Asked Questions on International Law Aspects of Countering Terrorism, 2009; see also UNODC, The Use of the Internet for Terrorist Purposes, 2012, para 49.
[18] See, e.g. General Comment no. 34, *op.cit*.

Other regional instruments, which have not gained widespread traction, set forth at most a handful of content-based offences:

- The Budapest Convention, contains **nine** offences. Apart from child exploitation materials and copyright, **none** of these offences are content-based.

- The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) contains **twenty-two** offences and **four** content-based offences, apart from child exploitation materials and copyright.[19]

- The Arab Convention on Combating Information Technology Offences contains **thirteen** substantive offences, including **three** content-based offences, apart from child exploitation materials and copyright.[20]

- The agreement on cooperation of the State Parties of the Commonwealth of Independent States in the fight against crimes in the field of computer information contains **five** substantive offences and **no** content-based offences.[21]

In contrast, the Negotiating Document contains **thirty-four** offences (which does not include sub-offences), including at least **six** content-based offences.[22]

**In this table, title and nature of offence are compared, to the extent that they track. However, the specific elements, including intent, of offences in the Negotiating Document may differ from regional instruments. **The chart includes only substantive offences, rather than aiding/abetting offences featured in Cluster 11. ***Some regional instruments may contain offences that do not appear in the Negotiating Document, for instance the Arab Convention's prohibition of "pornography" generally.*

		Negotiating Document	Budapest Convention	Malabo Convention	Arab Convention	CIS Agreement
6	*Illegal access*	X	X	X	X	X
7	*Illegal interception*	X	X	X	X	
8	*Interference with information*	X	X	X	X	X
9	*Interference with a system*	X	X	X		X
10	*Misuse of devices and programs*	X	X	X	X	X
11	*Forgery*	X	X	X	X	
12	*Fraud*	X	X	X	X	
13	*Theft*	X				
14	*Illicit use of electronic payment instruments*	X			X	

[19] African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014.
[20] Arab Convention on Combating Information Technology Offences, enacted in 2010. ARTICLE 19 does not endorse this instrument, due to the number of vague content-based offences included.
[21] State Parties of the Commonwealth of Independent States in the fight against crimes in the field of computer information, 1 June 2001.
[22] These offences include: encouragement or coercion to suicide (Article 23), non-consensual dissemination of intimate images (Article 25), 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). This list is greater when child exploitation and copyright offences are included.

15	*Violation of personal information*	X			X	
16	*Identity-related offences*	X				
17	*Infringement of copyright*	X	X		X	X
18	*Offences related to online sexual abuse or exploitation material*	X	X	X	X	
19	*Facilitation of child abuse material through a system*	X	X	X		
20	*Grooming or procuring of a child for sexual purposes through a system*	X				
21	*Cyberstalking of a child*	X				
22	*Involvement of minors in the commission of illegal acts*	X				
23	*Encouragement of or coercion to suicide*	X				
24	*Sexual extortion*	X				
25	*Non-consensual dissemination of intimate images*	X				
26	*Incitement to subversive or armed activities*	X				
27	*Extremism-related offences*	X		X		
28	*Denial, approval, justification or rehabilitation of genocide or crimes against peace and humanity*	X		X		
29	*Terrorism-related offences*	X			X	
30	*Offences related to the distribution of narcotic drugs and psychotropic substances*	X			X	
31	*Offences related to arms trafficking*	X			X	
32	*Illegal distribution of counterfeit medicines and medical products*	X				
33	*Money-laundering*	X			X	
34	*Obstruction of justice*	X				

ARTICLE 19 calls into question the need to require universal adoption of measures and associated procedural obligations that have never even been mandated at a regional level.

2. Problematic inclusion of privacy-related offences

The provisions of Articles 15 and 16, which provide for identity- and privacy-related offences may criminalize a broad range of conduct in ways that not only raises freedom of expression issues, but also conflict with existing data protection frameworks. Namely, Article 15 punishes the "accessing" or "sale" or "making available" material "containing personal information about a person" where it is done with intent of "obtaining a financial benefit" without consent. Article 16 requires the prohibition of obtaining or receiving passwords, or the "fraudulent" or "dishonest" use of electronic signatures or unique identifiers.

These provisions are problematic because they are vague and are not necessary to pursue a legitimate aim; specifically restricting the publication of "personal information" is not a legitimate aim. They also attach criminal liability without requiring dishonest intent or serious harm for all elements, and include numerous terms that are overly broad and undefined.

ARTICLE 19 also notes that offences criminalizing the dissemination of personal information can be disproportionately used to limit the public's right to know regarding public figures. For instance, it can be easily argued that newspapers or other publications which rely on sales or advertising for their dissemination stand to obtain a "financial benefit" on anything they report. While individuals maintain a right of privacy and reputation, the right of privacy of individuals acting in public positions must be balanced against the right of the public to be made aware of activities about their government. Any broad prohibitions on reporting on private lives may strike this balance in a manner that undermines the public's right to know.[23]

Further, entire advertising industries exist based on the collection and sale of personal information; it is unclear that Article 15 is drafted in mind with the realities of modern electronic commerce and existing data protection debates that occur around this.

Moreover, provisions of Article 16 risks prohibiting legitimate security research which may often attempt to access systems for the purpose of identifying key vulnerabilities in the public interest. It appears to be duplicative of Article 10, misuse of devices and programs, which criminalizes the dissemination of passwords or access credentials.

3. Repetitive provisions of the Negotiating Document

ARTICLE 19 also notes that the Negotiating Document is repetitive and provisions re-appear in numerous instances. Some examples of this include Article 10, which prohibits making available passwords or access credentials, and Article 16 also punishes distribution of passwords or credentials. Additionally, Article 27 prohibits distribution of materials calling for, among other things, racial, ethnic or religious hatred, while Article 29 also prohibits "spreading of strife, sedition, hatred or racism."

We recommend striking these provisions entirely. We draw attention to the fact that these repetitive elements further call into question the quality control of the inputs into a drafting process which has grave implications for freedom of expression.

4. Problematic procedural provisions (Articles 47-48)

While this analysis does not address procedural aspects entirely, ARTICLE 19 does note that provisions that mandate the assistance of service providers threaten to be used to circumvent judicial warrant requirements by allowing investigators to simply compel any individual to disclose information they seek. The vagueness of "assist" is especially problematic because it could mean anything from the forced disclosure of records, to commandeering service providers to become extensions of law enforcement. That might entail forcing providers to re-write

[23] ARTICLE 19's 2017 Defining Defamation principles further discuss the factors that should be considered in protecting the reputation of individuals.

computer code to insert security 'back doors' into their products or engage in active surveillance of users. It may also apply to compelled assistance to decrypt communications.

Further, we note that the 2015 report of the Special Rapporteur on freedom of expression[24] stipulated, in the case of orders for compelled assistance to decrypt communications, that such orders should be necessary and the least intrusive means available, based on publicly accessible law, clearly limited in scope focused on a specific target, and implemented under independent and impartial judicial authority.

However, Articles 47 and 48 of the Negotiating Document, covering real-time collection and interception of content data, reference precisely this type of language. They require providers within "existing technical capacity" to access content, among providing other assistance.

ARTICLE 19 's recommendations

In the light of foregoing ARTICLE 19 has the following recommendations to the Ad Hoc Committee:

- Human rights safeguards, including clearly relevant and binding international instruments such as the ICCPR, must be specifically named in the draft. The draft instrument explicitly restricts freedom of expression, but only calls for adherence with "applicable international human rights law" (Article 5). This lack of specificity of unacceptable. Any cybercrime treaty should be limited to cyber-dependent offences (Clusters 1 and 2).

- Cyber-dependent offences must require dishonest intent and serious harm.

- Additional sanctions for access to confidential government information must be stricken, as these are historically abused to prevent embarrassment and exposure of misconduct (Article 6).

- The content-based offences should be stricken entirely (Clusters 8, 9). This instrument attempts to reinvent the wheel in direct conflict with standards that have already been well-settled under international law.
    - The provisions on non-serious (merely illegal) incitement based on political ideology, racism, or hate speech provisions do not comply with the UN Rabat Plan of Action, which lays out a six-factor test and was already the result of a long drafting process across many stakeholders.

    - Prohibitions on genocide denial have been named as deeply problematic by the Special Rapporteur on FOE and Human Rights Committee.

[24] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 22 May 2015, A/HRC/29/32.

- Prohibitions on terrorism-related offences are vague and fail to articulate a legitimate aim. There are also no internationally agreed definitions of terrorism.

- Identity-related offences (Clusters 3 and 7) should be removed from the scope of a cybercrime treaty and addressed in existing national and regional data protection instruments.

- Copyright (Article 17) should not be addressed in an international criminal framework, where civil and other remedies are often and usually more appropriate to consider. This article should be stricken.

- Encouragement of suicide should be stricken as a cybercrime offence (Article 23); while the trend of online encouragement is alarming and troubling, States have a wide range of views on this issue which are likely impossible to harmonize, and the current provision includes vague and undefined provisions such as "psychological or other forms of pressure."

- Procedural provisions (Articles 47, 48) must be amended to explicitly protect personal data, require judicial review for searches and interception of data, and protect service providers from being forced to become extensions of law enforcement by requiring forced decryption or security "backdoors."

- Repetitive provisions (such as Article 10, and Article 16 or Article 27 and Article 29) should be stricken entirely. These repetitive elements further call into question the quality control of the inputs into a drafting process which has grave implications for freedom of expression.