AFRICA AGENDA FOR CYBER CAPACITY BUILDING (AA - CCB)

FROM AWARENESS TO CAPABILITY

GFCE

GLOBAL FORUM ON CYBER EXPERTISE

Table of Contents

Introduction

In today's digital age, the pervasive integration and dependency on technology in our lives has led to a surge of our exposure to vulnerabilities, with cyber threats escalating globally, targeting businesses, governments, and individuals.

In Africa, this trend is equally evident, with a rising tide of cybercrime wreaking havoc on livelihoods, economic stability, and national sovereignty. Cyberattacks have targeted all entities and institutions across the continent, imposing substantial financial losses on African countries.

While progress has been made in recent years, many African nations still struggle with inadequate cybersecurity infrastructure. This includes a shortage of skilled cybersecurity professionals, limited access to cybersecurity tools and technologies, and insufficient government investment in cybersecurity.

To tackle the digital challenge, Africa must invest in its youth through cyber capacity-building (CCB) programs, strengthening educational institutions and partnering with experts to equip them as cyber guardians. Innovation should be fostered to develop cutting-edge cybersecurity solutions, supporting startups and entrepreneurs within a thriving ecosystem.

Governments must adopt comprehensive cybersecurity policies and allocate resources to protect critical infrastructure. Africa should also collaborate internationally to share threat intelligence and combat cybercrime globally.

The Africa Cyber Capacity Building (CCB) Coordination Committee was established in 2021 to be Africa's leading consultative forum for CCB programs and initiatives in Africa, including the AU-GFCE Collaboration project (1). The committee is composed of more than 15 members drawn from leading African organizations (2) representing various stakeholder interests in cybersecurity and ICT in Africa.

Introduction

Based on the priority needs identified by AU member states during their engagement within the AU-GFCE Collaboration project, as well as additional inputs gathered from various stakeholders with similar CCB programs and initiatives on the continent, the Africa CCB Coordination Committee drafted this Africa Agenda on Cyber Capacity Building (AA-CCB). The AA-CCB is a document which advances actions and priorities that aims to enhance coordination and identification of successful policies, practices, and ideas for CCB programs and initiatives in Africa.

With a population of over 1.3 billion people and over 590 million registered Internet users, Africa is experiencing an ongoing digital revolution. Projections point to an Internet economy with the potential to reach US$180 Billion by 2025, and more than triple to US$712 Billion by 2050. This digital transformation, accompanied by an unprecedented population growth, is being threatened by an exponential growth in cybercrime and related cyber threats.

According to a 2022 report by INTERPOL, Africa is witnessing increases in illicit drug and human trafficking, organized crime, terrorism, financial crime and corruption. This increasing cyber threat landscape is in one way or another leveraged by phishing, ransomware, botnets and other forms of social engineering. Building the cyber capacities of state and non-state actors proves to be essential for the continent.

Background

Cognizant to the fact that cyber capacity, cybersecurity and cyber resilience play a significant role in supporting economic and social prosperity for the continent, there are several actors with CCB programs and initiatives on the continent.

At the continental level, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, or Malabo Convention which entered into force in June 2023. The convention is seen as a pivotal instrument for the attainment of resilient digital economies aligned to the Digital Transformation Strategy for Africa 2020 - 2030 for supporting e-commerce, e-services and free movement of people, goods and services, as envisioned in the African Continental Free Trade Area (AfCFTA) agreement.

At the sub-continental level, regional economic communities (RECs) and other regional institutions are developing and enacting various strategies, policy frameworks and initiatives complementary to the AU. The Economic Community of West African States (ECOWAS), for instance, has drafted several instruments that seek to harmonize personal data protection, electronic transaction, and cybercrime provisions within West Africa, including the ECOWAS Regional Cybersecurity and Cybercrime Strategy, adopted in 2021.

Similarly, the Southern African Development Community (SADC) developed the SADC Harmonized Cybersecurity Legal and Regulatory Framework consisting of 3 model laws on e-commerce, data protection and cybercrime. With support from UNCTAD, the East African Community (EAC) developed the Framework for Cyberlaws in 2008, which recommends the harmonization of legal reforms within East African partner states and the observance of international best practices. Furthermore, UNECA launched a Guideline for a Model Law on Cybersecurity, providing a comprehensive framework for cybersecurity. This model law sets out guidelines to establish a unified cyber norm across continents, enabling African member states to proactively combat cyber threats (3).

On a practical level, the implementation of the achievements listed above is being addressed by numerous CCB partners, implementors and collaborators working in different nations and regions within the continent. Launched in 2020, the Smart Africa Digital Academy has been rolled out to 6 countries (4) in which citizens can gain or improve their digital skills and gain qualifications to meet the emerging talent needs of employers or the industry.

In addition, Smart Africa in collaboration with key stakeholders, has developed the Continental Cybersecurity Blueprint to better identify and address cybersecurity challenges in the African perspective. The blueprint outlines essential guidelines and recommendations that aim to assist in developing or updating of Cybersecurity strategies at national, regional and continental levels.

One of the key outcomes from the AU-GFCE collaboration, was the establishment of the Network of African Women in Cybersecurity (NAWC). NAWC is composed of experienced women professionals from the African region, who aim to provide expert advice and technical guidance at various levels at national, regional and continental level. The objective is to address existing gaps in gender-responsive cybersecurity planning, development and implementation in Africa, focusing on the specific needs of women and girls in the process.

In 2022 UNECA announced several CCB activities, including the launching of the Connected African Girls Initiative which aims to empower African girls between the ages of 12 and 25 in STEM fields, including cybersecurity and online safety, ensuring they are prepared for the challenges of the Fourth Industrial Revolution. And then there is the AU-GFCE Collaboration project, implemented jointly by the Global Forum on Cyber Expertise (GFCE) and African Union Development Agency New Partnership for Africa's Development (AUDA-NEPAD) between 2021 and 2022. This project conducted a baseline analysis of cyber capacity building gaps and priorities of more than 30 AU member states.

The analysis of the CCB initiatives and programs indicate that while Africa's CCB initiatives are far and many, the divergence in levels of cyber security maturity and resilience across AU member states, and regions, is evident. Additionally, higher vulnerability of one state or region to cyber threats can have spill-over effects to other AU member states. Thus, CCB programming needs to have a clear roadmap pointing to priorities for the continent, as well as political support at the highest level. Given the importance of cyber capacity building as an instrument of cooperation for a free, open, peaceful and secure Internet, this document proposes the adoption of an Africa Agenda on Cyber Capacity Building (AA-CCB).

OBJECTIVES AND GUIDING PRINCIPLES OF THE AA-CCB

The objective of the AA-CCB is to propose strategic goals and priorities for CCB action in Africa. To achieve this, a review of AU-Member states' CCB needs and priorities gathered by the AU-GFCE Collaboration project was used, as well as expert inputs from members of the Africa CCB Coordination Committee. The final product is a document that represents a collective vision and roadmap for coordinated CCB action in Africa.

Bearing in mind the London process and its outcomes related to CCB, the AA-CCB is founded on the guiding principles of the UN General Assembly Resolution on ICT for Development (71/212), as well as the UN General Assembly Resolutions on the Creation of a Global Culture of Cybersecurity (57/239, 58/199, 64/211), the African Union Convention on Cyber Security and Personal Data Protection and the 2017 African Declaration on Internet Governance, the Hague Declaration and the Delhi Declaration.

Thereby, the guiding principles include:

1. Advocating for open, transparent, interoperable and inclusive cyberspace where human rights are respected, in particular freedom of expression, private life, and universal access.

2. Strengthening a multistakeholder approach involving governments, civil society, the private sector and the technical community.

3. Adopting shared responsibility, accomplished through national, regional, continental and international collaboration and cooperation.

4. Developing local expertise through using and creating regional expertise (capacity building multipliers).

5. Efficient and effective coordination and collaboration between development partners and donor, with countries in need of funding or technical assistance, avoiding duplicity and wastage of resources.

Identified priority needs

The strategic goals and actions of the AA-CCB are based on the priority needs identified by AU member states during their engagement during the AU-GFCE Collaboration project, as well as engagements with various key stakeholders with CCB programs and initiatives on the continent.

These priority needs included:

1. Facilitate the development and amendment of national cybersecurity strategy adopted by each African country.
2. Advocate for the establishment of national cybersecurity legislation, policies and regulatory framework.
3. Advocate for the establishment and support national, regional and continental computer emergency/incident response teams.
4. Enhancing regional and international cooperation.
5. Bolster educational institutions and building sustainable cybersecurity ecosystem and industry.
6. Increase investment in cyber in terms of funding and mobilizing resources.

Proposed strategic outcomes

The strategic goals of the AA-CCB are based on the priority needs identified by AU member states during their engagement during the AU-GFCE Collaboration project, as well as engagements with various key stakeholders with CCB programs and initiatives on the continent.

The AA-CCB has the following strategic goals which can be accomplished through the execution of the priority actions as detailed below:

1 Assessments and Development of National Cybersecurity Strategies

Action 1.1: Support the adoption of continental frameworks to enable African countries to develop or enhance their Cybersecurity strategies at national, regional and continental levels.

Action 1.2: Strengthen national capacities for the implementation of the agreed norms of responsible state behaviour.

Action 1.3: Promote the development of a cybersecurity strategy or framework, respectful of human rights and fundamental freedoms, in each AU member state.

2 Legislation, Policies, Regulations and Standards

Action 2.1: Strengthen institutional and legal frameworks to detect, prevent, and respond to cyber incidents and crises, including at regional and international levels.

Action 2.2: Support the development of standards, norms, institutional and regulatory frameworks for strengthening cyber resilience of critical digital services and critical sectors (e.g., finance, health, energy and education).

Action 2.3: Encourage appropriate and robust legislation, policy and regulatory framework that would promote a secure cyber space.

3 CIIP/CIP, CERTS/CSIRTS & Incident Management

Action 3.1: Facilitate the development of a secure information infrastructure across the continent to support safe access to the Internet and ensure the implementation of the AU agenda 2063 and the Digital Transformation Strategy for Africa (2020-2030).

Action 3.2: Support identification of critical information infrastructure and entities responsible for their functioning, those relevant in a broader regional and/or the continental context

Action 3.3: Strengthen institutional and legal frameworks to detect, prevent, and respond to cyber incidents and crises, including at regional and international levels.

4 Capacity Building, Awareness and Outreach

Action 4.1: Promote the establishment of regional matchmaking programs to encourage South-South knowledge-sharing regarding development of cyber capacities.

Action 4.2: Develop and implement strategy to raise awareness among the relevant target groups on cyber threats.

5 Technical Capabilities, Skills, Research & Development

Action 5.1: Leverage existing learning modules, lessons learned and good practices from national and regional CCB projects into the African Union Cyber Security Expert Group (AUCSEG), the Africa Cybersecurity Expert (ACE) community, and other peer-to-peer working groups that support the regional and sub-regional implementation of CCB initiatives.

Action 5.2: Promote inclusivity of women, youth, marginalized and minorities in cybersecurity education, training, and workforce development.

Action 5.3: Support and connect workforce development programs to professionalize cyber as a profession in Africa.

Action 5.4: Promote the establishment of cyber educational curricula at primary and tertiary level.

Action 5.5: Develop and expand the body of knowledge through the development of practical products, tools, guidelines, and knowledge on CCB for Africa.

6 National, Regional, and International Collaboration, Cooperation and Partnerships

Action 6.1: Promote the establishment of regional matchmaking programs to encourage South-South knowledge-sharing regarding development of cyber capacities.

Action 6.2: Foster and support national cyber diplomacy capacities and regional coalitions of an integrated continent capable of advocating united positions based on the ideals of Pan Africanism at international negotiation forums.

Action 6.3: Strengthen judicial and law enforcement cybercrime capacities and cooperation among them, including at regional and international levels.

Action 6.4: Promote development of public-private partnerships, multistakeholder and international partnerships for cyber incident and crisis management.

Action 6.5: Encourage the establish a national competent authority for coordination of cybersecurity policies and procedures.

7 Funding and Resource Mobilisation

Action 7.1: Increase investment in Cybersecurity, in order to effectively secure the digital infrastructure and Cyber space.

Action 7.2: Encourage investment within the continent on cybersecurity research and development capacity, centres of excellence and Cyber hubs.

Action 7.3: Promote and develop incentives to improve delivery of competitive cybersecurity products and services at national, regional, and continental.

Governance structure

The Africa Cyber Capacity Building (CCB) Coordination Committee prepared this AA-CCB in coordination with the GFCE Africa team and shall continue providing general oversight on its implementation.

The Africa CCB Coordination Committee is comprised of representatives from institutions representing various stakeholder interests in Information and Communications Technology (ICT) and Cybersecurity in Africa. These institutions include the African Union Commission, the Regional Economic Communities (SADC, EAC, ECCAS, ECOWAS, UMA, COMESA, IGAD, CENSAD), AU specialized institutions (ATU, AUDA-NEPAD, ACBF, AFRIPOL), UNECA, some relevant Africa Tech institutions (AfricaCERT, AFRINIC, ZACR,) regional associations of regulators (CRASA, EACO, WATRA, ARTAC, ARICEA), regional research and education networks (WACREN, UbuntuNet Alliance, ASREN), Network of African Women in Cyber security (NAWC). Networks of African Cybersecurity Agencies (NACSA).

The GFCE Africa Hub and the GFCE Secretariat are mandated to operationalize the AA-CCB in coordination with the Africa CCB Coordination Committee, the GFCE Communities, Members and partners involved in CCB in Africa while the Africa CCB Coordination Committee will perform the monitoring and evaluation of the AA-CCB and report the results to both the African Union Commission and the GFCE Secretariat on an annual basis.

The establishment of the GFCE Africa Hub marks a crucial endeavor to secure Africa's digital future in the midst of rapid technological advancements. Focusing on three key challenges, the GFCE Africa Hub aims to pioneer proactive security programs, promote harmonized security practices, and enhance the effective utilization of available data.

By collaborating with African countries and fostering a proactive cybersecurity mindset through education, real-time threat intelligence sharing, and the removal of silos, the hub aspires to lead Africa from a reactive to a proactive cybersecurity model. Its strategy emphasizes unity of actions, knowledge-sharing, and resource accessibility, paving the way for a digitally secure and resilient Africa, underpinned by a commitment to education, collaboration, and data-driven analysis.

Resource mobilization

It is envisaged that stakeholders of the AA-CCB will work together to mobilize resources and expertise for the activities described above, leveraging existing platforms and relationships, as well as global events on CCB, including the Global Conference on Cyber Capacity Building (GC3B) which aims to mainstream cyber resilience and capacity building in the international development agenda.

Stakeholders may include international development agencies, international or African organizations, or private sector partners. Their contributions will differ and could be either in cash or in kind, such as offering content, expertise, and other means of contribution.

The GFCE Africa Hub Mobilization strategy for the implementation of AA-CCB shall be part of the above overall resource mobilization strategy of the Global Forum on Cyber Expertise (GFCE) with focus special on African development and funding institutions. The objective is to have these institutions provide resources for the implementation by the Africa Hub of AA-CCB. A resource mobilization strategy and plan for the would be critical to support its mission and activities related to strengthening international cooperation on cybersecurity capacity building.

References & Contact

1. The AU-GFCE Collaboration project was implemented jointly by the Global Forum on Cyber Expertise (GFCE) and African Union Development Agency New Partnership for Africa's Development (AUDA-NEPAD) between 2021 and 2022 to conduct a baseline analysis of cyber capacity building gaps and priorities of 55 AU member states. The needs and challenges were subsequently used to develop relevant knowledge modules and knowledge products that have been put at the disposal of all AU member states and stakeholders.
2. AFRINIC, AfricCERT, Registry Africa, AUCSEG, EAC, CRASA, UNECA, IGAD, AUC, ECOWAS, WACREN.
3. https://www.uneca.org/stories/eca-launches-the-guideline-for-a-model-law-on-cybersecurity-during-the-17th-igf
4. The Republic of Congo, Rwanda, Ghana, Benin, Sierra Leone and Côte D'Ivoire.

For more information, please reach out to africahub@thegfce.org. The Africa Hub team welcomes any inquiries and proposals.

Stay updated with our news by checking our website at: gfce.org and follow @thegfce and #theGFCE hashtag on social media.

@thegfce

GFCE GLOBAL FORUM ON CYBER EXPERTISE

GFCE AFRICA HUB