Abridged version - Output document of the AfriSIG22 Multi-stakeholder Consultation on African Participation in the OEWG on ICTs, Lilongwe, 6th to 18th July 2022

Table of Contents

Introduction

1. This document was developed as an input into the Open-Ended Working Group on ICTs (OEWG) during a multistakeholder consultation held in Lilongwe, Malawi from 16th to 18th July 2022 immediately prior to the 11th African Internet Governance Forum. The consultation, linked to the 10th African School on Internet Governance[1], convened by the Association for Progressive Communications and Global Partners Digital, was attended by a diverse group of individuals from African governments, law enforcement and security agencies, the African Union Commission, civil society organisations, digital rights and media groups, and cybersecurity experts. The document identifies the cyber capacity needs of various state and non-state actors in Africa, and then proceeds to respond to the questions proposed by Ambassador Gafoor, the chair of the OEWG, in preparation for its second substantive session starting on 25 July 2022. Participants contributed to this document in their individual capacity and are listed in the annex at the end of the document.

A - Cybersecurity capacity-building needs in Africa

We recommend that it is necessary to establish and enhance capacity at national, sub-regional[2] (including regional economic communities) and regional levels in Africa for:

1. AfriSIG is an initiative of the Association for Progressive Communications, the African Union Commission and Research ICT Africa - https://afrisig.org/afrisig-2022/
2. In the African context this refers to sub-regions which are also often referred to as ‘regional economic communities’.

5.1 Developing comprehensive cybersecurity strategies, policies, regulations and diplomacy that emphasise the security of individuals and communities, and that integrate applicable norms, confidence building measures and international law.

5.2 Harmonising legal frameworks and embracing the Malabo convention.

5.3 Protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII).

5.4 Preventing and responding to cyber incidents, including through information sharing, minimising risks and mitigating consequences and preparedness within Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to be able to better predict and mitigate cybersecurity threats. This includes enhanced capacity for effective communication among response teams, and between them and other concerned state and non-state actors.

5.5 Transparent feedback reporting mechanisms for all state representatives that attend sub-regional, regional and global engagements in order to institutionalise knowledge and information sharing.

5.6 Coordination and collaboration between state and non-state actors, especially in the global South.

6. Further areas where specific capacity-building is needed include:

6.1 Conducting comprehensive national cyber-needs assessments to determine gaps and needs of the different actors and stakeholder groups participating in cybersecurity processes.

6.2 Developing Confidence Building Measures (CBMs) for the African region as has been done in other regions.

6.3 Implementation, and monitoring of such implementation, of agreed cyber norms and engaging with the applicability of international law and how to operationalise this in the African context.

6.4 Mobilising resources needed to meet cybersecurity needs and to carry out substantive national consultations with non-state actors in the development of national cybersecurity positions and strategies.

6.5 Combating cybercrime including through cross-border cooperation and evidence exchange.

7. We believe that in the process of responding to these capacity-building needs, the following considerations should be prioritised:

7.1 Mainstreaming gender responsiveness.

7.2 Closing the digital divide, particularly the gender digital divide.

7.3 Developing, implementing and enhancing data protection and privacy frameworks.

7.4 Developing and implementing reporting measures and mechanisms on cybersecurity incidents so as to enable transparency, access to information (e.g. via publicly available information sharing mechanisms) and accountability.

7.5 Adequate financial resources to enhance the human resource capacity of institutions responsible for cybersecurity.

8. Different state and non-state actors have specific capacity-building needs which are included in the longer version of this document (see above). Needs that were identified as common to state and non-state actors include:

8.1 Knowledge of applicable cybersecurity and human rights norms and standards as well as relevant international human rights instruments, including non-binding norms and standards initiated by industry and civil society.

8.2 Understanding the opportunities that exist for engagement in multilateral policy processes and how to engage effectively.

8.3 How state and non state actors can engage with one another in a manner that builds trust and confidence.

9. Additional needs identified for state actors (government and national security agencies) include: understanding the value of multistakeholder and expert-based delegations at the UN and other international cybersecurity and diplomacy processes; the applicability of international law and norms in their national contexts; institutional capacity for developing and sustaining cyber-diplomacy and digital foreign policy; how to protect critical infrastructure, critical information infrastructure and respond to ICT related emergencies; how to apply a human-centric and multi-sectoral approach; and how to establish confidence building measures.

10. The Judiciary and/or Justice, Law and Order Sector (JLOS) needs to understand digitalisation and cybersecurity issues, laws and how to prosecute cybersecurity offences, including cross-border offences; digital evidence management; and how to consider human rights in the adjudication of cyber-crime cases.

11. Law enforcement institutions need to understand that the prosecution of cybercrime offences might require new and specialised approaches to the detection, investigation and prosecution of cybercrime cases and how to respect human rights in the investigation of cyber crime cases.

12. Parliamentarians need capacity to understand cybersecurity issues and promote awareness of cybercrime, security and cyber hygiene among their constituents; how to work towards harmonisation of cyber laws in the region; and how to better cooperate with other stakeholders in shaping policies which correspond to the digital age and that are agile, flexible, human-centric and that take into account human rights and gender equality.

11. The African Union Commission and Regional Economic Communities need capacity to: continue to support, and give greater visibility to the African Union Commission's Cybersecurity Expert Group (AUCSEG); understand the opportunities that exist for engagement at multilateral policy processes and how to do so effectively; and ensure consistent and effective technical coordination among states and relevant non-state actors.

B - Collaboration: Regionally and among state and non-state actors

Current non-state actor involvement in supporting and/or delivering capacity-building initiatives

12. Existing non-state actor involvement in ICT security capacity-building throughout Africa that stands out include:

12.1 Developing and sharing research methodologies for cybersecurity needs and readiness assessments at national, sub-regional and regional level.

12.2 Raising awareness of African and international human rights standards that apply to cybersecurity law, policy, regulation crafting and implementation.

12.3 Technical capacity building provided by technical community actors and digital safety and security training to cultivate cyber resilience.

12.4 Digital security training for journalists and human rights institutions and defenders, provided by civil society organisations.
12.5 Contributions to the development of laws, policies and regulations in the cyber and digital sphere by human rights expert organisations.
12.6 Training of the JLOS (provided by UNESCO).
12.7 The African Union Commission's Cyber Security Expert Group (AUCSEG), a multistakeholder group of experts that advises the AU on cyber security issues and policies.
12.8 Internet governance capacity building at regional and national provided through Schools on Internet Governance (SIGs)[3] and by technical organisations.[4]
12.9 Mobilising of financial resources to support capacity building, particularly among, but not only, non-state actors.
12.10 Development of knowledge products and training materials for community awareness and digital literacy by the technical community, civil society and business.
12.11 Supporting the alignment of cyber related activities by nations and prioritisation by development partners, donor agencies, and other non-state actors in assisting countries to enhance cyber capacity building.[5]
12.12 Closing the digital divide including the gender digital divide through establishing and sustaining community networks and by building the capacity of women and girls to be engaged in cyber related activities.
12.13 Combating gender-based violence online through awareness raising and building digital security skills provided by civil society groups.

What type of capacity-building initiatives are most suited to meaningful and effective contributions from non state actors?

13. Non-state actors including civil society, business and the technical community, can contribute in a range of ways to capacity building. This includes: analysing policies and developing model laws; integrating a human centric and human rights approach into ICT security law, policy and regulation; developing and promoting standards for ICT security; developing skills and capacity - including digital security and cyber hygiene capacity - in formal and non-formal contexts; developing training materials including for digital safety, security and literacy; designing programmes to achieve gender equality and equality in the cybersecurity sector – among others.

3. The African School on IG (AfriSIG) - www.afrisig.org.
4. ICANN, and the Internet Society provide regular internet governance training and security in Africa. The Diplo Foundation has provided cyber diplomacy training at regional level through collaboration with the AUC, at national level, and through their online courses. FIRST and AfriNIC also provide and facilitate capacity building on a regular basis. Multiple national schools of IG take place in Africa annually. They can be accessed via: https://www.igschools.net/mw-sig/wiki/Main_Page
5. E.g. the GFCE's "Clearing House" process to enable countries to prioritise their cyber capacity needs for assistance.

C - Proposals for collaborative actions

Specific proposals for collaborative actions - with reference to the action-oriented proposals made by states thus far in the 2nd OEWG and reflected in the draft annual progress report.

16. We recommend that state and non state actors collaborate to:

16.1 Promote awareness at national, regional and international level of cybersecurity not as only technical security, but as a form of societal security.

16.2 Develop and implement comprehensive national cybersecurity strategies, policies and regulations.

16.3 Develop national positions for global processes, such as the OEWG and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

16.4 Prioritise cybersecurity in national budgets to ensure adequate resourcing for cybersecurity capacity development including through integrating cyber hygiene and digital safety and security into standard educational curricula at primary, secondary, tertiary levels and in vocational training programmes.

16.5 Share resources and expertise nationally, sub-regionally and regionally. experts, etc

16.6 Develop and implement mechanisms for national, sub-regional, regional and continental collaboration between Cybersecurity Incidents Response Team (CSIRT) or Computer Emergency Response Team (CERT).

16.7 Establish CSIRTs and CERTs where they are not yet in place.

16.8 Provide support for collaboration with non-state actors in the development of national positions and inputs at regional and global ICT security forums.

16.9 Review existing frameworks and where applicable establish legislation or regulation to enhance the security and stability of cyberspace.

16.10 Develop cybersecurity related standards that address and are accessible to SMMEs.

16.11 Enhance coordination and collaboration at national, regional and international level between state and non-state actors, especially within the global South

16.12 Enhance the capacity and capability of law enforcement agencies to tackle cybercrime and child online protection at national, regional and international levels.

16.13 Enhancing resilience of national Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) by developing and operationalising national risk mitigation frameworks for identifying national critical assets and sectors.

Proposals for including non-state actors in the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report.

17. We recommend:

17.1 That member states avoid using veto power to limit the engagement of non-governmental organisations without ECOSOC accreditation, and if they do, to do so

responsibly, proportionally, in a transparent manner and with providing clear case-by-case justifications to others states and the broader community.

17.2 That collaboratively, inclusive open consultations to gather relevant input from non-state actors, are convened throughout the remainder of the OEWG's mandate on all issues on its agenda, not only on capacity-building. Non-stakeholder input can also add value to discussions on issues such as the applicability of international law, confidence building measures (CBMs) and norm development and implementation.

17.2 Continuous information sharing by all stakeholders including with and among academic and technical communities.

17.3 That states include non-state actors in national delegations at the OEWG on ICTs, and, if this is not possible, to at the very least include them in the national process of preparing positions as well as in informal negotiations with other states and non-state actors

17.4 A human centric approach which considers how cyber security affects peoples' well-being, rights, livelihood, environment, culture, belief systems and mindsets

17.5. Countries develop capacity to effectively understand and implement the GGE norms on responsible behaviour in cyberspace by states.

18. We propose collaboration between state and non-state actors to:

18.1 Facilitate and participate in the creation of multi-stakeholder spaces at national and continental levels that bring interested stakeholders, including businesses, non-governmental and civil society organisations and academia together to come up with measures to support local and continental capacity building efforts in cyber security expertise, information-sharing, and training.

18.2 Conduct and publish technical reports and white papers (e.g., cyber threat horison reports etc) on national cyber status of the country

18.3 Engage stakeholders in developing strategies, policies and regulations that are relevant and comprehensive.

18.4 Develop a sustainable framework for cyber capacity enhancement. One approach is to build and give greater visibility to existing expert communities from within Africa - where they exist, and to create them where they do not - to take ownership and lead in sustaining cyber capacity building. A key example is the African Union Commission's Cybersecurity Expert Group.

18.5 Establish peer-to-peer knowledge transfer at innovation hubs, centres of excellence and techno parks to encourage home grown expertise in Cyber and related areas.

18.6 Promote ethical cyber stars and champions through competition events e.g. ICT in girls gender tech initiatives and mentorship and coaching in order to influence cybersecurity culture and resilience.

END