AFRICA CENTER
FOR STRATEGIC STUDIES

CYBERSPACE SECURITY PRIORITIES FOR AFRICA’S NATIONAL SECURITY ACTORS

INFORMATION NOTE

WHAT: The Africa Center will facilitate a four-week virtual program to examine the role of national security actors in responding to cyberspace security challenges in Africa. This program will discuss how the security sector can cooperate with other public and private sector stakeholders to address the continent’s growing cyber-related threats. Participants who complete the program will receive certificates that recognize their accomplishment.

The program objectives are to:

1. Enhance understanding of Africa’s cyberspace security threats and challenges.
2. Identify priorities for African defense and security actors to consider when preparing for and responding to malicious cyber activity.
3. Compare experiences, perspectives, and good practices in cyberspace security policy across a range of security sector, civilian, private sector and non-governmental stakeholders.

WHERE: Online, via Zoom for Government

WHEN: August 3-4, 2021
August 10-11, 2021
August 17-18, 2021
August 24-25, 2021

WHO: Participants with a wide range of backgrounds in the security sector, government, the private sector and civil society will be invited to participate. The following countries are invited to nominate participants: Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Central African Republic, Chad, Comoros, Congo, Democratic Republic of the Congo, Cote d'Ivoire, Djibouti, Egypt, Eswatini, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, Sudan, Tanzania, Togo, Tunisia, Zambia. Each country is invited to nominate three participants: at least one of whom should be from the uniformed security sector; at least one of whom should be civilian; and at least one of whom should be female. Additional participants will be invited from regional economic communities, multilateral organizations, and academia, as well as some representatives of the U.S. government.

Participants should be mid-to-senior level officials, lieutenant-colonel or equivalent and above, ideally serving in positions responsible for cybersecurity or emerging technology policy and strategy. Examples of possible nominees include:

- officers in the air force or military intelligence seeking to defend their countries against threats from emerging technology;
- police and gendarmes from cyber threat or financial intelligence units charged with collecting digital forensic evidence or investigating digital crimes; and
- Civil servants, appointees, or senior-level technical experts working on cyber policy and strategy for offices of the president, ministries of foreign affairs, telecommunications ministries, national security advisors, and/or computer incident response teams (CIRTs).

WHY: Rising internet penetration and rapid innovation in digital technology is amplifying and changing the nature of security challenges from a wide array of state, non-state and criminal actors across Africa. The security sector has a crucial role to play in protecting critical national infrastructure from cyberattack and in responding to the malicious uses of information technology by organized, violent actors. Effective cyberspace security policy requires cooperation among stakeholders.

HOW: This virtual engagement will combine live plenary conversations (90 minutes) and weekly not-for-attribution discussion groups (90 minutes). Participants will be asked to review the readings and videos from previous cyber webinars in advance of the program.

The program will be composed of four sessions:

1) Africa’s Cyberspace Threat Landscape
2) Key Elements of a National Cyberspace Security Response
3) Critical Infrastructure Cybersecurity
4) National Security and Cyberspace Security Strategies

The program will be conducted in English, French, and Portuguese.