ARTICLE 19's Recommendations for the UN Cybercrime Convention

As the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes commences its first session, ARTICLE 19 presents its position on the development of a comprehensive international convention on cybercrime (the UN Convention). ARTICLE 19 is not persuaded there is a need for an international convention on cybercrime. We are concerned that such a convention would be subject to abuse, perpetuating many of the repeated and existing problems we have seen in many 'cybercrime' laws around the world. Further, an international convention would threaten to implement global investigatory and mutual legal assistance obligations without simultaneously universalising regional human rights and data protection measures, leading to lopsided availability of remedies and undermining existing measures on the regional and national levels. If the UN Convention is to proceed, the goal should be to combat the use of information and communications technologies for criminal purposes without endangering the fundamental rights of those it seeks to protect, so people can freely enjoy and exercise their rights, online and offline. Any proposed convention should incorporate clear and robust human rights safeguards. This briefing addresses some of the key issues surrounding the Convention, as well as our key recommendations for the process.

Background to the Convention

The UN General Assembly in 2019 established an open-ended Ad Hoc intergovernmental committee to explore the development of a comprehensive international convention on cybercrime. In May 2021, the General Assembly adopted Resolution 75/282, titled "Countering the use of information and communications technologies for criminal purposes" which provided an outline for the Ad Hoc Committee to proceed over a series of meetings. The Committee's objective is to present a draft convention to the General Assembly at its seventy-eighth session. The Ad Hoc Committee held its first meeting on 24 February 2022.

In July 2021, the Russian Federation presented a draft Proposal to the Chair of the Ad Hoc Committee (the Russian Proposal). In October, the EU and its Member States presented its draft position regarding the Convention and in November comments on the upcoming first session. Numerous Member States have also submitted comments in anticipation of the first session to be tentatively held in New York in January 2022.

ARTICLE 19's experience with cybercrime laws

ARTICLE 19 has extensive experience monitoring the impact of emerging cybercrime laws on freedom of expression. We have worked worldwide to analyse numerous proposed and existing cybercrime measures, including legislation in Bangladesh, Brazil, Cambodia, Ethiopia, Iran, Kenya, Mexico, Pakistan, Sudan or Thailand. These types of laws have also comprised an important component of submissions in the Universal Periodic Review of UN Member States such as Sudan, Cambodia, and Tanzania. ARTICLE 19 in 2015 submitted comments to the UN Special Rapporteur on freedom of expression for his comprehensive report on anonymity and encryption.

ARTICLE 19 has also closely followed the process surrounding the current Proposal for several years, in 2019 issuing an open letter to the UN General Assembly with a coalition of civil society organisations

voicing concerns regarding the measure. ARTICLE 19 also issued the comments on the Russian Proposal for the Convention.

Based on our work, we see several trends with respect to cybercrime laws:

- First, **criminalising ordinary activities through the application of cybercrime laws** is a growing, problematic trend in many countries around the world. Broad and vaguely-defined provisions that do not require "serious" harm or "dishonest" intent may be used to criminalise legitimate expressive activities involving computers, content-based conduct, or activities such as security testing, research, and the sharing of passwords for academic or personal use. Further, a public interest defence is necessary to prevent the abuse of cybercrime laws against individuals or organisations conducted in legitimate security or academic research, engaging in digital security activism, or who expose violations of rights, corruption, or serious waste, abuse, or fraud.

- Second, numerous terms appearing in cybercrime laws **are routinely vague and subject to abuse**. These include terms such as "unauthorised" or "without authority" (typically not clearly defined in law, and are ambiguous as to who is required to provide relevant authorisation or authority); 'critical information systems' or 'protected systems' (referring systems that are essential to society or defence, but in reality, are often applied loosely and subject to abuse in order to protect public authorities from criticism).

- **Procedural provisions** may be implemented in a manner that undermines human rights protections for privacy and due process. For instance, investigatory measures that broadly require ICT providers to "assist" or "enable" investigations can be used to attempt to force companies to become extensions of law enforcement in problematic ways. These include forcing providers to re-write computer code to insert security 'back doors' into products or engage in active surveillance of users. Further, 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.

It is crucial that these types of problems are not replicated in the Convention.

ARTICLE 19's recommendations

ARTICLE 19 reiterates that we consider an international convention on cybercrime to be unnecessary and ill-advised. We provide the following recommendations with the understanding that the drafting process will proceed nonetheless. As the Ad Hoc Committee commences its work drafting the UN Convention in the coming months, it is vitally important to apply a human rights-based approach to ensure that the proposed text is not used as a tool to stifle freedom of expression, infringe on privacy and data protection, or endanger individuals and communities at risk. The important work of combating cybercrime should be consistent with States' human rights obligations set forth in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights instruments and standards. In other words, efforts to combat cybercrime should also protect, not undermine, human rights.

Based on our experience in regional and international advocacy, with the cybercrime laws and the problems in the Russian Proposals, ARTICLE 19 offers the following ten recommendations for the drafters of the Convention.

Recommendation 1: Scope of the Convention should be narrow and cybercrime must not be used as a pretext to prosecute content-based offences
From a human rights perspective, the scope of the UN 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.

As we outlined earlier, several cybercrime laws contain vaguely worded and overbroad speech offences, such as those related to terrorism and extremism, disinformation, 'hate speech' or morality. These laws are then frequently misused to imprison those critical of authorities or dissenting voices, or even block entire platforms.

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.

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, in the reports of the UN Special Rapporteur on freedom of expression and other standards in this area.

Recommendation 2: Criminal sanctions in cyberspace must be strictly limited in number, scale, and scope.
From 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 that have been replicated elsewhere (e.g. the UK Computer Misuse Act 1990) and to our knowledge there have been no concerns raised that such countries are not properly equipped to deal with cybercrime. 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 overinterpretation and abuse.

Recommendation 3: 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 any harm or risk of harm to a legitimate interest in engaging in the proscribed activity is outweighed by the public benefit in the activity. 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.

Numerous expressive activities in the public interest might involve access to computer systems and data, such as security and academic research, or whistleblowing to expose government or private wrongdoing. A public interest defence is crucial to ensure the protection of these types of activities, as

well as the activities of journalists, civil society, and academics who may rely on or utilise information or data accessed in the public interest.

Recommendation 4: 'Unauthorised access' offences must be defined by specifying the scope of what is meant by 'authorised' and who determines that authorisation

The term "unauthorised" may raise serious issues as a matter of legal precision and has important implications for freedom of expression, particularly government and public sector whistle-blowers. The term on its face does not require bypassing technical restrictions or engaging in 'hacking.' Nevertheless, the term is used frequently in cybercrime legislation with no further definition.

The key question for any mention of the term "unauthorised" is who exactly is responsible for providing authorisation, and under what terms it is provided. Further, it is often unclear whether authorisation refers to the access or the use of a system. In other words, is a user who possesses authority to utilise a system running afoul of that authorisation simply by using information or data in a manner that is not approved? Is access "unauthorised" if a government employee accesses a database in order to provide evidence of waste, fraud, or corruption to a journalist? Finally, can 'unauthorised access' provisions be used to punish a journalist as an accessory for their relationship with a source who obtained journalistic materials via unauthorised access to a computer system?

This distinction, though it may appear technical, has important implications for freedom of expression. Whistle-blowers who may have every right to access systems but are using that information in a manner that a government may wish to retaliate for. Thus, it is crucial to conduct a meaningful inquiry into state of mind, by requiring that access be done not only without authorisation, but by infringement of security measures, and with dishonest intent and that the person had a "reasonable belief" that access to data would expose wrongdoing set out in the law and that the concern is in the public interest.

Recommendation 5: Cybercrime offences must hinge on state of mind, rather than the specific technologies used

Like many tools, technologies are dual-use and it is in the nature of technology that it can be used both for legitimate and illegitimate purposes. Attempting to define 'malicious software' is difficult as it is akin to calling a tool 'malicious.' It depends on the manner in which it is used. Most companies would know that the software they manufacture or sell could be used for dual purposes, including for the purposes of unauthorised access to computer data and systems. For this reason, specific intent to commit offences, rather than mere possession or use of certain technologies, must be required.

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). DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be used after sale. 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 engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use."

Additionally, double standards must be avoided, and governments must not criminalise technologies only to turn around and purchase them for themselves. The Special Rapporteur for freedom of expression expressed that he was "most concerned" with the commercial spyware and international

surveillance market, which includes over hundreds of companies marketing and selling products to governments.

Recommendation 6: The use of encryption and anonymity must not be criminalised
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 or 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. For instance, in his 2015 report on encryption and anonymity in the digital age to the UN General Assembly, the Special Rapporteur on freedom of expression stated that restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law, as both are essential components for the exercise of freedom of expression online. The Rapporteur noted that a "surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protestors in many countries around the world." In a follow-up report in 2018, the Special Rapporteur observed how, since his previous report, numerous States including Pakistan, Iran, and Turkey, have adopted criminal laws banning the use of, and dissemination of, encryption and anonymity technologies.

Similarly, the European Court of Human Rights recently held that ICT companies have an interest in keeping their users anonymous so as to help promote the free exchange of ideas and information as covered by Article 10 of the ECHR. In accordance with this, tools that provide robust rights to privacy should not be met with suspicion, as they are integral to the realisation of human rights online.

Recommendation 7: Information and communication technology providers must not be forced to become extensions of public authorities
Investigatory measures that broadly require information and communication technology providers to "assist" or "enable" investigations can be used to attempt to force companies to become extensions of law enforcement in problematic ways. These include forcing providers to re-write computer code to insert security 'back doors' into products or engage in active surveillance of users.

Provisions that mandate the assistance of ICT companies 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 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, the 2015 report of the Special Rapporteur on freedom of expression 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 scrutiny.

Recommendation 8: Mutual legal assistance and extradition obligations must preserve international, regional, and national due process safeguards.
A major issue with the concept of an international convention in the area of cyberspace, where a wealth of expressive activities occur, is the possibility of individuals and organisations effectively losing the procedural ability to enjoy rights and/or remedies under national and regional instruments. 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 those of regional instruments and accompanying courts such as the European Court of Human Rights, the Inter-American Court of Human Rights, or the African Court on Human and Peoples' Rights. For example, more recently Turkey enacted a data law that provides far less protection than that enjoyed by EU Member States, leading to legal questions as to the data control obligations of entities that maintain a presence in both jurisdictions. Without proper safeguards, and without adequately connecting any convention to the protection of human rights instruments, the substantive rights and enforcement under such a convention would vary greatly purely based on geography and jurisdiction.

As one scholar of mutual legal assistance has argued, "by profoundly increasing the scope of law enforcement data collection powers, while simultaneously depriving individuals of protections against abuse of those powers, poorly designed MLAT reform policies will potentially result in the surveillance of states worldwide." For this reason, the availability of strong procedural human rights protections must be weighed in any grant of investigatory powers or mutual legal assistance obligations.

Recommendation 9: Interference by public authorities with non-government computer systems or equipment should be presumptively prohibited

Cybercrime laws are often written from the perspective of holding individuals, rather than governments, accountable. We have argued previously that the trend of government interference with computer systems or equipment, known as "government hacking," is one of the greatest present threats to freedom of expression. Such interferences, whether they be in the form of surveillance, intrusive software, or exploiting vulnerabilities, threatens to have a chilling effect on online expression. This is because individuals may opt to self-censor out of concern that their communications may be tracked. The IACHR Special Rapporteur for freedom of expression has addressed the close link between "the violation of the communication privacy [which] has a chilling effect and hampers the full exercise of the right to communication."

The Special Rapporteur for freedom of expression also insisted that States take measures to prevent commercialisation of surveillance technologies, including research, development, trade and export, on account of their ability to facilitate violations of rights. His successor recommended that States implement public mechanisms for approval and oversight of surveillance technologies, arguing that mere judicial authorisation of government use of surveillance technologies is necessary but insufficient. In 2018, the Special Rapporteur also observed the extent to which civil society has uncovered evidence of State-based surveillance, manipulation of data, and interference with computer systems in order to undermine dissent.

Since State-sponsored or government hacking substantially interferes with human rights it should be presumptively prohibited in the Convention. The Convention could specify that only in the limited cases where a government can overcome that presumption, solely for the purposes of surveillance or intelligence-gathering, human rights safeguards must be put in place, including robust public oversight and access to an effective remedy.

Recommendation 10: Meaningful participation of all stakeholders in the drafting process, including civil society, must be ensured

As we have already stated together with our partners, the Ad Hoc Committee must actively include civil society organisations in consultations — including those dealing with digital security, human rights and groups assisting vulnerable communities and individuals. This should be done through a simplified accreditation process for participation, ensuring that modalities for participation recognise the

diversity of civil society, and proactively sharing comprehensive and up-to-date information about the process and the state of negotiations.

This recognition should extend to an actual consideration of their inputs. The Ad Hoc Committee should ensure that the concerns and recommendations raised by these various stakeholders inform and influence the drafting process.