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

March 2022 intersessional meeting
Panel discussion on Agenda Item 2: "Criminalisation" (24 March 2022)

Delivered by Raman Jit Singh Chima (Senior International Counsel and Global Cybersecurity Lead)

Thank you Madame Chair; we are grateful for this opportunity to address you all in this intersessional meeting of the Ad Hoc Committee. My organization, Access Now, is an international human rights organization that seeks to protect and further digital rights at risk, with a focus on vulnerable communities. As part of this, we operate a global digital security helpline for human rights defenders, journalists, and other civil society users at risk. Through this work, we are deeply aware of the impact that cybercrime activity as well as badly designed and improperly applied cybercrime laws have on the functioning of democracies, civil society, journalists, and the institutions so crucial for securing our human rights everyday.

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.

All criminal law practitioners and experts are deeply familiar with the reality that design and implementation of criminal law frameworks - particularly defining what is a crime - has an intimate and intense impact on protected human rights.

As the Freedom Online Coalition's (FOC) Working Group 1 - "An Internet Free and Secure" - noted, we need to recognise that cyber-attacks and cybercrime undermine not just a nation's infrastructure and economy, but also an individual's digital security and infringe their human rights, in particular the rights to freedom of expression, information, privacy, and association. The FOC also noted that cyber laws and frameworks can have a harmful effect on human rights.

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

International harmonization efforts must absorb the lessons around national practices, including on focusing on cyber dependent crime versus cyber enabled crime.

If we wish to see true uptake and implementation of a new international legal instrument in this space, we must focus on where we have clear consensus and agreement - a core understanding. That requires us to focus on core cybercrime issues, that is efforts to address and ensure harmonized criminalisation of cyber-dependent crime. We must avoid catch-all, over-expansive approaches towards criminalisation in cybercrime laws.

Seek to advance 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.

As I will note later, 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.

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

- Access to or interference with computing systems without authorisation and with criminal intent;
- Interfering with with or damaging computer data and systems without authorisation and with criminal intent;
- illegal interception of communications;
- misuse of devices with the intent of committing one of these above offenses

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

We must protect the humans critical to ensuring global cybersecurity.

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. I encourage the Ad Hoc Committee to hear further from security researcher communities

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.

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.

Thank you Madame Chair.