NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

17 January 2022

OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes

In advance of the first meeting of the United Nations Ad Hoc Committee tasked with elaborating the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes scheduled later this month, OHCHR highlights the need to put human rights protection at the centre of the Ad Hoc Committee discussions.

Undeniably, cybercrime endangers the rights of people around the globe. A universal convention under the auspices United Nations has the potential to reduce impunity of cybercriminals by harmonising approaches to criminalisation, provide effective investigatory frameworks, and facilitate cross-border data exchange. At the same time, provisions regulating cybercrimes and their application may pose significant human rights risks, as evidenced by the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly.

The Ad Hoc Committee meetings provide an opportunity to develop, transparently and inclusively, a new convention that would elevate the level of safeguards and protections in criminal justice and reduce the risk of exploiting cybercrime laws for arbitrary restrictions of rights and freedoms. However, to seize this opportunity, the parties should see integrating human rights into the process as fundamental.

The recommendations below aim to address human rights issues related to the main pillars of a possible future cybercrime convention: substantive criminal law and criminalization, procedural criminal law, mutual legal assistance, and the process of negotiations itself. Addressing these issues will assist clearly framing the deliberation process in human rights terms.

1. Recommendations concerning the deliberation process

Inclusive and meaningful civil society participation in the discussions and negotiations is essential. Diverse civil society should be able to meaningfully participate in the meetings of the United Nations Ad Hoc Committee**.** Civil society organizations have played an essential role in developing cybercrime frameworks at national and regional levels, raising human rights concerns, and helping to minimize the potential for human rights violations. It is key to have civil society organizations' views throughout the drafting process, by facilitating access to information and to all relevant meetings and discussions, online and offline. Safe, inclusive and meaningful participation of diverse civil society will ensure that relevant human rights concerns

are raised and will enable transparency and accountability in relation to both the process of negotiations and the implementation of any future cybercrime convention.

2. Recommendations on substantive criminal law provisions

Criminalizing offences committed using information and communication technologies is a necessary and powerful instrument to protect the human rights of victims of cybercrime. At the same time, the use by some States of substantive criminal law to limit conduct that is legitimate under international human rights standards, taking steps, for example, to silence political opponents, oppress peaceful protests, prosecute human rights defenders and hamper the work of journalists, is well-documented. It is, therefore, necessary to ensure that any future international instrument on cybercrime cannot be interpreted to justify such steps.

Focus on core cybercrimes. In OHCHR's view, any future cybercrimes convention should focus on offences that are specific to computer data and systems and require explicit criminal law provisions due to the lack of protection provided by existing criminal law. On that basis, only a narrow set of offences inherent to cyberspace should be criminalized, such as crimes against integrity, confidentiality and availability of data and systems, misuse of devices for the purpose of committing these crimes, and, where appropriate, a limited number of specific computer-related offences, such as computer fraud and forgery.

In addition, a future agreement on cybercrime should avoid including offences based on the content of online expression ("content offences"). Cybercrime laws have been used to impose overly broad restrictions on free expression, for example by criminalizing various online content related to extremism, terrorism, public morals, or hate speech. A future cybercrime convention should expressly ensure that its provisions neither apply nor could be interpreted to apply to improperly restrict conduct protected under human rights standards.

The scope of criminalization should be clear and focused, rather than open to broad interpretations. The principles of legality and legal certainty require criminal law provisions to be publicly accessible, clear, and precise in scope, so that individuals can reasonably ascertain which conduct is prohibited and adjust their behaviour accordingly. Vague and imprecise definitions of offences leave room for arbitrary interpretations and risk infringement of human rights. To reduce these risks and to avoid over-criminalization, any international instrument should define criminalised conduct in a clear and narrow manner. Cybercrime provisions without a requirement of intent to commit an act have proven problematic in the past.

The legitimate work of civil society organisations, journalists, and other actors pursuing the public interest should be protected. Cybercrime laws can be used to restrict lawful activities of a wide range of civil society actors which are essential for transparency, accountability, and the protection of human rights in democratic, pluralistic societies. Overbroad or vague criminalization of access to data and systems can limit and penalize legitimate access to information and its disclosure by, among others, journalists and whistle-blowers. Poorly-constructed offences against confidentiality, integrity and availability of data also risk impeding the work of

cybersecurity researchers and have a chilling effect on discovering information system vulnerabilities, putting users and businesses at higher risk of cybercrime. The parties to negotiations of a cybercrime convention thus should ensure that the provisions of a future international agreement do not hamper legitimate activities, notably of journalists, human rights defenders, cybersecurity researchers, and cannot be used to prosecute whistle-blowers.

3. Recommendations on procedural and investigatory powers

Effective procedural frameworks that enable access to electronic evidence in a timely manner are crucial for tackling the problem of cybercrime. However, access to digital data in criminal investigations can also have a detrimental impact on human rights when covertly or intrusively procured, and potentially allows for the collection of a large amount of sensitive information beyond the scope of a particular case, interfering with the privacy of suspects as well as third parties. As procedural frameworks developed for cybercrime can be used to obtain evidence in investigations of any alleged crime possessing digital traces, strong human rights protections regarding access to and use of such tools are key. Insufficient safeguards could affect the integrity of and public confidence in criminal justice globally, enabling human rights violations and abuses both at the national level and across borders. Any future convention should include robust safeguards related to relevant procedural powers.

Investigative and procedural measures that may affect human rights should be necessary and proportionate. Criminal investigations typically entail restrictions of rights. Such restrictions, for instance to the right to privacy, can only be imposed to pursue a legitimate aim. While the investigation of crimes constitutes such a legitimate aim, it is essential that any investigative or procedural measure that constitutes a limitation on human rights, is necessary and proportionate to achieving the aim and is the least intrusive approach possible. In particular, a future cybercrime convention should ensure that particularly intrusive measures, such as the interception of content data or other forms of acquiring the content of communication are limited to the investigation of serious crimes only.

Investigative measures should be expressly limited in scope and duration. A future cybercrime convention should take care to avoid risks of exposing individuals are subjected to arbitrary surveillance. Any future convention should require parties to establish clear scope and temporal limits for ongoing measures concerning any form of access to, production or acquisition of any types of private communications and personal data in criminal investigations, and to put in place measures to ensure those limits are adequately respected and enforced.

Procedural measures should be grounded in reasonable suspicion be sufficiently targeted. A cybercrime convention should also include provisions that prevent overbroad interferences with rights. For example, procedural powers should always be grounded in reasonable suspicion that an individual has committed or is committing a criminal offence and should target only a specific, justified number of persons, such as suspects and third parties relevant to the investigation. Such provisions are necessary to avoid legitimizing bulk collection of data in the absence of any crime or indiscriminate monitoring, constituting privacy intrusions that are not permissible under international human rights law.

Judicial authorisation and ongoing supervision is essential for covert investigatory measures. Covert access to and collection of any type of private data in criminal investigations represents a significant interference with the privacy of suspects and other parties. It is widely recognized that the collection of metadata itself reveals sensitive information about individuals, making such approaches at times as intrusive as access to the content of communications themselves. The absence of robust safeguards in the application of covert investigatory measures can undermine privacy and have a chilling effect on freedom of expression, freedom of association, and other human rights.

Interference of investigative and procedural measures with human rights, including the right to privacy, requires the existence of independent and impartial oversight before, during, and after the application of such measures. Such protection is best guaranteed by mandating independent judicial control over the application of such steps by law enforcement agencies or other executive authorities. Any future cybercrime convention should therefore conceive any exceptions to this rule narrowly, such as in acute time-sensitive circumstances, and in any event require subsequent judicial review within strict timeframes. Covert investigatory measures should also be subject to ongoing oversight, including judicial supervision and control by other independent bodies.

Search and seizure methods should be subject to robust safeguards and independent oversight. Personal electronic devices frequently contain highly sensitive personal information not only about their user/owner, but also many third parties. Search and seizure measures regarding such devices therefore can carry even greater risk to human rights, including the right to privacy, than covert access to data on a particular individual. It is essential that a possible cybercrime convention recognizes the need for additional robust safeguards for search and seizure of personal devices and ensures that these measures are subject to sufficient independent oversight and control.

Protect privileged communications, such as attorney-client communications. Protection of privileged communications between protected persons foster important public interests, such as, in the attorney-client context, protection of the right to a fair trial, amongst other interests. The lack of such protection can deprive suspects and other persons of effective legal representation of their interests. A future cybercrime convention should provide robust safeguards for the confidentiality of legitimate attorney-client and other privileged communications, in accordance with international human rights law and standards. Furthermore, to guarantee adequate protection of sensitive data, a future agreement on cybercrime should also consider additional safeguards to protect communications of specific professions commonly regarded as appropriately attracting additional legal protection through privilege rules, such as medical professionals and journalists.

4. Recommendations on mutual legal assistance mechanisms

Any international cybercrime convention should ensure that mutual legal assistance mechanisms cannot be used for the exchange of evidence in criminal investigations in a manner that jeopardizes human rights. A system of robust safeguards should underpin provisions on cross-border exchange of information in criminal

investigations, guaranteeing proper scrutiny of requests and enabling refusal of requests for cooperation on human rights grounds.

Mutual legal assistance should be subject to a dual criminality requirement. The dual criminality requirement mandates that acts are considered a crime in both jurisdictions at issue when assistance is provided to ensure the principle of legality is upheld. This requirement is particularly relevant to a future cybercrime convention, in which mutual legal assistance provisions may go beyond the criminal offences included in the scope of the convention itself to other crimes requiring electronic evidence.

Mutual legal assistance requests should be subject to the approval of competent authorities in both States. To guarantee the protection of human rights in cross-border exchange of electronic evidence, a strong level of scrutiny is necessary for data requests in mutual legal assistance procedures. In executing mutual legal assistance requests, states should apply the same level of safeguards as provided under domestic laws for the same investigative measures. Any future convention should ensure decisions about producing data upon request for mutual legal assistance are subject to safeguards guaranteed in both jurisdictions and should need to be approved by competent authorities in both the requesting and executing state.

State should evaluate requests to ensure compliance with human rights. The obligation to provide mutual legal assistance should be subject to strict compliance with applicable human rights standards, and should include a responsibility for an executing State to evaluate the request for compatibility with human rights standards, and to refuse the request on such grounds where applicable. Refusal of mutual legal assistance on such grounds would also include cases in which there are substantial reasons to believe that a person is being investigated or prosecuted on the grounds of political opinions, religious beliefs, nationality, sexual orientation, gender, race, or ethnic origin, or other prohibited ground of discrimination, or in respect of conduct which is protected under international human rights law.

Industry or other private parties should not have final decisional authority whether or in what scope data is produced in response to a request for mutual legal assistance. Cooperation with communication providers and other private parties is essential for the timely production of electronic evidence. However, private parties will generally not have sufficient capacity to assess the legality and validity of requests for data issued by foreign law enforcement authorities. Public authorities should have the responsibility to perform the essential task of scrutinising mutual legal assistance requests to sufficiently protect human rights in cross-border criminal investigations.

_____