Information Note

Advancing Regional Cyber Security and Stability in Africa
Port Louis, Mauritius; 21-23 May

WHAT: The Africa Center for Strategic Studies (ACSS) and the U.S. Department of State Bureau of Cyberspace and Digital Policy will organize a three-day workshop with senior officials from Africa's regional institutions and representatives from national computer emergency response teams. Discussions will focus on lessons learned, and attendees will come up with recommendations to advance Africa's continental cybersecurity architecture in alignment with the United Nations-affirmed Framework of Responsible State Behavior in Cyberspace.

WHERE: Port Louis, Mauritius

WHEN: May 21-23, 2024

WHO: 30 attendees, including subject matter experts, representatives from leading national Computer Emergency Response Teams (CERTs), as well as U.S. government, E.U., and U.K. officials will be invited. Representatives from multilateral institutions, including the African Union, ECOWAS, IGAD, SADC, ECCAS, as well as the Forum of Incident Response and Security Teams and the Global Forum on Cyber Expertise will also be invited. CERT representatives will come from the following countries (1 per country): Cote D'Ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, Mozambique, Nigeria, South Africa, and Zambia. U.S. government attendees will come from the U.S. Department of State, the George C. Marshall European Center (GCMC) for Security Studies, the U.S. Agency for International Development, the U.S. Department of Homeland Security, and the U.S. Department of Defense. Africa Center alumni with relevant expertise will also be included.

Participants must be able to read and engage in detailed, sector-specific discussions in English or French.

WHY: African states have varying levels of digitization, cyber capabilities, and expertise. The AU and Regional Economic Communities (RECs) play a crucial role in navigating these differences to pursue the common interests of member states in advancing the globally recognized norms of state behavior in cyberspace and in responding to sophisticated cyber threats from state-backed actors and organized cybercriminal networks. Regional institutions 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; drafted model laws and legislation 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.

Leveraging the Africa Center's peer learning model, this three-day long workshop will seek to enable participants to share insights and identify opportunities to build cyber capacity at Africa's regional institutions to implement the United Nations-affirmed Framework of Responsible State Behavior in Cyberspace and advance confidence, coordination, and trust in cyberspace among member states.

HOW: The program will be in-person and will include plenary sessions with moderated question-and-answer periods as well as working groups that will discusses lessons learned and generate recommendations for advancing Africa's regional cybersecurity architecture in alignment with the framework. Each group will have an opportunity to present its findings and suggest next steps at a final brief-back session.

All discussions and activities will be conducted under a policy of strict non-attribution.

PROGRAM OBJECTIVES:

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 the first steps towards implementing the recommendations identified and discussed by program attendees.