AFRICA CENTER FOR STRATEGIC STUDIES

25 YEARS

U.S. DEPARTMENT of STATE

Advancing Regional Cyber Security and Stability in Africa

May 2024

READ-AHEAD

May 21-23, 2024

ADVANCING REGIONAL CYBER SECURITY AND STABILTY IN AFRICA

READ-AHEAD

TABLE OF CONTENTS

Port Louis, Mauritius
21-23 May 2024

Program Overview **3**

Session 1: Advancing International Security and Stability in Cyberspace: Challenges and Opportunities **5**

Session 2: Advancing Regional Cyber Security and Stability in Africa **7**

Session 3: Taking Stock of Africa's Regional Cyber Security Architecture **8**

Session 4: Taking Stock of Regional Economic Community (REC)-Led Cyber Security and Stability Initiatives **10**

Session 5: Advancing National and Regional Computer Emergency Response Architectures Across Africa **11**

Session 6: Advancing U.S.-Africa Cybersecurity Cooperation **12**

Working Group Guidance: Recommendations for Advancing Africa's Cybersecurity Architecture **13**

Program Overview

Introduction

The African region faces a diverse, expanding array of cyber threats, from state actors who conduct cyberattacks for geopolitical gain to cybercriminal networks that exploit Africa's increasingly digitally dependent financial architecture in pursuit of profit. The UN Framework for Responsible State Behavior in Cyberspace,[1] forms the backbone of global efforts to promote stability and security in cyberspace. The framework includes the application of international law to cyberspace, voluntary norms, and confidence building measures. Embedded in the voluntary non-binding norms are commitments to protect critical infrastructure, including by taking feasible steps to mitigate malicious activity occurring within a state's jurisdiction and to facilitate international cooperation to prevent and combat cybercrime.

By navigating differences in capabilities and divergent interests among member States, Africa's regional bodies play a crucial role in coordinating the efforts of their member states to implement the UN Framework. The African Union (AU) and Regional Economic Communities (RECs) have, for example, facilitated the adoption of the Malabo Convention to enable its members to assist one another in detecting and responding to cross-border cybersecurity threats[2]; drafted common positions and model laws to enable African countries to defend cyberspace in line with international legal standards; and provided technical assistance to build out the continent's emergency computer response infrastructure.

While the foundations of a multilateral cybersecurity architecture in the African region are being laid, there is a need to improve mechanisms for cooperation and refine other aspects of how the AU, RECs, individual states, and external actors work to ensure and advance their shared interests in a safe, secure cyberspace. At this workshop, key stakeholders from the AU, RECs, and African states will share insights and identify opportunities to build cyber capacity at Africa's regional institutions to implement the UN Framework and advance confidence, coordination, and trust in cyberspace among member states. As well as considering multilateral African structures and initiatives, the workshop will also identify opportunities for effective cooperation and support for these efforts from the United States.

By the end of this 3-day leadership and expert level workshop we hope to capture consolidated insights, lessons learned, and recommendations to strengthen growing regional cybersecurity cooperation mechanisms in line with national need and interests. To this end, there will be facilitated small group discussions throughout the event, and the program will conclude with briefings to the plenary by each discussion group.

[1] United Nations General Assembly (UNGA). *Final Substantive Report Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[2] African Union. "Malabo Convention on Cyber Security and Personal Data Protection." Adopted July 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Program Objectives

The objectives of the workshop are to:

1. Convene the AU, RECs, and key African states to share insights, good practices, and lessons learned from their efforts to build cyber capacity and improve cooperation in cyberspace amongst themselves.
2. Informed by examples of successful regionally led initiatives to build cyber capacity, generate recommendations for advancing Africa's regional cybersecurity institutions and architecture in alignment with the UN framework.
3. Catalyze progress towards implementing the recommendations identified and discussed by program attendees.

Workshop Components and Approach

Drawing on the many decades of expertise present, this workshop will seek to capture important lessons and sound practices through:

- *Plenary sessions* led by seasoned practitioners and experts, focused on collaborative, two-way learning.
- *Academic content* focused on evidence-based analysis supported by practical examples.
- *Group discussions* that provide a trusted platform for participants to network and share their perspectives on the program content.
- *Strategic dialogue* with representatives and participants from the United States to help inform U.S. policy in support of Africa's regional cybersecurity institutions.

The workshop will succeed only with honest analysis and productive dialogue. To this end, the Africa Center for Strategic Studies (ACSS) seeks to provide empirical evidence to facilitate frank and open exchange on critical issues, as well as to lay the foundation for effective peer networking. To facilitate learning, we provide this read-ahead and recommended readings. We encourage participants to familiarize themselves with the materials in advance of the workshop so they can actively engage with the other participants. The readings are intended to foster a healthy dialogue on a wide range of African cybersecurity challenges, and to spark discussion of how regional actors can work in concert with national and international actors to address them. ***To allow for candid discussion of sensitive issues, this workshop will be conducted in its entirety under a strict policy of non-attribution, which is binding during and after the seminar.***

Preparation for the Workshop

Before the workshop, we ask participants to:

1. Skim this read-ahead before traveling to the workshop and spend time thinking about the discussion questions and conferring with colleagues, if helpful.

2. Review each portion of the read-ahead and recommended readings the day prior to each session and note for yourself any questions, comments, or experiences you would like to share.

Day 1: Perspectives on Advancing Stability and Security in Cyberspace

Session 1: Advancing International Security and Stability in Cyberspace: Challenges and Opportunities

Objectives:

- Provide an overview of international efforts to maintain global peace and security in cyberspace by advancing norms, applying international law, promoting confidence-building measures – and a common understanding of the need for capacity building.
- Discuss the challenges and opportunities these efforts face internationally and in Africa.

Background:

On seven occasions beginning in 2003, the U.N. General Assembly established groups of governmental experts (GGEs) to study State use of ICTs. Across three cumulative consensus reports (2010, 2013, 2015), the GGEs laid out an initial framework for responsible State behavior in cyberspace by which, in General Assembly resolution 70/237, all Member States agreed to be guided. This same framework was reaffirmed by the U.N.'s Open-Ended Working Group[3] as the foundation for further global work toward a peaceful and secure cyber domain.

There are three main components to this framework. First, states have agreed on the application of international law to the ICT environment. Second, they have agreed to the implementation of confidence-building measures, including regular consultations and the establishment of points of contact (PoCs) to promote transparency and information sharing. Third, the framework contains 11 voluntary, non-binding norms of responsible state behavior in the use of ICTs, including:

1) Cooperate to increase security and stability in the use of ICTs.
2) Consider all relevant information when attributing a cyber incident.
3) Do not knowingly allow the use of ICTs for intentionally wrongful acts.
4) Cooperate to address the terrorist and criminal use of ICTs.
5) Respect human rights.
6) Do not use ICTs to damage or impair the use of another state's critical infrastructure to provide services to the public.
7) Protect critical infrastructure within their territories from ICT threats.
8) Respond to requests for assistance from States whose critical infrastructure is subject to malicious cyber activity.
9) Ensure supply chain security.
10) Encourage responsible reporting of ICT-related vulnerabilities.
11) Do not harm computer emergency response teams (CERTs) and do not use CERTs to engage in malicious cyber activity.[3]

The African region played an important role in negotiating the framework, and in raising awareness of the importance of building international cyber capacity to implement it, including through the establishment of national cybersecurity strategies, programs, policies, and computer emergency response teams. Because of growing internet penetration rates, increasing influence in international institutions, and advances in cyber awareness and capacity, African countries are

[3] UNGA, *Consensus Report of United Nations Group of Governmental Experts (UN GGE)* July 2015, https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False

likely to have a decisive impact on the framework's implementation. And while the framework has been universally agreed to, implementation has been a challenge. This is due to a variety of issues, from limited cyber capacity in some regions of the world, ambiguity with respect to how to apply human rights and international legal norms to cyberspace, and an increasingly fractious global geopolitical environment.

Recommended Readings:

United Nations General Assembly (UNGA). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. July 2021, A/76/135,https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135&Language=E&DeviceType=Desktop&LangRequested=False

Bart Hogeveen, "The UN Norms of Responsible Behavior in Cyberspace." Australia Strategic Policy Institute, March 2022, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

Louise Marie-Hurl, "The Rocky Road to Cyber Norms at the United Nations," Council on Foreign Relations Net Politics Blog, September 2022, https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0

African Union Peace and Security Council, "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace," January 2024, https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

Session 2: Advancing Regional Cyber Security and Stability in Africa

Objectives:

- Take stock of existing region-wide efforts to promote peace, security, and stability in cyberspace.
- Discuss the comparative advantages, roles and responsibilities of national and regional actors in Africa in advancing cyber stability.
- Identify gaps in Africa's regional cyber security architecture and identify opportunities for further areas of capacity and confidence-building measures to take place.

Background:

Though Africa is the world's least digitized region, there is significant variation in cyber capabilities across the region. Seven African countries are among the world's top 50 most committed to cybersecurity, according to the International Telecommunications Union, including Mauritius, which is tied with Norway for the 17th spot.[4] Led by the African Union and Regional Economic Communities such as the Economic Community of West African States (ECOWAS), Africa's regional cybersecurity architecture is arguably the most vibrant and advanced of any region outside of Europe.

For Africa's regional institutions to maximize their growing role in promoting peace, security, and stability in cyberspace will require not only the acquisition of capabilities and capacity. It will also require the AU, the RECs, and other multilateral organizations to strategically leverage their convening and coordinating powers in the interests of member states. This involves careful thinking about the interests of those member states, the threats sub-regional and regional institutions are best equipped to address, and the potential partnership opportunities that exist with bilateral, multilateral, private sector, and non-profit entities.

Recommended Readings:

Nnenna Ifeanyi-Ajufo, "Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation" *Policy Design and Practice* 6:2, 146-159, https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2199960

Mailyn Fidler, "Infrastructure, Law, and Cyber Stability: An African Case Study." Chesney et al., eds *Cyber Stability and Instability,* 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897108

Nathaniel Allen and Noëlle van der Waag Cowling, "How African States Can Tackle State-backed Cyber Threats," July 15, 2021, https://www.brookings.edu/articles/how-african-states-can-tackle-state-backed-cyber-threats/

[4] International Telecommunications Union (ITU). 2020 Global Cybersecurity Index (GCI). ITU 2024, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E . The others include Egypt (23), Tanzania (37), Ghana (43), Tunisia (45), Nigeria (47), and Morocco (50). Kenya is #51.

Day 2: Advancing Africa's Cybersecurity Infrastructure

Session 3: Taking Stock of Africa's Regional Cyber Security Architecture

Objectives:

- Outline existing AU-led efforts to advance regional cyber security and stability in Africa.
- Identify challenges and gaps.
- Brainstorm and discuss steps for the AU, the international community, and the United States to further advance AU-led cyber security initiatives.

Background:

Over the past decade, the AU has supported or launched numerous initiatives to advance the interests of its member states in cyberspace. These include:

- The 2014 drafting and 2023 entry into force of the AU Convention on Cybersecurity and Personal Data Protection, also called the "Malabo" convention.[5] It remains the only regional cybersecurity treaty currently in existence. While an impressive achievement, the Malabo Convention remains ratified by only 15 member states. The Council of Europe's Budapest Convention on Cybercrime, a multilateral treaty designed to be global in nature and open to all countries, complements the provisions of the Malabo Convention. The United States and, as of March 2024, eight African countries are parties to Budapest.

- The 2024 adoption of a Common African Position (CAP) on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace.[6] This is an important contribution to ongoing, global discussions over how best to apply international law to cyberspace, a pillar of the framework for Responsible State Behavior.

- The adoption of Cyber Security as a 'Flagship Project' of the African Union's Agenda 2063. With implementation being led by the African Union Development Agency-NEPAD (AUDA-NEPAD), this marks a recognition that Africa's economic future depends on a safe, secure, and reliable cyberspace.

These initiatives, as well as others such as the adoption of regional data protection guidelines and the establishment of the AU Cyber Security Experts Groups (AUCSEG), demonstrate the growing, cross-cutting importance of cybersecurity to the AU and its member states. The task now is for the AU to strengthen and build on these important initiatives, while navigating sometimes fractious and divergent views and interests among its member states and other members of the global community regarding interstate behavior and cooperation in cyberspace.

[5] African Union. "Malabo Convention on Cyber Security and Personal Data Protection." Adopted July 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[6] African Union Peace and Security Council, "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace," January 2024, https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

Recommended Readings:

Nnenna Ifyeani-Ajufo. "The AU Took Important Action on Cybersecurity at its 2024 Summit – but More is Needed," Chatham House, 23 February 2024, https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed

ALT Advisory, "Africa: AU's Malabo Convention Set to Enter Force After Nine Years," 19 May 2023, https://altadvisory.africa/2023/05/19/malabo-convention-set-to-enter-force/

AUDA-NEPAD, "AUDA-NEPAD Cybersecurity Assessment Report,"23 December 2020, https://www.au-pida.org/download/cybersecurity-assessment-report/

Nate Allen, Matthew La Lime, and Tomslin Samme-Nlar, *The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats*, Global Initiative Against Transnational Organized Crime, 2 December 2022, pp. 52-53, https://globalinitiative.net/analysis/digital-revolution-africa-cyber-threats/

Session 4: Taking Stock of Regional Economic Community (REC)-Led Cyber Security and Stability Initiatives

Objectives:

- Outline existing REC-led efforts to advance regional cyber security and stability in Africa.
- Identify good practices, challenges and gaps.
- Brainstorm and discuss steps for the RECs, the international community, and the United States to further advance REC-led cyber security initiatives.

Background:

Africa's Regional Economic Communities (RECs) have played varying roles in advancing cybersecurity policy, strategy and cooperation in their regions. By far the most active REC on cybersecurity in Africa has been the Economic Community of West African States (ECOWAS), which has adopted a regional cybersecurity strategy, drafted and influenced the adoption of model cybersecurity legislation among its member states, and, in partnership with the European Union, launched an initiative to address cybercrime in West Africa. Other RECs, including the Southern African Development Community (SADC) and East African Community (EAC) have adopted model laws and legislation on issues such as cybercrime, cybersecurity and data protection. Others, such as the Intergovernmental Authority on Development (IGAD), are in the process of considering how cybersecurity challenges faced by their member states might benefit from a regionalized approach.

Because of limited resources, the truly global scope and scale of the cybersecurity challenge, and at-times contentious relations within each region, REC leaders may need to be particularly selective with respect to which cybersecurity challenges on which they engage. On certain issues, such as cyber-enabled threats from non-state actors that span borders within their regions or the adoption of model laws that reflect regional interests and needs, African states may benefit from a more regionalized approach to cybersecurity. On others, it may be more prudent for member states to work bilaterally or defer to regional or international bodies.

Recommended Readings:

Economic Community of West African States, "ECOWAS Regional Cybersecurity and Cybercrime Strategy," February 2021, https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf

Intergovernmental Authority on Development (IGAD), "IGAD SSP Holds IGAD Regional Conference on the Existing Cybersecurity Frameworks of all IGAD Member States," 8 July 2023, https://igad.int/igad-ssp-holds-gad-regional-conference-on-the-existing-cybersecurity-frameworks-of-all-igad-member-states/

The NATO Cooperative Cyber Defence Centre of Excellence, "South African Development Community," https://ccdcoe.org/organisations/sadc/

MISA-Zimbabwe, "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights," 2021, https://cybilportal.org/publications/cybersecurity-and-cybercrime-laws-in-the-sadc-region-implications-on-human-rights/

Session 5: Advancing National and Regional Computer Emergency Response Architectures Across Africa

Objectives:

- Take stock of existing efforts by national and regional actors to develop computer emergency response capabilities suited to the threat and environment in Africa.
- Identify challenges and gaps.
- Brainstorm and discuss how national and regional actors can work together to further bolster Africa's CERTs.

Background:

CERTs, at times referred to as Computer Security Incident Response Teams (CSIRTs), are critical nodes within any nation's cybersecurity ecosystem. As centers of technical excellence and expertise, national CERTs often play a central role in raising cybersecurity awareness, monitoring internet traffic for threats, protecting and enabling the recovery of critical information infrastructure in the event of an attack, and responding to requests for international cooperation and assistance. So essential are CERTs that one of the UN norms counsels that States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State [17]

The CERT landscape in Africa is diverse and rapidly changing. The majority of African countries have yet to establish a national CERT, but the number of national CERTs in Africa grew by nearly 50 percent between 2018 and 2021, from 13 to 19.[8] Some countries, such as Ghana, Egypt, and Mauritius, possess robust CERT and CII protection infrastructures. Organizations such as the global Forum of Incident Response and Security Teams and AfricaCERT have for more than a decade been involved in helping to found, build capacity, and exchange good practices among CERTs based in Africa. Support from donor countries via implementing expert partners has also been integral. Moving forward, these entities need to move beyond a focus just on building capacity and consider broader opportunities for collaboration and partnership with multilateral organizations, national governments, and key bilateral partners.

Recommended Readings:

Internet Society and African Union Commission (AUC), *Internet Infrastructure Security Guidelines for Africa*, 24 May 2017, https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

Jean-Robert Hountomey, Hayretdin Bahsi, Unal Tatar, Sherif Hashem & Elisabeth Dubois, *Cyber Incident Management in Low-Income Countries*, AfricaCERT and the Global Forum on Cyber Expertise (GFCE), 2022, https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/

Nate Allen, Sherif Hashem, and Elizabeth Kolade, "'Leapfrogging' or 'lagging'?: highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria," forthcoming, *Journal of Cyber Policy*, https://doi.org/10.1080/23738871.2024.2304560

[7]UNGA, *Consensus Report of United Nations Group of Governmental Experts (UN GGE)* July 2015, https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False

[8] ITU, *2020 Global Cybersecurity Index* (GCI), https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, p. 7

Day 3: Advancing U.S. – Africa Cybersecurity Cooperation

Session 6: Advancing U.S.-Africa Cybersecurity Cooperation

Objectives:

- Take stock of existing U.S.-Africa cybersecurity cooperation efforts being taken by the State Department, the Defense Department, and the Department of Homeland Security.
- Identify additional areas for partnership, focusing on opportunities for regional cooperation and multilateral partnerships.

Background:

For close to two decades, the cornerstone of U.S. international cyberspace policy has been to support an open, interoperable, reliable and secure internet. In Africa, it has emphasized achieving these objectives by seeking to implement the UN framework and by assisting partner nations to strengthen their national cybersecurity through a whole-of-government, multistakeholder approach. Cybersecurity in Africa is of growing interest to U.S. foreign policy. Launched in 2022 at the U.S.-Africa Leaders Summit, the White House's signature Digital Transformation with the Africa (DTA) Initiative includes promoting governance and regulation to ensure a secure digital enabling environment as among the Initiative's key objectives.[9] In 2023, cyber was featured for the first time during U.S. Africa Command's Justified Accord Military exercise in Kenya.[10] The United States has held bilateral cyber and digital dialogues with Kenya and South Africa.

With Africa's rapid digitization, increasing influence in global affairs, and growing cyber capabilities in many countries, the United States and its many partners across the African region have a vested interest in deepening this cooperation. Considering opportunities for deepened collaboration not only depends on identifying areas of mutual interest, but also in considering areas where cooperation with or technical assistance from the United States may have comparative advantages to African states and regional organizations.

Recommended Readings:

U.S. Department of State, "Declaration for the Future of the Internet," 28 April 2022, https://www.state.gov/declaration-for-the-future-of-the-internet

The White House, "FACT SHEET: New Initiative on Digital Transformation with Africa (DTA)," 4 December 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/

Colin Demarest, "Cyber to be Featured for First Time at US Military Exercise in Africa," C4ISRNet, 22 December 2022, https://www.c4isrnet.com/cyber/2022/12/22/cyber-to-be-featured-for-first-time-at-us-military-exercise-in-africa/

[9] The White House, "FACT SHEET: New Initiative on Digital Transformation with Africa (DTA)," 4 December 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/

[10] Colin Demarest, "Cyber to be Featured for First Time at US Military Exercise in Africa," C4ISRNet, 22 December 2022, https://www.c4isrnet.com/cyber/2022/12/22/cyber-to-be-featured-for-first-time-at-us-military-exercise-in-africa/

Working Group Guidance: Recommendations for Advancing Africa's Cybersecurity Architecture

Objectives:

- Share key insights and lessons learned in discussion that are relevant to the entire group.
- Develop a complete and shared assessment of Africa's cybersecurity architecture including the regional level (AU), sub-regional level (RECs & others), and national level and how these pieces fit together.
- Capture recommendations for how to expand, change, revise or improve Africa's existing regional and sub-regional cybersecurity architecture in alignment with the framework.
- Identify opportunities for partnership between African governments, regional institutions, and the United States to implement proposed recommendations.

Background:

A key component of this workshop will include a series of "working" discussion groups which will generate recommendations to advance Africa's regional cybersecurity architecture in alignment with the framework and in partnership with the key actors and institutions present. The working groups will comprise approximately 10 participants each and will be curated to include a combination of stakeholders from multilateral institutions, African governments, experts, and U.S.-based participants.

Over the course of three meetings, participants in these working groups will: 1) identify what they consider to be Africa's most significant cyber threats, 2) take stock of Africa's regional cybersecurity architecture, and 3) devise specific recommendations for the AU, the RECs and their countries to, in partnership with the United States and other actors, advance Africa's regional cybersecurity architecture in alignment with the framework.

At the back brief session on the final day, groups will present their findings and recommendations to a panel of experts, who provide feedback and foster further discussion. More specific instructions regarding the conduct of the working groups accompanies this read-ahead.