Written Statement delivered during the informal intersessional consultative meeting of the OEWG on developments in the field of information and communications technology in the context of International security[1]

02 December 2019

OEWG Session B: Rules, laws, and norms: Creating a cyber space based on rules, laws, and norms. How can stakeholders support governments

409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa

[1] This written statement was prepared by Nils Berglund and Enrico Calandro.

Research ICT Africa is a regional think tank which aims at providing the necessary data and information for an evidence-based digital policy-making, including issues related to responsible state behaviour in cyberspace. With this in mind, we are delivering this statement with the aim of providing some evidence on the debate on rules, laws, and norms from an African perspective.

African stakeholders have remained largely absent from the evolving norms debate of the last two decades. Voluntary and non-binding norms, rules, and principles, some of which are embedded in international law, were originally developed in a largely state-driven, top-down approach to norms-building. Given the region's specific internet ecosystem, characterised by lack or under-utilisation of physical resources such as IXPs, dearth of local content, poor quality of service, and high prices and latency, in many African countries cybersecurity was not recognised as a regional or national priority and participation from African stakeholders was very limited.

Unsurprisingly then, the 11 norms of the 2015 UN GGE report (A/70/174, 2015), while feasible in principal and global in ambition, were not all grounded in African perspectives or realities, and may not sufficiently consider the particular challenges of resource-constrained nations with different levels of ICT development. Several norms encouraging substantial cooperation through various methods may prove specifically difficult given unclear institutional arrangements, difficult to enforce legal frameworks and low cyber maturity of several African nations. Assessing and reporting on ICT incidents and vulnerabilities requires states to have the technical capacity to do so, and according to the ITU only 13 African countries currently have national Cyber Security Incident Response Teams (CSIRTs) as of March 2019[2]. Without sufficient technical capacity to prevent or respond to cyber incidents, moreover, exposing vulnerabilities or lack of capacity may make resource-constrained nations even more vulnerable to external attacks.

Norms also call on states to "prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats" (13d) and, "respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory" (13h). Yet in addition to technical capacity, such cooperation is likely to necessitate legislative tools and relative consensus on cyber laws, a challenge for many African nations as only 28 nations on the continent (52%) have enacted cybercrime legislation according to UNCTAD[3].

Cooperation in for example, "developing and applying measures to increase stability and security in the use of ICTs and to prevent harmful ICT practices" (13a) may be further hindered by the lack of cyber policy and strategy, which define roles, responsibilities and institutional arrangements in regard to the securement of cyberspace. As only 14 nations in Africa have ITU recognised National Cybersecurity Strategies[4], methods for multilateral cooperation are likely to remain unclear for a number of states in the region.

The limited technical and institutional capacity of African nations may also mean that some norms directed towards the responsible behaviour of nations with greater cyber maturity are still theoretical in

[2] ITU. (2019a). National CIRT. Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[3] UNCTAD. (2019). Summary of Adoption of E-Commerce Legislation Worldwide. Retrieved from United Nations Conference on Trade and Development:

https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-GlobalLegislation.aspx

[4] ITU. (2019b). National Cybersecurity Strategies Repository. Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/NationalStrategies-repository.aspx

an African context. In regards to (13h) and (13j) for example, no state-sanctioned cyber-attacks to critical information infrastructure have emanated from Africa[56], Rather, as African countries generally do not have the cyber capacity to escalate, weaponise, and develop cyber arms, they are simply at potential risk from the attacks of more developed countries. Similarly, (norm 13j) calls for states to "take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products" and "seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions," yet unlike other regions such as North America, Asia and Europe, ICT supply chains generally do not originate in Africa. Rather, African nations adopt standards and information communication technologies from foreign producers[7], who retains more power in determining the transparency and integrity of supply chains and the meeting of safety and security requirements.

Another notable norm promoting responsible behaviour calls for states to "respect resolutions by the Human Rights Council and UNGA to promote and protect enjoyment of human rights on the Internet, and to guarantee full respect for human rights" (13e). However, in emerging economies and developing countries, democratic assumptions about human rights, freedom of expression, privacy and security underpinning the International human rights framework and principles of good governance, often collide with the political economy of relatively new independent states, and with their under-resourced institutional arrangements, which often lack necessary technical skills, capacities, and financial resources to effectively implement cyber legislative measures.

So, what role can CSOs, academia, and other stakeholders play to support their own countries to socialise and observe norms at a national level?

First, there is a need to bring evidence to the debate on norms at a national level through research, to bring national contexts and realities to this global debate and processes;

Second, CSOs can support national consultations in a multistakholder way, so that all relevant stakeholders are involved in this debate beyond government organisations;

Third, capacity building is needed to observe the non-binding, and voluntary norms, principles and rules on responsive state behaviour in cyberspace agreed upon with resolution, and to support governments in creating a cyberspace based on rules, laws, and norms. However, stakeholders in the public, private and civil-society sectors need to improve the coordination of cyber capacity objectives and activities, to reduce fragmentation and improve impact.

Last but not least, we would like to reiterate that as a number of cases from Africa demonstrate, a technical and normative approach to institutions, processes and rules in this area, outside a human rights and good governance framework, may have the unintended outcome of effectively weakening the protection of individual rights.

[5] The only state-sanctioned cyberattack recognised by the Council on Foreign Relations' Cyber Operations Tracker originated in Ethiopia, and was a largely failed spyware campaign targeting Ethiopian political dissidents in several foreign nations

[6] Council on Foreign Relations, (2019). Cyber Operations Tracker. Available at https://www.cfr.org/interactive/cyber-operations#Takeaways

[7] Wilson, T. (2019, May 31). Huawei and African Union boost relationship with deal. https://www.ft.com/content/30ec5c54-83aa-11e9-b592-5fe435b57a3b