AFRICA CENTER FOR STRATEGIC STUDIES
25 YEARS
IMPACT THROUGH INSIGHT

ADVANCING REGIONAL CYBER SECURITY AND STABILITY IN AFRICA WORKSHOP

EXECUTIVE SUMMARY

PORT LOUIS, MAURITIUS | MAY 21-23

PROGRAM OVERVIEW

The Africa Center for Strategic Studies (ACSS) and the U.S. Department of State convened a workshop to discuss how to advance cyber security in Africa in alignment with the UN Framework for Responsible State Behavior in Cyberspace. The roundtable convened 36 participants, including representatives from the African Union (AU), the Economic Commission of West African States (ECOWAS), Southern African Development Community (SADC), East Africa Community (EAC), the Intergovernmental Authority on Development (IGAD), the United States, the United Kingdom, and the European Union, as well as leading representatives from computer emergency response teams (CERTs) and other civilian agencies from Benin, Côte d'Ivoire, Ghana, Kenya, Mauritius, Mozambique, Nigeria, Senegal, South Africa, and Zambia. The roundtable offered participants the opportunity to exchange experiences and lessons learned from efforts to advance cyber security across the continent, and to discuss how to improve cooperation within Africa's growing cyber security architecture.

KEY INSIGHTS

African participation and influence in institutions that shape international cyber security policy is growing. The continent's representation in institutions where global cyber security norms, treaties, and standards are decided is steadily increasing. African states strongly support more inclusivity in these fora. They played a role in shifting the center of gravity in United Nations (UN) cyber security fora from the Governmental Group of Experts (GGE), which represented 15 to 25 member states, to the Open-Ended Working Group (OEWG), which is open to the participation of all UN members. With the African Union granted permanent membership on the G20, discussion of a permanent African seat on the United Nations Security Council, and over a dozen African states along with the African Union actively participating in UN cybercrime treaty negotiations, this influence is likely to grow.

The African region has made progress in implementing the UN Framework for Responsible State Behavior in Cyberspace. Africa's growing influence is in part a product of the progress the continent is making in implementing the UN Framework for Responsible State Behavior in Cyberspace. Driven by growing cyber threats and ongoing cyber capacity building initiatives, the Africa has seen rapid growth in cyber legislation, national strategies, and national CERTs. According to participants, the total number of national CERTs in Africa has nearly doubled over the past five years to approximately 37. The African Union and the Regional Economic

Communities have put into place critical infrastructure protection policies, treaties, and common positions meant to enable member states to implement the UN Framework.

Africa has a growing regional cyber security architecture. Participants highlighted how growth in cyber capacity has led to the development of an emerging regional cyber security architecture. This architecture consists of at least three main components:

1) **The African Union.** Participants compared the African Union's role to the roof of a house, enabling continent-wide cyber security cooperation and setting policies, positions, and standards for member states to implement. Over the past two years, African Union Malabo Convention on Cyber Security and Personal Data Protection has entered into force and a Common African Position (CAP) on the Application of International Law in Cyberspace has been adopted. The AU has also incorporated cyber security into other initiatives, such as its Agenda 2063, the Africa Continental Free Trade Agreement (AfCTFA), and a forthcoming Global Digital Compact. It is currently working to assist with implementation, update, and extend the number of countries that have acceded to the Malabo Convention, to implementation the CAP on the Application of International Law to Cyberspace, and to adopt a continental cyber security strategy.

2) **Regional Economic Communities (RECs).** Several of Africa's regional economic communities are playing a dynamic role in increasing cyber capabilities among their member states, fostering cooperation via South-South cyber capacity building, and assisting with the implementation cyber strategy and policy. ECOWAS has, for example, adopted regional cybercrime and critical infrastructure protection policies and spearheaded, with international support, a regional initiative to combat cybercrime. SADC has adopted a harmonized cyber security legal and regulatory framework consisting of model cybercrime, data protection and e-commerce laws. Both RECs are seeking to establish or deepen regional cyber security cooperation mechanisms.

3) **Computer Emergency Response.** Africa's rapid growth in CERTs have been facilitated by non-profit organizations such as the Forum for Incident Response Teams (FIRST) and the Africa Computer Emergency Response Team (AfricaCERT). These two entities have helped facilitate the growth of and provide fora for regular interaction of CERTs throughout Africa. As a result, even when they are not formally aligned with the RECs or the AU, CERTs across the continent have regular opportunities to interact, share good practices, and hone their skills through workshops, table-top exercises, and hackathons.

There exists a need for greater coordination and alignment within this regional architecture. As with any emergent architecture, there exists a need for enhanced coordination and cooperation. In broad strokes, participants felt that the division of labor and responsibility between the three components was clear, with the AU setting continent-wide policies and standards, the RECs helping to implement, share best practices, and facilitate cyber security cooperation among their member states, and CERTs engaged in capacity building at a more technical and operational level. Nevertheless, participants highlighted the need for more formal

clarity on these the roles to avoid the potential for duplication, as well as greater integration between AU, RECs, and CERTs to ensure greater coordination and facilitate an alignment of resources and effort.

Cyber security strategies and policies across the continent face significant implementation gaps. Like many of the policies authored at the REC or AU level, implementation can be a challenge. Participants cited a lack of funding and prioritization at the cabinet and presidential level within their countries as significant barriers to the implementation. They are a key reason why the Malabo Convention, despite recently entering into force, took a decade to do so and has not yet been adopted by most member states.

Existing cyber capacity building initiatives lack sufficient coordination and coherence. Despite the existence of clearinghouses such as the Global Forum on Cyber Expertise (GFCE) that seek to align external expertise with cyber capacity building needs, bilateral requests of multiple partners by states often lead to duplicative, wasted efforts. One participant cited an example whereby two partners, responding to a request from a state seeking a capability, unknowingly conducted two workshops on the same theme within weeks of one another. The problem is exacerbated when external actors undertake cyber capacity building initiatives without a strong demand signal from recipient countries, or when cyber capacity building recipients make requests that do not suit their current capability levels.

Critical information infrastructure across the continent is increasingly threatened. Due to threats such as ransomware and AI-augmented cyberattacks, the continent's critical infrastructure is at growing risk. Interdependencies within the continent's ports, telecommunications, and financial sectors are making attacks on critical infrastructure increasingly costly and potentially destabilizing. Necessary certifications and specialized training to protect software and systems that run Operational Technology (OT), Incident Command Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems are in high demand and limited supply. Participants highlighted that where possible, the AU and its member states should take a harmonized approach to defining, identifying, and protecting critical infrastructure, particularly where there are cross-border dependencies and vulnerabilities.

RECOMMENDATIONS:

1. ***Map Africa's cyber security architecture***. Participants recommended that a study be undertaken to map cyber maturity in Africa at the national, regional, and continental levels. Common indicators, such as those used in the International Telecommunications Union's (ITU's) Cyber security Maturity Index, could identify cyber capacity building needs. The AU, in partnership with a research organization or the ITU itself, would be a natural candidate to undertake such an assessment.

2. ***Improve regional and national threat intelligence and analysis capabilities.*** Participants recommended that African countries create or sponsor the creation of more context specific tools to identify and respond to the cyber threats their countries face. Widely available commercial tools and methodologies may not be well-suited to quantify the most common techniques and tactics of malicious cyber actors operating in Africa, who

tend to rely on fraud and phishing rather than sophisticated malware, nor the types of systems, such as used or second-hand mobile phones, most often targeted. The main responsibility for developing such tools would likely vary by country but could rest with a CERT or independent cyber security authority.

3. ***Adopt a continental cyber security strategy.*** The African Union should publish a continental cyber security strategy, a task which has already been mandated to be developed by the African Union Cyber Security Expert Group (AUCSEG). This strategy should assign clear cyber security roles and responsibilities to the AU, RECs, member states, CERT community, and international partners.

4. ***Establish bi-annual or yearly high-level capacity building coordination meetings, led by the AU-GFCE.*** To address duplicative efforts among the world's major cyber capacity building donors, participants recommended that the AU-GFCE convene high-level coordination conferences every one or two years. The aim of these conferences would be for major international donors to align cyber capacity building priorities, resources, and focus areas across the continent.

5. ***Establish regional cyber security cooperation mechanisms.*** The African Union and Regional Economic Communities should establish regional cyber security cooperation mechanisms to enable formal, operational-level cyber security cooperation between African states. These mechanisms may vary by region but could include regional Information Sharing and Analysis Centers (ISACs) to share threat intelligence, Computer Emergency Response Teams (CERTs) to respond to and recover from threats, or Centers of Excellence (CoE) to provide training, publish model curricula and exchange good practices. These mechanisms could focus on the types of threats for which their member states possess a shared interest in addressing and where regional cooperation might be useful, such as cyber threats from external actors, cross-border critical information infrastructure, disinformation, or transnational cybercriminal groups. Participants suggested that peace operations, where certain member states cultivate certain kinds of capabilities and, when needed, make them available at the regional level, could be a useful model.

6. ***Make implementation of existing cyber security policies a focal point for cyber capacity building***. Participants highlighted persistent challenges that member states often face in implementing continental and regional cyber security policies and strategies. They recommended that implementing existing initiatives, including the Malabo Convention and the Common African Position on the application of international law to cyberspace, are crucial steps in continuing to foster responsible cyber behavior among African states. They recommended that the implementation of these initiatives be a focal point of cyber capacity building efforts.

7. ***Prioritize REC-led South-South cyber capacity building.*** To address duplicative, siloed, or misaligned programming, participants recommended that more cyber capacity building efforts be channeled through Regional Economic Communities such as IGAD, ECOWAS, EAC, ECCAS, COMESA, and SADC. The RECs have comparative advantages

over other external actors in their knowledge of the specific capacity building needs of their member states, presence of interdependent infrastructure in their regions, and ability to convene South-South cyber capacity building initiatives.

8. ***Align the continent's emerging computer security incident response architecture.*** As the continent's computer emergency response architecture continues to grow, participants suggested there was a need for greater coordination and cooperation between Africa's CERTs. They suggested that Malware Information Sharing Platforms (MISPs) be adopted at both the regional and national level, that the RECs take steps to enhance cooperation, coordination, and alignment of capabilities and resources across regional CERTs or CERT networks, and Africa-CERT establish a formal relationship with the African Union.

9. ***Identify and take steps to protect transnational cyber-dependent critical infrastructure.*** The African Union and RECs should take steps to identify, coordinate, and capacitate the protection of critical information infrastructure whose compromise would have significant consequences for multiple member states. Key multinational institutions, ports, undersea cables, telecommunication networks, and multinational companies in the tech, telecom and finance sectors could potentially be candidates to be designated as regional or continental critical infrastructure. 24/7 cyber points of contacts should be established, using national CERTs as focal points.