# Bridging the cyber norms debate with evidence

04 December 2019

Discussion Paper submitted to the UN Open Ended Working Group (OEWG) on developments in the field of information and communications technology in the context of International security

RESEARCH ICT AFRICA

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

Multistakeholder models for participation in the governance of the Internet have served as key mechanisms in the preservation of a free and open network since the establishment in 2004 of the UN Working Group on Internet Governance. However, fifteen years later, in a vastly different and changing technological landscape, traditional forms of Internet governance are facing considerable pressure to be reformed. As the next three billion Internet users will likely come from Africa, Southeast Asia, and Latin America, and as the Internet grows increasingly central to the economy and societies of these countries, different political and cultural values and characteristics will likely emerge in the debate on norms, rules, and principles on responsible state behaviour in cyberspace. Along with the often competing agendas of states, civil-society and the private sector, different views will influence debates on cyber norms, including discussions of the UN Group of Governmental Experts (UNGGE) on Development in the field of Information and Telecommunications in the Context of Information Security and of the Open Ended Working Group. Nevertheless, 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 through UNGA processes in the First Committee on Disarmament and the UN Group of Governmental Experts in the late 1990s and early 2000s, in a largely state-driven, top-down approach to norms-building.

The last decade has also seen 'communities of practice' enter the normative debate in the form of regional organisations, such as the European Union (EU), Organisation of American States (OAS), and Association of Southeast Asian Nations (ASEAN); and in the form of expert communities, such as the Global Commission on Stability in Cyberspace and Geneva Dialogue on Responsible Behaviour; and also through private sector initiatives, such as the Siemens Charter of Trust or Microsoft Tech Accord. However, such communities of practice represent commercial and donor state interests or initiatives, which might diverge from African priorities[1], while the perspectives and distinct challenges of under-resourced nations and emerging and developing economies have remained consistently under-represented in discussions about the future of the cyberspace and its governance. Instead, dominant interests of more mature economies and global private sector players generally have set agendas on norms through resolutions, recommendations, international treaties, and regional economic regulation and initiatives. It is through epistemic networks of experts and consultants that development initiatives related to the future of cyberspace are set, and their values and priorities are recommended nationally through international, multilateral, and regional organisations.

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. Since 2004, for example, only nine African

[1] Calandro, E., & Berglund, N., (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case. 2019 GIGANet Conference Paper. Available at https://www.giga-net.org/2019-annual-symposium/

nations have held UNGGE memberships[2], none of which have been held for more than a total of 5 years, and none African nations are permanent members of the UN Security Council[3].

It is in this context that the dialogue on cyber norms and on preventing conflicts and their escalation in cyberspace should be understood. Considering that a number of developing countries have not articulated clear and functional national co-ordination mechanisms to respond to cyber-incidents, most probably will not be able to observe the norms[4] and to "cooperate in developing and applying measures to increase stability and security in the use of ICTs" (A/70/174, 2015, 13a).

Unsurprisingly then, the 11 norms developed by the 2015 UN GGE[5], 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. For example, norms indicate that "in case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution and the nature and extent of the consequences" (13b) and they call for states to, "encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats" (13j). However, 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[6]. 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 out of 54 nations on the continent have enacted cybercrime legislation according to UNCTAD[7].

---

[2] There countries are Morocco, Mali, Ghana, Senegal, Botswana, South African, Kenya, Egypt, Mauritius.

[3] Geneva Internet Platform, (2019). The UN GGE and OEWG. Digital Watch Observatory. Available at https://dig.watch/processes/un-gge

[4] Radunović, V. (2019). Usual Suspects: Questioning the Cybernorm-Making Boundaries. Report. Available at https://dig.watch/sessions/usual-suspects-questioning-cybernorm-making-boundaries (Accessed Nov 2019)

[5] A/70/174. (2015, July 22). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from United Nations General Assembly: https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf

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

[7] 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

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[8], 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 an African context. In regards to (13h) and (13j) for example, no state-sanctioned cyber-attacks to critical information infrastructure have emanated from Africa[9,10]. 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, (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 some 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[11,12], who retain 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, 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.

While increasing socio-economic opportunities have been emerging from digitalisation processes, benefits are accompanied by increasing cyber-threats and risks, and in part as a result of the inability to tackle cybercrime through the enforcement of laws, governments in developing economies are implementing measures that rather than protecting people from cyber-threats through cybersecurity

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

[9] 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.

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

[11] According to the Financial Times, the Chinese company Huawei is currently the largest supplier of ICTs in Africa.

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

legislation, deny Internet access and use, for instance during election time by shutting down the net[13], via imposing social media taxes on Internet users[14], or via mass surveillance of vulnerable people[15]. As several African cases have demonstrated, 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.

*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, civil society organisations can support national multistakholder consultations, so that all relevant stakeholders are involved in this debate beyond government organisations. Third, capacity building is needed indeed to support governments to observe the non-binding, and voluntary norms, principles and rules on responsive state behaviour in cyberspace agreed upon resolution, and to clarify how international laws apply in cyberspace. Yet, efforts to build cyber capacity in Africa have been fragmented, with inconsistent outcomes[16]. Therefore, policies should aim at improving coordination efforts between all stakeholders dealing with cyber capacity building to allow existing UN resolutions to be effectively implemented, to reduce fragmentation and improve impact. At the same time, capacity building efforts and international cooperative measures need to take into account local contexts, and involve local expertise for capacity building activities to be effective. Nationally, cyber maturity assessments can, for example, support the identification of specific points of policy intervention and identify distinct needs and priorities of national or regional contexts. The future of the UN GGE must therefore encourage new models of hybrid engagement, through apparatuses like the OEWG, involving not only inputs from stakeholders of all sectors, but also more coordinated and grounded ('bottom-up') approaches to building confidence and capacity.

The strength of international rules, laws and norms in cyberspace depend upon their adherence by the international community, and without cyber capacity or confidence in the international procedures and structures upheld by the UN GGE, they will likely remain ineffective in many under-resourced African nations. As such, international resolutions on responsible state behaviour in cyberspace remain difficult to uphold or implement in a developing-country context. Even more difficult to ratify are international treaties, which due to severe capacity constraints are an ineffective approach to encouraging responsible state behaviour in cyberspace. International or regional agreements, and the norms that underpin them, are in a sense only influential to the extent to which

[13] BBC. (2019, December 31). DR Congo election: Internet shut down after presidential vote. Retrieved from BBC News: https://www.bbc.com/news/world-africa-46721168

[14] Gillwald, A., Mothobi, O., Ndiwalana, A., Tusubira, T. (2019). The State of ICT in Uganda. Research ICT Africa. Available at https://researchictafrica.net/2019_after-access-the-state-of-ict-in-uganda/

[15] Links, F. (2018). Tackling Cybersecurity/Cybercrime in Namibia – Calling For a Human Rights Respecting Framework. Institute for Public Policy Research.

[16] Calandro, E., & Berglund, N., (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case. 2019 GIGANet Conference Paper. Available at https://www.giga-net.org/2019-annual-symposium/

they can be effectively implemented at a national level, and the failure of ratifying conventions like the Budapest Convention and the Malabo Convention in Africa are evidence of this.

Rather than another treaty, developing nations need new and coordinated forms of building confidence and capacity to strengthen the understanding of and ability to adhere to existing norms on responsible state behaviour in cyberspace. While international law and its application in cyberspace is essential, it is not nearly enough to ensure the adoption of human rights frameworks in the implementation of cyber norms, or effective multistakeholder participation, and the OEWG mandate must recognise this through an emphasis on international cooperation and coordination on building capacity. The UN GGE norms must always be contextualised in the particular regional or national contexts in which they are intended to be socialised, to reflect the particular challenges and perspectives of all member states in global debates and processes—an ambition of multistakeholderism that remains to be realised.

---

*For more RIA updates, sign up here.*

## Authors

Enrico Calandro (PhD)

ecalandro@researchictafrica.net

Nils Berglund

nberglund@researchictafrica.net

Enquiries

info@researchictafrica.net

409 The Studios, Old Castle Brewery, Beach Road, Woodstock, Cape Town

T: +27 214476332

W: www.researchictafrica.net