Access Now contribution to UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes:

On Criminalization, Procedural measures and Law Enforcement

8 April 2022

Access Now is an international organization that defends and extends the digital rights of users at risk around the world; in furtherance of this, we operate a global Digital Security Helpline for civil society to mitigate specific technical threats. We are a member of the Forum for Incident Response (FiRST), the leading global incident response network, and also helped co-found CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the incident response capabilities of its members and share information on threats that affect NGOs, journalists, and human rights defenders around the world. Our contribution here provides our inputs to the Ad Hoc Committee's work on proposing provisions on Criminalisation, and Procedural Measures and Law enforcement.

Criminalisation

1. **The proposed treaty should limit itself on the criminalisation of a core set of cyber-dependent crimes**

International harmonization efforts must absorb the lessons around national practices, including on focusing on cyber dependent crime versus cyber enabled crime. As the discussions in the first substantive session and intersessional of the Ad Hoc Committee demonstrated, ensuring the true uptake and implementation of a new international legal instrument in this space will require focusing on the elements where participating states have clear consensus and agreement - a core understanding. That requires us to focus on core cybercrime issues; efforts to address and ensure harmonized criminalisation of cyber-dependent crime. The Ad Hoc Committee must avoid catch-all, over-expansive approaches towards criminalisation in cybercrime laws.

Advancing a harmonized, human rights respecting, internationally adopted approach to combating misuse of ICT to facilitate cybercrime requires us to be careful, and arguably, err on the side of caution and consensus. Even a limited approach around cyber dependent crimes can have impacts on human rights and the information security community that makes more robust cybersecurity possible.

Access Now submits that there are four core cyber-dependent crimes that should be the focus of any criminalisation effort in this proposed treaty:

1. Access to or interference with computing systems without authorisation and with criminal intent;
2. Interfering with with or damaging computer data and systems without authorisation and with criminal intent;
3. Illegal interception of communications;
4. Misuse of devices with the intent of committing one of these above offenses

We do not recommend that the principal text of the proposed treaty should initially seek to outline cyber-enabled crimes as part of its core criminalisation articles. Doing so would likely result in a breakdown in international consensus, and also likely increase the danger of the treaty's criminalisation chapter negatively impacting human rights. If participating states believe that certain crucial cyber-enabled crimes should also be part of the enhanced international legal cooperation sought to be facilitated by the treaty, they should seek to be selective rather than over-expansive. One potential model could be for states to indicate where cyber-enabled activities are criminalized at the national level, and create a compendium of such domestic criminalisation definitions in order to facilitate increased international agreement and understanding around where dual-criminality on cyber-enabled crime may already exist amongst states.

2. Content-related measures should not be included in the proposed treaty

Far too often, we have seen the design and implementation of cybercrime laws - particularly around criminalisation - have a harmful impact on legitimate activities and intrude upon protected human rights. In particular, over broad definitions of cybercrime and adding content or political speech related provisions in the definitional ambit of cybercrime laws in several states. Decisions around the approach and scope of criminalisation in cybercrime legal frameworks have a direct bearing on human rights, particularly around potential criminalisation of protected speech and legitimate online behavior.

Crimes pertaining to content - and content regulation issues more generally - should be strictly excluded from the purview of the proposed treaty. We therefore also caution against including any measures seeking the inclusion of provisions on criminalizing mis/dis/malinformation within this instrument.

3. **Criminalisation efforts on cybercrime also need to help ensure that the cybersecurity community is enabled and not harmed**

We strongly recommend that the Ad Hoc Committee ensure that any proposed cybercrime treaty requires a sharper focus on "intent" and other related standards when addressing unauthorized access to ICT systems and networks.

It is now globally recognised that cybercrime laws and their implementation can sometimes unfortunately result in unlawful surveillance, improper persecution, or harassment of security researchers; the very people who help ensure our cybersecurity is enhanced. As we outlined in the first substantive session, we believe that the Ad Hoc Committee must endeavor to protect the humans critical to ensuring global cybersecurity, i.e. the information security research community that helps reveal and fix vulnerabilities in ICT systems exploited by criminals and malicious actors.

The Ad Hoc Committee must therefore ensure that it does not create international legal frameworks that generate uncertainty for or directly enable the persecution of the information security community. We must ensure that we create clear requirements around "intent" when criminalizing unauthorized access, and that national laws across all agreeing states require a heightened intent requirement that is beyond mere knowledge in cases of unauthorized access to computer systems or databases. We also suggest that the Ad Hoc Committee deliberate on the inclusion of a specific article that requires states to ensure that their criminalisation of the core cybercrimes noted above is subject to a good faith exception for lawful security research. In effect, requiring signatory states to implement this good faith exception to the criminalisation article can help ensure that legitimate information security research - crucial to revealing and fixing the ICT vulnerabilities that are often exploited for cybercrime - has a legal backstop it can rely on. A positive obligation must be cast on states to help protect and encourage the security researcher community.

Additionally, the proposed treaty should also indicate that states strive to ensure that authorities must not create hostile environments for those who speak up with concerns about information security; specifically, they must seek to not persecute, discredit, or defame individuals who express their concerns about computer systems, security mechanisms, databases, and other related tools.

<u>Procedural measures and law enforcement</u>

4. **Ensure that strong safeguards to protect human rights are incorporated on procedural measures and international cooperation provisions**

International cooperation measures are crucial, but can also have the danger of impacting privacy and other fundamental human rights. Any international legal framework on cybercrime cooperation must

therefore ensure appropriate accountability, remedy, authentication, and oversight in legal assistance - including a clear role for judicial institutions. States participating in any such framework must commit to public transparency reporting with clear, easily accessible information covering the way users' data records are shared amongst law enforcement across jurisdictions and by notifying users when their data are accessed. Data sharing initiatives must adhere to principles of dual-criminality, proceed in writing under standard protocols, and raise, not lower, protections against arbitrary or unlawful interference.

We recommend that the Ad Hoc Committee adopt the definitions and procedural safeguards outlined in the International Principles on the Application of Human Rights to Communications Surveillance (also called the "Necessary and Proportionate Principles"). That includes avoiding legacy legal definitional approaches such as metadata versus content data, and instead adopting the term "Protected Information" as a technology-neutral standard. At its simplest, Protected Information is taken to mean user data that includes, reflects, arises from, or is about a user's communications and that is not readily available and easily accessible to the general public. As the Necessary and Proportionate Principles further explain, this approach avoids outmoded models of binary classification, and also recognise that in some cases persistent, widespread collection of data that would otherwise not be treated individually as protected information can in fact rise to the threshold of legal concern due to technology or intrusive techniques revealing private information in excess of the individual parts of such data.

We recognise that many states hope to achieve further progress on international legal cooperation on cybercrime issues, addressing the problems they face with the existing mutual legal assistance treaties (MLAT) system that many of them have to work through. However, MLAT reform and bypasses must find ways to address the law enforcement shortcomings without sacrificing rights. Access Now has previously called for measures that improve the current system for cross-border data exchange while maintaining and improving upon existing protections by:

- ensuring human rights protections throughout implementation of treaties, with appropriate accountability, remedy, authentication, and oversight in legal assistance,
- closing the gaps via more MLATs, increased resources, electronic request forms, and a single, well-trained agency designated as a point of contact for each country, and
- clarifying the jurisdictional questions by using an analysis of factors, including location of the data, location of the entity holding the data, location of the data subject, and location of the victim or harm. A country should be required to establish an intimate relationship with data to demonstrate jurisdiction.

5. **Provisions on procedural obligations and cooperation with law enforcement should not increase cyber insecurity by undermining secure communications or the integrity of ICT systems**

Encryption and secure communications tools play a key role in deterring unauthorized access to communications and data, and preventing crime. Therefore, the Ad Hoc Committee should be guided by the May 2015 report of the UN Special Rapporteur on Freedom of Expression. Proposed powers for law enforcement or other measures on cybercrime cooperation should not necessitate the undermining of encrypted communications or the introduction of general vulnerabilities into software systems; such vulnerabilities facilitate greater insecurity and unauthorized access.