African Cybersecurity Capacity Building priorities: Output document of AfriSIG 2022 and the Multistakeholder Consultation on African Participation in the Open-Ended Working Group, Lilongwe
16th to 18th July 2022

Preamble

Cybersecurity is a critical enabler for socio-economic transformation and development. It is, therefore, important that Africa identifies and prioritises specific cyber capacity building needs, in order to achieve its digital transformation agenda. Some of these priority areas for cyber capacity-building include: governance, policy-making including harmonisation of policy, legislation and regulation, technical tools and infrastructure, understanding, innovation, planning, and research and development. In addition, greater capacity is needed by both state and non-state actors in Africa so that they are able to participate effectively, and consistently, in relevant United Nations processes such as the Open-Ended Working Group (OEWG) and other related international cyber capacity and security initiatives.

Capacity-building is critical for improving the quality and substance of discussions by African states that aim to engage and influence global rules, norms and principles for responsible state behaviour in cyberspace, and the establishment of cybersecurity resilience and culture. Multi-stakeholder engagement at all levels, global, regional, subregional and national - implemented in an inclusive, transparent and accountable manner - should be at the core of Africa's approach to cybersecurity; especially in the development of human-centric and human-rights aware cybersecurity policies, laws, and strategies.

These strategies should be premised on the reality that cybersecurity threats can be complex and are constantly evolving; hence the need for continuous learning and capacity-building. This would enable state actors to be more prepared to respond to cyber threats and criminals as well as keep up with developments on international norms, standards and laws. Such approaches, will therefore, improve Africa's cybersecurity posture, and promote investment, trade and public trust in ICTs in African states.

This document was developed as an input into the Open-Ended Working Group on ICTs during a multistakeholder consultation held in Lilongwe, Malawi from 16 to 18 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. Participants in the consultation who contributed to this document in their individual capacity are listed in the annex at the end of the document.

A - Cybersecurity capacity-building needs in Africa

General capacity-building needs including institutional capacity

1. It is important that Africa identifies specific cybersecurity capacity building needs in order to achieve its digital transformation agenda. Priority areas for cyber capacity building include: governance, technical and policy upskilling, innovation, research, planning and development.
2. Capacity-building is also needed in building tools and infrastructure, and in harmonisation of laws and policies.
3. African actors also need greater capacity to be able to contribute effectively to UN Processes such as the Open Ended Working Group (OEWG) and other global cybersecurity initiatives.
4. We therefore recommend that it is necessary to establish and enhance capacity in Africa for:
    a. Developing comprehensive cybersecurity strategies, policies, progressive regulations and diplomacy that emphasise the security of individuals and communities and that integrates applicable norms, confidence building measures and international law.
    b. Harmonisation of legal frameworks at national, sub-regional[2], regional and international levels.
    c. Measures to ensure the resilience and protection of both Critical Infrastructure (CI) and Critical Information Infrastructure (CII).

1https://afrisig.org/afrisig-2022/

2 In the African context this refers to sub-regions which are also often referred to as 'regional economic communities'.

d. Preventing and responding to cyber incidents, including through information sharing, minimising risks and mitigating consequences, at national, sub-regional and regional levels.
e. 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.
f. Transparent feedback reporting mechanisms for all state representatives that attend sub-regional, regional and global engagements in order to institutionalise knowledge and information sharing.
g. Cybersecurity awareness, advocacy and outreach at the national, sub-regional (including regional economic communities) and regional level.
h. Development of cybersecurity expertise through innovation hubs, centres of excellence, upskilling, research and development.
i. Coordination and collaboration at national, sub-regional, regional and international level between state and non-state actors, especially at global south-to-south level.
j. Standards, certification and accreditation frameworks that are comprehensive and effective in ensuring cybersecurity protection for all.
k. Cybersecurity training and skilling that enables the workforce to protect and secure critical infrastructure and critical information infrastructure, from basic ICT skills to advanced cybersecurity skills and competencies.

5. Specific capacity development is needed to build the awareness and skills required to refocus the traditional state-centric conception of cybersecurity to a human-centric, human rights respecting approach that also builds cyber resilience among users.

6. Further areas where specific capacity-building is needed include:
    a. Conducting comprehensive national cyber-needs assessments to determine gaps and needs of the different actors and stakeholder groups participating in cybersecurity processes.
    b. Developing Confidence Building Measures (CBMs) for the African region as has been done in other regions.
    c. Implementation, and monitoring of such implementation, of agreed cyber norms.
    d. Engaging with the applicability of international law and how to operationalise this in the African context.
    e. Effective convening of negotiation teams with the relevant subject matter expertise across a range of required competencies such as: technical issues; negotiation skills; international human rights law; international diplomacy; and drafting of written statements and submissions;
    f. 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.

7. In addition to the above areas where capacity-building is needed we believe that the following must be prioritised:
    a. Mainstreaming gender responsive training into all processes aimed at building cybersecurity expertise.

b. Interventions aimed at closing the digital divide particularly the gender digital divide.
c. Developing, implementing and enhancing data protection and privacy frameworks that will complement cybersecurity efforts.
d. 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.
e. Prioritising and budgeting adequate financial resources to enhance the human resource capacity of institutions responsible for cybersecurity.
f. Capacities to combat cybercrime including through cross-border cooperation and evidence exchange.
g. Harmonise laws across Africa and embrace and implement the Malabo convention.

Needs specific to particular stakeholder groups/ actors / institutions

8. Different state and non-state actors have specific capacity-building needs. These include:
    a. Business and the technical community:
        i. Knowledge of applicable cybersecurity and human rights norms and standards as well as relevant international human rights instruments, including those initiated by industry;
        ii. Producing transparency reports on cyber incidents and data breaches.
        iii. Understanding the opportunities that exist for engagement in multilateral policy processes and how to engage effectively.
    b. Civil society:
        i. Understanding the implications of binding and non-binding policy outcomes at the UN level in relation to State ICT Security and the processes for adopting such instruments and monitoring compliance.
        ii. Understanding the opportunities that exist for engagement at multilateral policy processes and how to engage effectively.
        iii. Ability to conduct research and contribute text and commentary on cybersecurity policy being developed at national, sub-regional, regional and international level.
        iv. How to engage with governments in a manner that builds trust and confidence.
        v. Accessing resources to participate in and engage multilateral policy processes.
    c. Media practitioners / journalists
        i. How to follow and report on treaties and other instruments so that audiences can digest the information, and understand how it relates to them.
        ii. How to report on cyberthreats and incidents in a way that builds awareness and promotes cyber hygiene.
    d. Academia
        i. Resources for sustained research and sharing outputs to inform and participate in international (e.g. UN) cyber diplomacy and cybersecurity processes.
    e. Government
        i. How to engage with non-state actors in a manner that builds trust,

confidence and ensures inclusive process.

ii. Understanding the value of multistakeholder and expert-based delegations at UN and other international cybersecurity and diplomacy processes.
iii. Institutional capacity for developing and sustaining cyber-diplomacy and digital foreign policy.
iv. How to collaborate and build consensus with other governments within and outside their regions (such as those that have shared interests).
v. How to protect critical infrastructure, critical information infrastructure and respond to ICT related emergencies.

f. National security institutions
   i. Training on broader cyber security issues including on applying a human-centric and multi-sectoral approach and on the intersection between cybersecurity and human rights .
   ii. Knowledge of applicable human rights norms and standards as well as of relevant international, regional and national human rights instruments.
   iii. Understanding how to approach and build confidence building measures (CBM) and the applicability of international law and norms in their national contexts..
g. Judiciary
   i. Understanding digitalisation and cybersecurity matters, laws and how to prosecute cybersecurity offences, including cross-border offences.
   ii. Awareness of, and support to engage in relevant treaty and policy processes and conferences.
   iii. How to consider human rights in the adjudication of cyber crime cases.
   iv. Digital evidence management
   v. Knowledge of regional, continental and international cyber related instruments and conventions, and norms and principles.
h. Law enforcement institutions
   i. Understanding broader cyber security issues and that the prosecution of cybercrime offences might require new and specialised approaches.
   ii. Capacity in cyber forensics.
   iii. Specialised capacity in the detection, investigation and prosecution of cybercrime cases.
   iv. How to consider human rights in the investigation of cyber crime cases.
i. Parliamentarians
   i. Capacity to understand cybersecurity issues and and promote awareness of cybercrime, security and cyber hygiene among their constituents.
   ii. How to work towards harmonisation of cyber laws in the region.
   iii. 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.
j. The African Union Commission and Regional Economic Communities
   i. Understanding the opportunities that exist for engagement at multilateral policy processes and how to do so effectively.
   ii. Capacity for consistent and effective technical coordination among states and relevant non-state actors.
   iii. Continue to support, and give greater visibility to the African Union Commission's Cybersecurity Expert Group (AUCSEG).

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

9. Cyber capacity-building cooperation and information sharing efforts that are ongoing, inclusive and transparent should be established and enhanced at national, sub-regional, regional and international levels between and within different stakeholder groups. Priority should be given to collaboration and information sharing among:
    a. Governments and various relevant non-state stakeholders in-country;
    b. Civil society organisations nationally, regionally and continentally
    c. Civil society organisations and technical organisations and businessesStates, including through statutory cybersecurity authorities such as CERTs.

Current non-state actor involvement in supporting and/or delivering capacity-building initiatives in the context of the current ICT security capacity-building landscape.

10. There is extensive non-state actor involvement in ICT security capacity-building throughout Africa. Areas where such involvement stands out include:
    a. Developing and sharing research methodologies for cybersecurity needs and readiness assessments.
    b. Research and awareness-raising by civil society organisations of African and international human rights standards that should underpin cybersecurity law, policy, regulation crafting and implementation.
    c. Awareness-raising and technical capacity building provided by technical community actors.
    d. Human rights organizations contribute to the development of laws, policies and regulations in the cyber and digital sphere.
    e. 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.
    f. Civil society organisations provide digital safety and security training to cultivate cyber resilience among communities as well as digital security training for journalists and human rights defenders.
    g. Development of knowledge products and training materials for community awareness and digital literacy.
    h. Internet governance capacity building at regional and national Schools on Internet Governance (SIGs)[3] and provided by technical organisations.[4]
    i. Mobilising financial resources to support capacity building, particularly among, but not only, non-state actors.
    j. Providing subject matter expertise on emerging cybersecurity issues and their societal impact as the landscape evolves.
    k. Supporting the alignment of cyber related activities by nations and prioritisation by development partners, donor agencies, and other non-state

3The African School on IG (AfriSIG) - www.afrisig.org.
4Aside from many initiatives driven by civil society, ICANN, and the Internet Society also 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

actors in assisting countries to enhance cyber capacity building.[5]

l. Closing the digital divide including the gender digital divide building the capacity of women and girls to be engaged in cyber related activities.
m. 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?

11. Non-state actors including civil society, business and the technical community, can meaningfully and effectively:
    a. Policy analysis and development of model laws and policies.
    b. Integrate a human-centric and human rights approach into ICT security law, policy and regulation.
    c. Develop and promote standards for ICT security
    d. Capacity and skill development - including digital security and cyber hygiene capacity - provided in formal and non-formal contexts.
    e. Development of training materials including for digital safety, security and literacy.
    f. Conduct cybersecurity needs assessments
    g. Convene and participate in community consultations on cybersecurity processes
    h. Convene and participate in consultations with businesses to raise awareness of cyberthreats and security.
    i. Design of programmes to achieve gender equity and equality in the cybersecurity sector.
    j. Design, development and supply of infrastructure, tools and devices to support digital hygiene and cyber resilience, for example blockchain technologies.
    k. Training of technical teams to support the cybersecurity incident response management .
    l. Facilitate and support multistakeholder engagement in policy formulation that is inclusive in nature.

What forms of non-state actor involvement (e.g. contribution of technical resources, co-creation of programmes, contribution of time and expertise of skilled individuals) work well and what forms of stakeholder involvement work less well?

12. Non-state actor involvement that has worked well include:
    a. Contribution of technical and financial resources including specialised expertise.
    b. Co-creation of programmes including organising trainings to build the capacity of actors
    c. Providing expertise including specialised expertise in cyber policy and strategy development processes.
    d. Providing oversight in terms of monitoring and evaluation
    e. Assessment of impact

5For example, the GFCE has a "Clearing House" process that enables recipient countries to prioritise Cyber Capacity needs for assistance.

f. Input into development of structures, legal and policy frameworks.
g. Research to support evidence-based policy making

Non-state actor initiated processes that are not inclusive have not worked well. Lack of resources for sustaining processes over time can also weaken their effectiveness. Cyber capacity-building cannot be done on a 'once-off' basis, it has to be continuous and be integrated into all capacity development linked to digitalisation.

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.

13. We recommend that state and non state actors collaborate to:
    a. Promote awareness at national, regional and international level of cybersecurity as societal security.
    b. Develop and implement comprehensive national cybersecurity strategies, policies and regulations.
    c. 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 .
    d. 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.
    e. Share resources and expertise nationally, sub-regionally and regionally. experts, etc
    f. Develop and implement mechanisms for national, sub-regional, regional and continental collaboration between cybersecurity incidents response team (CSIRT) or Computer emergency response team(CERT).
    g. Establish CSIRTs and CERTs where they are not yet in place.
    h. Provide support for collaboration with non-state actors in the development of national positions and inputs at regional and global ICT security forums.
    i. Review existing frameworks and where applicable establish legislation or regulation to enhance the security and stability of cyberspace.
    j. Develop cybersecurity related standards that address and are accessible to SMMEs.
    k. Enhance coordination and collaboration at national, regional and international level between state and non-state actors, especially within the global South
    l. Enhance the capacity and capability of law enforcement agencies to tackle cybercrime and child online protection at national, regional and international levels.
    m. Enhancing resilience of national Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) by developing and operationalizing national risk mitigation frameworks for identifying national critical assets and sectors.

Proposals for including nonstate 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.

14. In terms of proposals for including non-state actors in concrete action proposals made by states, we recommend:
    a. Inclusive open consultations to gather relevant input from non-state actors 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.
    b. Continuous information sharing by all stakeholders including with and among academic and technical communities
    c. 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
    d. Technical coordination at local, regional and intercontinental level
    e. Strengthening academia to effectively support ICT security research and development
    f. A human centric approach which considers how cyber security affects peoples' well-being, rights, livelihood, environment, culture, belief systems and mindsets
    g. Review of training content for key players involved in cyber incident response plans.

15. Countries should develop requisite capacity to effectively understand and implement the GGE norms on responsible behaviour in cyberspace by states.
16. Member states should use veto power to limit the engagement of non-governmental organisations without ECOSOC accreditation responsibly, proportionally, in a transparent manner and with providing clear case-by-case justifications to others states and the broader community.
17. African governments should contribute to the facilitation and/or 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. Conduct and publish technical reports and white papers (e.g. cyber threat horizon reports etc) on national cyber status of the country
19. Engage stakeholders in developing strategies, policies and regulations that are relevant and comprehensive.
20. 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.
21. 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.
22. 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

Signatories

This statement was developed by the following people who participated in the AfriSIG2022 consultation on African cybersecurity capacity-building priorities held in Lilongwe, Malawi from 16 to 18 July 2022.

Ababacar Diop	JONCTION	Senegal
Abdul-Hakeem Ajijola	African Union Cyber Security Expert Group	Nigeria
Albert Antwi-Boasiako	Cyber Security Authority	Ghana
Anriette Esterhuysen	Association for Progressive Communications	South Africa
Bala Fakandu	Office of the National Security Adviser	Nigeria
David Moepeng	Through InFuture Foundation	Botswana
Margaret Nyambura Ndung'u	PRIDA, African Union Commission	Kenya/ Ethiopia
Edetaen Ojo	Media Rights Agenda	Nigeria
Elizabeth Kolade	Cyber Security Experts Association of Nigeria	Nigeria
Enrico Calandro	Cyber4Dev	South Africa
Frederico Links	Namibia Media Trust	Namibia
Geoffrey R Zgambo	Zambia Police Service	Zambia
Grace Githaiga	KICTANet	Kenya
Jimmy Haguma	Uganda Police Force/Uganda Communications Commission	Uganda
Khadijah El-Usman	Paradigm Initiative	Nigeria
Lillian Nalwoga	CIPESA	Uganda
Martin Koyabe	The Global Forum on Cyber Expertise	Kenya / Netherlands
Moses Owiny	Centre for Multilateral Affairs	Uganda
Muheeb Saeed	Media Foundation West Africa	Ghana
Nompilo Simanje	MISA Zimbabwe	Zimbabwe
Obioma Okonkwo	Media Rights Agenda	Nigeria
Peterking Quaye	West African ICT Action Network	Liberia
Ruby Khela	Global Partners Digital	UK
Sheetal Kumar	Global Partners Digital	UK
Thobekile Matimbe	Paradigm Initiative	Zimbabwe
Victor Kapiyo	KICTANet	Kenya