PARADIGM INITIATIVE

ASSESSING THE UNITED NATIONS CYBERTREATY PROCESS: AN AFRICAN PERSPECTIVE.

Assessing The United Nations Cybertreaty Process: An African Perspective.

Authors:
Adeboro Odunlami, Adeboye Adegoke

Edited by:
Bulanda T. Nkhowani

Design and Layout:
Kenneth Oyeniyi

Published By:
Paradigm Initiative

PARADIGM INITIATIVE @ParadigmHQ

Abstract

The United Nations' proposed treaty on Countering the Use of Information and Communication Technologies for Criminal Purposes, could not have come at a more strategic time. With the rise of illegal cyber activity across the globe and the concurrent concerns on cyber safety, transparency and inclusion in the creation of cyber norms, the debate on what a standard cybercrime policy should look like wages on at this multilateral forum. However the questions remain: How multilateral is the ongoing conversation? How multilateral should it yet be? While countries across the globe are lending their voices to this momentous issue, there are key stakeholders who are noticeably silent or poorly represented at these negotiations. This policy brief highlights the crucial significance of a broader engagement of civil society, academia, members of the technical community and governments of States in the Global South, especially in Africa, who are currently grappling with the effects of problematic cybercrimes legislations. The brief also includes five key recommendations to stakeholders which include, cooperation for robust and diverse outcomes, innovation around consultative process to allow for meaningful engagement with stakeholders, consideration of international human rights in the formulation of the substantive treaty, cooperation for capacity building and mutual learning and the need to remove barriers to broad participation by actors from Africa and the rest of the global south.

Overview of The UN Cybercrime Treaty Process

In 2021, Russia drew up and presented a Draft Convention to the United Nations titled "United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes."[1] The document[2] is essentially a 7 chapter Treaty to prevent, detect, suppress, investigate and prosecute about 23 types of cybercrime and cybersecurity related offences.

Prior to the introduction of this proposed treaty, there also existed the Council of Europe's Budapest Convention on Cybercrime which was created to address cybercrimes by harmonising laws of nations, enhancing investigative methods and fostering cooperation among states. The Budapest Convention was adopted by the Committee of Ministers by the Council of Europe and then opened up for signature and ratification to non-member states. Only four African countries have ratified this treaty.

Furthermore in June 2014, the African Union published and adopted the African Union Convention on Cyber Security and Personal Data Protection (nicknamed the 'Malabo Convention') which addresses electronic transactions, personal data protection and cybersecurity and cybercrime in the region. Of the 55 AU states, only 14 countries have signed and 5 have ratified[3] the Convention as at the creation of this brief. This data is perhaps an insight into the nature and degree of participation by African states in the procedure for formulating cybercrime and cybersecurity related international instruments.

While the Budapest Convention did not mandate the Council of Europe to involve or carry along African and other Global South states, the current UN Cybercrime Treaty being negotiated requires the full participation of all member states; the Global South states inclusive.

Since the negotiations for the Treaty began, there has been a reportedly apparent lack of consensus among member states on how far the treaty will

1 "Russia Initiates Its Draft of Int'l Convention on Countering Cybercrime." Tass Russian News Agency, Tass, 27 July 2021, https://tass.com/politics/1318319?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com. Accessed 11 Apr. 2022.

2 United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. July 2021. https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf

3 AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, 18 June 2020, African Union, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

reach and what exactly cybercrime is[4]. Members states such as Norway, the UK, the USA, the European Union, Brazil, and Dominican Republic, are arguing for a narrow crime-focused approach to the treaty as opposed to a wider, far reaching approach which imposes controls on the borders of States on the internet.

In the midst of these arguments, the contributions and involvement of African governments are noticeably sparse and far between. Apart from Nigeria lending its voice[5] to support the maintenance of a law enforcement focus and South Africa[6] and Egypt[7] also making submissions, there is not much evidence of feedback or contribution from many other African member states.

The first session of the Ad Hoc Committee to commence the negotiation of the convention was held from 28 February to 11 March and though was ridden with debates about the ongoing Russia-Ukraine war, some relevant and salient points were highlighted. One was the need for capacity building and technical assistance given the digital gap between the Global North and South. Another was a support-in-principle for the participation of Civil Society, NGOs, academia and the private sector as an effort to better understand best practices to combat cybercrime.

4 Rodriguez, Katitza, and Meri Baghdasaryan. "UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope." Electronic Frontier Foundation, 15 Feb. 2022, https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among. Accessed 11 Apr. 2022.

5 Nigeria Comments, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Nigeria_comments_AHC.pdf

6 South Africa's views on scope, objectives and structure (elements) of the envisaged International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/SOUTH_AFRICA_SUBMISSION_ON_SCOPE_OBJECTIVES_AND_STRUCTURE_17_DECEMBER_202171.pdf

7 Egypt's Comments, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Egypt_AHC_comments.pdf

Cybercrimes in Africa & the Potential Effect of the Treaty on Africa

There exists an underlying problem with approaching the formulation of cybercrime policies strictly from a crimes perspective. This narrow one-way appreciation of the subject of cybercrimes may be advantageous for the creation of a strict legal system to tackle these criminal activities but will inevitably result in a restriction or even an overt suppression of rights, a lack of transparency and a generally non-inclusive outcome. There is a need to approach cybercrimes regulations holistically; considering the technical, criminal, procedural, and human rights angles. A balance is necessary.

In 2015, the United Nations General Assembly called on its Member States to be guided in their use of ICTs, noting the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies.[8] Additionally, the United Nations Human Rights Council has affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."

However, what we see from the many attempts by African states to create cybercrime policies is not an adherence to preserving an open, secure, inclusive, accessible or peaceful cyberspace but a weaponization of laws and a stifling of rights.

The consequences of this, all over the continent, are recorded and verifiable.

In Kenya, a major bane of human rights in the country manifests in a 'cybercrimes law'; the Computer Misuse and Cybercrimes Act[9]. A law created to "enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes" but is in fact being ambiguously interpreted to criminalise 'fake news' and back up unlawful arrests.

The Southern African Development Community (SADC) also have developed a similar law called the "The SADC Model Law on Cybercrime 2012" which essentially seeks to foster the harmonisation of domestic laws on Cybercrimes. It identifies certain offences that can be incorporated into domestic laws for

8 Resolution A/RES/70/237

9 COMPUTER MISUSE AND CYBERCRIMES. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=-No.%205%20of%202018. Accessed 11 Apr. 2022.

the combating of cybercrime. This Model law was also adopted as part of a project for the harmonisation of ICT laws in Sub-Saharan Africa. Since its development, many member states have gone ahead to develop their own cybercrime laws. However, as pointed out by experts[10], certain provisions in the model law fundamentally affect the fundamental right to privacy. For instance, section 25 of the law which has been adopted by many of the countries regionally, addresses the search and seizure of electronic equipment suspected to have been used to commit an offence or to contain information related to the commission of an offence. The drawback with this provision is that it prescribes a warrant to be issued for the search of these computers; which warrant can be used to search all devices connected to a network of devices.

In Nigeria, the Cybercrimes Act 2015, though drafted to serve as an "an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes" has become notorious as the empowering law for several human rights abuses. In the bid to criminalise what it calls 'Cyberstalking', the Act criminalises even the communication of any information deemed 'annoying' or 'insulting'. The dangerous effect of this has been the weaponization of this provision by politicians and people with access to state resources and as such this provision had demonstrably impacted the health of human rights in Nigeria.

Whether by unintentional oversight or malicious intent, the examples above show the effect of the current regime of cybercrimes legislation on the continent and the typical disposition of African governments to cybercrimes; a less-than-progressive interpretation and application of laws meant to protect users online. Currently, there are more African states with draft cybercrime and cybersecurity laws under consideration. Hence, the development of a standard global cybercrime treaty could not have come at a more strategic time.

Human rights defenders, and civil society actors in the African region approach domestic and even international judiciary to seek reliefs from the grievances occasioned as a result these cybercrimes policies, citing existing global laws and standards as basis for which the laws should be overturned or declared unlawful (see, SERAP v. Federal Government of Nigeria & Ors[11] where the ECOWAS court held that section 24 of Nigerian Cybercrime Act is inconsistent and incompatible with Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the International Covenant on Civil and Political Rights. See also, the case of Bloggers Association of Kenya (BAKE) v Attorney General

10 Hove, Kuda. "The SADC Model Law on Computer Crime and Cybercrime: A Harmonised Assault on the Right to Privacy?" LinkedIn, 18 July 2017, https://www.linkedin.com/pulse/sadc-model-law-computer-crime-cyber-crime-harmonised-assault-kuda-hove/. Accessed 11 Apr. 2022.

11 ECW/CCJ/APP/09/19

& 3[12] others where the petitioner argued that the certain portions of the Kenya Computer Misuse and Cybercrime Act violate and threaten rights as contained in Articles 19 of the ICCPR and UDHR).

These standards such as the Universal Declaration of Human Rights, the African Charter on Human and People's Rights, the Declaration on Principles of Freedom of Expression and Access to Information in Africa, the International Covenant on Civil and Political Rights and so on, have become more than just norms or treaties but are extremely valuable tools for advocates all over Africa as the continued fight for a better-balanced cybercrimes policy regime wages.

There is therefore a crucial burden and vitally important responsibility on the United Nations to get this momentous Treaty right; because if gotten right, it will serve not only as an expectation of appropriate behaviour but as a compelling and authoritative reference for policymakers, judiciary and advocates all over Africa as they navigate a more well-rounded, rights-respecting and inclusive Treaty. Key issues such as inclusion and even capacity deficits need to be highlighted as well in the consultation for the Cybercrime Treaty. This cannot be done without in-depth and immersive discourse with civil society, academia and even the private sector especially from the Global South to ensure that their perspective on a much-battled subject contributes to the eventual outcome of this global cyber norm.

12 "Petition 206 of 2019." Kenya Law, http://kenyalaw.org/caselaw/cases/view/191276. Accessed 11 Apr. 2022.

Questions the UN should consider as it undertakes this process

Some questions that may be beneficial for the UN's perusal as it undergoes its processes and procedures for this treaty:

1. What roles and benefits does the UN consider civil society to contribute to building robust and all-inclusive norms?
2. Does the UN appreciate the impact of its policies on the policy outcomes of its member states?
3. How can the UN create more inclusive opportunities for stakeholders in the Global South to contribute to the conversation on cybercrimes (opportunities including even capacity building for stakeholders and the proactive removal of structural barriers impeding significant engagement)?

Recommendations for UN & Other Stakeholders

1. **All member states should proactively cooperate and contribute to the development of the UN Cybertreaty to ensure a more robust and diverse perspective and outcome:** One of the founding norms of the United Nations is that States shall cooperate to maintain international peace and security and in developing and applying measures to increase stability and security. This also applies to cyberspace. As the United Nations seeks to develop an international treaty for cybercrimes, all member states should cooperate to develop measures to ensure cybersecurity and also cyber peace. What this entails is that representation should be made at every stage by every member state including those of the Global South and such representation should be robust enough to contribute tangible value and perspective to the general conversation. These representations will help to promote a common understanding of current, evolving and potential threats to peace and safety on the internet. Hence, each member state should make an effort to engage its own micro-stakeholders at State and regional levels such as its civil society organisations, private sector players, as well as its academia.

2. **The UN should appreciate the complex nature of ICTs and the Internet and make provision for a consultation process that is particularly diverse and easily accessible:** A key feature of the topic of cybercrime and cybersecurity is that it is still evolving and highly complex. If the few negotiations at the UN on this Treaty is anything to go by, then it must be obvious that this consultative process has to take on a more flexible and dynamic form to allow for wider contributions, especially from categories of stakeholder whose views are essential to the subject matter; the private sector, academia, the technical committee and civil society. Given the cross-border and ubiquitous nature of cyberspace, there are farther-reaching consequences of international laws and norms that seek to set standards for the regulation of the space. Therefore, an appreciation of this fact must lead the United Nations to seek a broad range of consultation which is inclusive and transparent in nature and to further reduce structural barriers to access for stakeholders

such as civil society and researchers. As submitted[13] by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, "engaging the voices of stakeholders in policy-making processes relevant to ICT security can support efforts for the promotion, protection and enjoyment of human rights online and help clarify and minimise potential negative impacts of policies on people, including those in vulnerable situations." The OHCHR further buttresses this point by recommending that inclusive and meaningful civil society participation is essential in the meetings of the United Nations Ad Hoc Committee to enable transparency and accountability in these negotiations. A letter[14] by nearly 130 public interest organisations also buttresses this.

3. **The UN should greatly consider the Human Rights Council resolution 20/8 and 26/13 and the General Assembly resolutions 68/167 and 69/166 which highlight the promotion, protection and enjoyment of Human Rights on the Internet and the respect for the right to privacy and free expression in the digital age:** These resolutions emanating from the United Nations itself are direct commitments by the Organisation to pay attention to the effect of its own resolutions, laws and treaties on these rights. The Cybercrime Treaty is a perfect example of an occasion where the United Nations must rise in the protection and consideration of rights online. The United Nations must ensure that every wording and provision of the treaty passes through a vigorous human-centred impact assessment to ensure that whilst cybercrimes are being punished, discriminatory crimes against humanity and rights are not being promoted and fostered.

4. **Member States should cooperate particularly for capacity-building and mutual learning purposes:** In order to strengthen not just the development of this Treaty but also the eventual effective application of its provisions to domestic contexts, members states join hands to build the capacity of key players (including technical, civil society, academia and government) to ensure better skills in detecting responding and investigating threats to cybersecurity and cyber peace. This would help to ensure that this process helps to bridge the policy, financial and digital divide to enhance cyber safety.

13 Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

14 Rodriguez, Katitza, and George Wong. "Nearly 130 Public Interest Organizations and Experts Urge the United Nations to Include Human Rights Safeguards in Proposed UN Cybercrime Treaty." Electronic Frontier Foundation, 13 Jan. 2022, https://www.eff.org/deeplinks/2022/01/nearly-130-public-interest-organizations-and-experts-urge-united-nations-include. Accessed 11 Apr. 2022.

5. **The UN must work to remove barriers hindering the participation of actors from the global south and its processes:** The various barriers impacting the participation of African actors in the global cyber treaty process must be addressed. These barriers include capacity gaps, and access to information, including information about funding and available resources to support their ongoing work. These barriers must be spotlighted and eradicated, thus allowing for a free flow of information as permissible in law. The lack of strong participation in the process must not be defined as an indication of a lack of interest but as an economic issue.