AFRICA CENTER
FOR STRATEGIC STUDIES

Cyberspace Security Priorities for Africa's National Security Actors

SYLLABUS

Online, via Zoom for Government

3 – 25 August 2021

AFRICA CENTER
FOR STRATEGIC STUDIES

CYBERSPACE SECURITY PRIORITIES FOR AFRICA'S NATIONAL SECURITY ACTORS

3 – 25 August 2021

Online, Zoom for Government

SYLLABUS

TABLE OF CONTENTS

ABOUT THE AFRICA CENTER

Since its inception in 1999, the Africa Center has served as a forum for research, academic programs, and the exchange of ideas with the aim of enhancing citizen security by strengthening the effectiveness and accountability of African institutions, in support of U.S. - Africa policy.

VISION

Security for all Africans championed by effective institutions accountable to their citizens.

Realizing the vision of an Africa free from organized armed violence guaranteed by African institutions that are committed to protecting African citizens is the driving motivation of the Africa Center. This aim underscores the Center's commitment to contributing to tangible impacts by working with our African partners – military and civilian, governmental and civil society, as well as national and regional. All have valuable roles to play in mitigating the complex drivers of conflict on the continent today. Accountability to citizens is an important element of our vision as it reinforces the point that in order to be effective, security institutions must not just be "strong," but also be responsive to and protective of the rights of citizens.

MISSION

To advance African security by expanding understanding, providing a trusted platform for dialogue, building enduring partnerships, and catalyzing strategic solutions.

The Africa Center's mission revolves around the generation and dissemination of knowledge through our research, academic programs, strategic communications, and community chapters. Drawing on the practical experiences and lessons learned from security efforts on the continent, we aim to generate relevant insight and analysis that can inform practitioners and policymakers on the pressing security challenges that they face. Recognizing that addressing serious challenges can only come about through candid and thoughtful exchanges, the Center provides face-to-face and virtual platforms where partners can exchange views on priorities and sound practices. These exchanges foster relationships that, in turn, are maintained over time through the Center's community chapters, communities of interest, follow-on programs, and ongoing dialogue between participants and staff. This dialogue—infused with real world experiences and fresh analysis—provides an opportunity for continued learning and catalyzes concrete actions.

MANDATE

The Africa Center is a U.S. Department of Defense institution established and funded by Congress for the study of security issues relating to Africa and serving as a forum for bilateral and multilateral research, communication, exchange of ideas, and training involving military and civilian participants. *(10 U.S.C 342)*

MAP OF AFRICA

Map No. 4045 Rev. 7 UNITED NATIONS
November 2011

Department of Field Support
Cartographic Section

OVERVIEW

Rising internet penetration and rapid innovation in digital technology is amplifying the nature of Africa's security challenges. African governments, security sector actors, and their citizens are vulnerable to array of vast evolving cyber threats from a variety of state, non-state, and criminal actors. The proliferation of cheap sensors, surveillance technology, and sophisticated malware has led cyberspace to become the predominant medium of state-sponsored espionage. Increasing technology dependence makes critical infrastructure such as military systems, government networks, and sectors such as energy and banking vulnerable to cyber sabotage. New forms of digital organized crime are emerging, along with changes in how more traditional forms of organized crime are organized and financed. The spread of information technology also has implications for how violent state and non-state actors recruit, organize, and finance themselves, and the strategies and tactics they use to commit violence.

Despite these growing threats and vulnerabilities, the African security sector has been largely absent from national and regional efforts aimed at improving cyberspace security. Nevertheless, the security sector has a crucial role to play in securing government systems and networks, stopping the spread of organized cybercrime, protecting critical national infrastructure from cyberattack and in responding to other malicious uses of information technology by organized, violent actors. Crucially, effective cyberspace security policy requires multistakeholder cooperation and coordination. Much of the innovation, expertise, and human capital needed for cyberspace security maturity rests with the private sector. Oversight from civilian actors and civil society is required to ensure cybersecurity policies are aligned with sound security sector governance principles. To stay ahead of tomorrow's threats, governments across the continent will have to adopt a collaborative, whole of government, citizen-centric approach to cyberspace security.

PROGRAM OBJECTIVES:

1. Expand understanding of the main challenges interdependent information technology poses to national and citizen security in African countries.

2. Identify key priorities for African defense and security actors to better prepare for and respond to malicious cyber activity that threatens national security interests.

3. Compare experiences, perspectives, and good practices in cyberspace security policy across a range of security sector, civilian, private sector and non-governmental stakeholders.

4. Socialize the benefits of maintaining an open, reliable, and secure internet to maximize the advantages of interdependent information technologies for business, governments, and societies while minimizing cyberspace security threats and vulnerabilities.

PROGRAM FORMAT:

Each week, the program will feature (1) a plenary session comprised of a moderated discussion with an array of experts – from policymakers, practitioners, and academics – followed by an

interactive question-and-answer session; and (2) small group discussions for participants to discuss their reactions to the plenary session and share experiences with each other.

The program will be conducted in English, French, and Portuguese. In order to foster frank discussions and create trust among participants, discussions will be conducted under a policy of non-attribution, meaning specific comments or interventions by any participant will not be identified by name or country in any summaries, reports, or sharing of the insights gained from the seminar by any participant, speaker, or the organizers.

SYLLABUS:

This syllabus provides an overview of academic goals and key policy questions this program seeks to raise regarding the African security sector's priorities in cyberspace security in Africa. For each session, we provide a brief introduction and list questions for discussion. We also include selected articles, whose primary purpose is to help frame the issues within the context of available scholarship and policy documents. The syllabus likely covers more issues and materials than can be sufficiently discussed in the available time. It is beneficial to read some or all of the recommended readings on the syllabus prior to the seminar, because the readings will place participant and speaker comments into appropriate context. However, we also hope that you use these materials as resources even after the program concludes, and that you return to them for relevant details.

The outside materials and academic content included in this syllabus do not reflect the views or official position of the Department of Defense or the United States government. This syllabus is an educational document intended to expose participants to a variety of views and perspectives to help prepare them to take full advantage of the program.

PROGRAM PREPARATION:

Before the seminar, we encourage you to:

1. Read this syllabus.

2. Read the recommended readings and watch the recommended videos.

3. Spend time thinking about and answering the discussion questions.

4. Consider what experiences from your work might be relevant to share in discussion groups.

5. Be prepared to participate actively in discussion groups and to learn from participants from other countries.

Plenary Session 1: Africa's Cyber Threat Landscape

OBJECTIVES:

- Describe the scope and scale of the cyber threats African countries face from espionage, critical infrastructure sabotage, organized crime and combat innovation
- Explore how the nature of Africa's cyber threats are likely to change and evolve in the future.
- Consider the scope and scale of these cyber threats in South Africa

BACKGROUND:

The rapid diffusion of information and communications technology (ICT) is reshaping Africa's security landscape. Though digitization has brought enormous economic and social benefits, it is also amplifying and altering the nature of the continent's security challenges. All computer networks, local-area networks (LANs), and wide-area networks (WANs) are vulnerable to attempts to breach the confidentiality, alter the integrity, or disrupt access to information stored within them. More broadly, the spread of ICT is altering how and by whom information is processed, stored, and disseminated. These aspects of digital technology allow it to be exploited for nefarious purposes by criminal networks, terrorist groups, lone hackers, rival nation states, and other malicious actors. The greater the degree of connectivity, the more African countries and their citizens risk having their technologies turned against them.

Africa's central cyber threats and challenges include:

- **Espionage and Surveillance.** Information systems have fundamentally transformed the methods and the sources that nation-states, businesses, and non-state actors use to gather and protect sensitive information. Though the most significant cyber espionage concerns in Africa have centered around foreign actors, espionage and surveillance capabilities are rapidly diffusing across the continent.

- **Critical Infrastructure Sabotage.** Africa's government networks, military systems, banking, and telecommunications industries are vulnerable to cyberattacks that seek to disable or destroy them. African countries are particularly vulnerable because most of the continent's ICT infrastructure is supplied by external actors and key sectors such as power, water, and energy often possess single points of failure.

- **Organized Crime:** The spread of cyberspace has led to the formation of entirely new forms of organized criminal networks who exploit digital tools to steal, transfer, and extort resources. In recent years, the African continent has grown both as a target and a source of organized cybercrime. Just as crucially, the spread of ICT is also influencing how traditional organized crime enterprises such as human smuggling, terrorism, violent extremism, criminal actors at sea and arms trafficking are structured and financed.

- **Combat Innovation.** Information technology is becoming increasingly central to the way security is managed and delivered to citizens, including security strategies, operations, and tactics. As security institutions and actors across the continent are seeking to benefit from enhanced surveillance capabilities and emerging technologies such as drones, non-state actors are exploiting emerging technologies to raise money, recruit, organize, and commit violence.

DISCUSSION QUESTIONS:

- What do you consider to be your country or regions principal cyber threats and challenges? How severe are they?

- What sectors in your country or region are most vulnerable to cyberattack?

- How do you see the cyber threat landscape in your country or region evolving over the coming five or ten years?

RECOMMENDED READINGS:

Nathaniel Allen, "Africa's Evolving Cyber Threats," Africa Center for Strategic Studies, January 19, 2021.
EN: https://africacenter.org/spotlight/africa-evolving-cyber-threats/
FR : https://africacenter.org/fr/spotlight/lafrique-a-lepreuve-des-nouvelles-formes-de-cybercriminalite/

Noëlle van der Waag-Cowling, "Stepping into the Breach: Military Responses to Global Cyber Insecurity," International Committee of the Red Cross, June 17, 2021.
https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/

Mourad El Manir, "L'Afrique Face aux Défis Proteiformes du Cyberespace, " Policy Center for the New South Policy Paper, Décembre 2019.
https://www.policycenter.ma/sites/default/files/PP_19-20_Al-Manir.pdf

ENACT and INTERPOL, *Online Organized African Crime from the Surface to the Darkweb*, INTERPOL Analytical Report, July 2020.
https://enact-africa.s3.amazonaws.com/site/ uploads/2020-08-20-interpol-darkweb-report%20.PDF

African Union and Symantec, *Cyber Crime and Cyber Security Trends in Africa*, November 2016.
https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf

RECOMMENDED VIDEOS:

Africa Center for Strategic Studies, "Emerging Cyber Dimensions of Africa's Security Landscape," December 3, 2020
EN: https://africacenter.org/programs/emerging-cyber-dimensions-africa-security- landscape/
FR : https://africacenter.org/fr/programs/nouvelles-cyber-dimensions-paysage-securitaire-africain/

PO: https://africacenter.org/pt-pt/dimensoes-ciberneticas-emergentes-paisagem-seguranca-africa/

Africa Center for Strategic Studies, "Cyber Dimensions of Violent Extremism in Africa," March 18, 2021
EN: https://africacenter.org/programs/cyber-dimensions-statecraft-africa/
FR : https://africacenter.org/fr/programs/dimensions-cybernetiques-habilete-politique-afrique/
PO: https://africacenter.org/pt-pt/dimensoes-ciberneticas-aparelho-estado-africa/

Africa Center for Strategic Studies, "Cyber Dimensions of Violent Extremism in Africa," May 19, 2021
EN: https://africacenter.org/programs/cyber-violent-extremism-africa/
FR : https://africacenter.org/fr/programs/dimensions-cybernetiques-extremisme-violent-afrique/
PO: https://africacenter.org/pt-pt/dimensoes-ciberneticas-extremismo-violento-africa/

Africa Center for Strategic Studies, "Emerging Cyber Dimensions of Transnational Organized Crime in Africa," July 8, 2021
EN: https://africacenter.org/programs/cyber-dimensions-of-organized-crime-in-africa/
FR : https://africacenter.org/fr/programs/les-dimensions-cybernetiques-de-la-criminalite-organisee-en-afrique/
PO: https://africacenter.org/pt-pt/dimensoes-ciberneticas-do-crime-organizado-em-africa/

Plenary Session 2: Key Elements of a National Cyberspace Security Response

OBJECTIVES:

- Identify key elements of the national-level response necessary to confront cyberspace-related challenges to national security.
- Identify key actors and stakeholders in designing and effecting a national cyberspace security response and the role for national security actors within a multistakeholder approach.
- Assess national-level cyberspace security policy, strategy, and institutions of leading African countries.
- Take stock of the security sector's role in national efforts to confront cyber threats from espionage, critical infrastructure sabotage, crime, and combat innovation.
- Discuss the benefits and challenges of maintaining an open, reliable, and secure internet to maximize the advantages of interdependent information technologies for business, governments, and societies while minimizing cyberspace security threats and vulnerabilities.

BACKGROUND:

Cybersecurity strategy and policy is at an incipient stage across much of Africa. Most African countries possess neither cybersecurity strategies nor national computer incident response teams, the bare minimum necessary for a basic national cyber threat management infrastructure. In leading countries, the role of the security sector as part of broader cybersecurity response varies substantially. In Kenya, Senegal, and Mauritius, telecommunications ministries are the lead agencies responsible for overseeing cybersecurity policy. In Nigeria and South Africa, the security sector has taken on more of a role: the lead agencies are the National Security Advisor and the State Security Agency, respectively.[1]

Addressing the continent's evolving cyber threats requires a comprehensive, government-led response. Key elements of this response include: [2]

a) National strategies, which articulate cybersecurity vision, strategic objectives and identify and prioritize a country's most critical cybersecurity challenges, direct resources, assign government-wide cybersecurity responsibilities, and ensure civilian oversight of security actors.

b) Legal and regulatory frameworks to address the growth of organized cybercrime and boost the capacity of law enforcement to use digital evidence.

[1] A repository of national cybersecurity strategies of each country can be found on the Internet Telecommunications Union website at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
[2] For an internationally accepted framework, see, for example, the Oxford Cyber Maturity Model: https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

c) Computer incident response and crisis management teams, which can identify, monitor, and protect critical national information infrastructure and help recover from inevitable security breaches.

d) National security sector cyber awareness, threat identification, and response capabilities.

Regardless of country or context, multistakeholder coordination is fundamental to an effective national response. The private sector, civil society, and security actors are key partners, and not opponents or obstacles, to government and security sector actors seeking to develop sound national approaches to cyberspace security. Governments across Africa rely on the private sector to supply the latest cybersecurity technology, to report incidents and monitor threats, and to take on a lead role in securing key sectors from cyberattack, such as telecommunications and banking. Civil society is an equally essential stakeholder for ensuring that cybersecurity policy remains consistent with human rights, democracy, and citizen security. The success of organizations such as the Kenya ICT Action Network[3] in fostering public dialogue and catalyzing ICT sector reforms illustrates the importance of a multistakeholder approach to cyberspace security.

What matters most is how cybersecurity policy and strategy is formulated and executed. Too little security sector involvement and a country may fail to secure sensitive government networks, develop needed capacity to monitor and respond to organized crime, and integrate digital technology into military strategies, operations, and tactics. An overwhelming security sector presence, however, can create unnecessary costs and reduce civilian oversight and accountability. Whatever their role, it is essential that government and security sector actors bear in mind that citizen security is fundamental to cybersecurity. They must guide efforts to respond to the threats posed by the spread of digital technology in a manner consistent with the values enshrined in the African Peace and Security Architecture: rule of law, human rights, and democracy.

DISCUSSION QUESTIONS:

- How effective is your country/region in responding to cyber threats and what are the challenges?

- What role does the security sector play in cyberspace security in your country? What other actors are involved in cyberspace security in your country?

- What role should the security sector have in confronting your country's cyber threats and challenges? How could this support a multistakeholder approach?

- What are the challenges and risks associated with security sector involvement in cyberspace security?

[3] For more information on the Kenya ICT Action Network, see: https://www.kictanet.or.ke/about-kictanet/

RECOMMENDED READINGS:

Global Cyber Security Capacity Centre, "Cyber Maturity Model Dimension 1: Cybersecurity Policy and Strategy,"Oxford University.
https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

Global Forum on Cyber Expertise, "Dehli Communiqué on a GFCE Agenda for Global Cyber Capacity Building," November 24, 2017.
https://thegfce.org/wp-content/uploads/2020/04/ DelhiCommunique.pdf

United Nations Information Technology Union, "2020 Global Cybersecurity Index," United Nations, June 29, 2021.
https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

DCAF, "How do Cyberspace and Cybersecurity Relate to Good Security Sector Governance" in *Guide to Good Governance in Cybersecurity,"* p. 25-38, January 2021.
EN: https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf#page=25FR:
https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_Jan2020.pdf.pdf

"A Problemática Da Cibersegurança E Os Seus Desafios," Centro de I&D Sobre direito e sociedade, September 2016.
http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problemática-da-cibersegurança-e-os-seus-desafios.pdf

Nathaniel Allen, "The Promises and Perils of Africa's Digital Revolution," Brookings Techstream Blog, March 11, 2021.
https://www.brookings.edu/techstream/the-promises-and-perils-of-africas-digital-revolution/

Plenary Session 3: Cyber Incident Management and Critical Infrastructure Protection

OBJECTIVES:

- Define critical infrastructure and examine the scale and scope of cyberspace threats and vulnerabilities to it in African countries.
- Discuss the role of national and sectoral Computer Security Incident Response Teams (CSIRTs) as part of a national cybersecurity response system to identify and respond to malicious cyberattacks on critical infrastructure.
- Discuss the role that national security actors play as key members of CSIRTS, interagency coordination cells, and other mechanisms for interagency cyberspace security cooperation.
- Explore how best to promote cross-sector partnerships between civilian, security actors, law enforcement, justice, and private sector partners to safeguard internet-dependent critical infrastructure.

BACKGROUND:

As African countries develop and digitize, their critical infrastructure (CI) systems, services and assets will become increasingly vulnerable to cyberattack. The International Telecommunication Union (ITU) provides a guiding definition of critical infrastructure as "the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these."[4] As a part of critical infrastructure, Critical Information Infrastructure (CII) includes critical telecommunications infrastructure, as well as the ICT systems necessary for the complete functioning of critical infrastructure across multiple sectors.[5] Critical information infrastructure assets operate amongst a network of interconnected and interdependent sectors where the ICT systems contain inherent vulnerabilities that can be exploited by attacking the controlling information systems of one infrastructure asset. Attacks on these "control systems" including supervisory data control and acquisition (SCADA) and incident command (ICS) systems, can produce a ripple effect of damages in other critical infrastructures.

Critical infrastructure cybersecurity involves sustained efforts to secure critical infrastructure assets from external attacks, alongside sustained efforts to support the continuity of infrastructure services when computer security incidents do occur. Computer Security Incident Response Teams (CSIRTs) are an integral mechanism of critical information infrastructure protection, allowing for incident and emergency response management and to monitor the threat environment, respond to, and recover from major cyberattacks. At the national level, CSIRTs provide broad and extensive services to the country by working closely with sectoral and private CSIRTS, allowing for the exchange of timely and relevant information and communication.

[4] ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat, Geneva (2008).
[5] Maglaras, Leandros, et al. "Threats, countermeasures and attribution of cyber attacks on critical infrastructures." EAI Endorsed Transactions on Security and Safety 5.16 (2018).

African countries face both opportunities and constraints when it comes to protecting critical infrastructure from cyberattack. On the one hand, a limited degree of technology dependence compared to more industrialized regions of the world, as well as a lack of legacy systems, provides many African nations the opportunity to build in cybersecurity into their infrastructure networks from the ground up. On the other, high dependence on external actors to provide critical infrastructure, single points of failure, and limited investments in critical infrastructure cybersecurity pose significant risks. Only 22 African countries possess national CSIRTS,[6] in part due to the intensive time, financial, and technical resource investments they require.[7] The existence of sectoral-level CSIRTS are rare, in part because of the presence of small and medium enterprises and organizations who face similar resource constraints.

DISCUSSION QUESTIONS:

- What would you characterize as critical infrastructure in your country or region? To what extent is this critical infrastructure cyber dependent?
- Does your country have CSIRTs and how effective are they in protecting cyber critical infrastructure?
- What laws, policies, or mechanisms does your country have in place to protect critical national infrastructure from cyberattack?
- What role does the security sector have in protecting critical national infrastructure in your country?
- How can cooperation, coordination, and information sharing between the security sector, other parts of government, and stakeholders outside of government be improved to increase the resilience of cyber-dependent national infrastructure?

RECOMMENDED READINGS:

Nathaniel Allen and Noelle van der Waag-Cowling, "How African Countries Should Address State-Sponsored Cyber Threats," Brookings Techstream Blog, July 15, 2021. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

Internet Society and the African Union Commission, "Internet Infrastructure Guidelines for Africa," March 24, 2017.
EN: https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa
FR: https://www.internetsociety.org/fr/resources/doc/2017/lignes-directrices-sur-la-securite-de-linfrastructure-internet-pour-lafrique

[6] See the latest data from the Information Technology Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx
[7] Mouton, Jean, and Ian Ellefsen. "The identification of information sources to aid with critical information infrastructure protection." 2013 Information Security for South Africa (2013): 1-8.

Redação Digital Security, "Segurança cibernética deve ser prioridade para setor de infraestrutura crítica," 09/20/2020.
https://revistadigitalsecurity.com.br/seguranca-cibernetica-deve-ser-prioridade-para-setor-de-infraestrutura-critica/

Hanneke Duijnhoven, Bram Poppink, Tom van Schie, and Don Stikvoort, "Getting Started with a National Computer Security Incident Response Team (CSIRT) Guide," Netherlands Organisation for Applied Scientific Research, 2021.
https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/

Eric Luiijf, Tom van Schie, Theo van Ruijven, and Auke Huistra, "The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers," GFCE-Meridian, 2016.
https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

Plenary Session 4: National Cybersecurity Strategy

OBJECTIVES:

- Discuss the process of drafting a national cyberspace security strategy and identify its core elements.

- Discuss the role of the security sector actors in the design and implementation of national cybersecurity strategy and policy.

- Outline core principles, good practices, and lessons learned during the crafting and implementation of national cybersecurity strategy and policy.

BACKGROUND:

In many respects, cybersecurity strategies lie at the heart of national efforts to respond to cyber challenges. National cybersecurity strategies are necessary to define and prioritize key threats, which vary significantly from country to country and region to region. Along with legislation, national strategies are the main vehicles through which intergovernmental roles and responsibilities for cyberspace security are assigned. They can also be used as tools to ensure that cybersecurity is adequately resourced, and to monitor the progress of nation-wide efforts to defend against cyber threats. If updated with regularity, cybersecurity strategies can ensure that national cyberspace security efforts respond and adapt to a changing threat environment.

As with any security-related strategy, the process through which the strategy is formulated matters as much as the content. High level political buy-in and support is necessary to resolve conflicts between different agencies and ministries, as well as ensure clear and consistent communication with the public. With a clear process for prioritizing threats, national strategies can be useful tools to manage scarce government resources and align external support to where it is most needed. Strategies that are the product of consultation with a wide range of government, civil society, and external stakeholders can achieve broad buy-in, improving government coordination and catalyzing national efforts to address key security challenges.[8] These considerations are particularly crucial in an African context, where governments often rely on external actors for support and where multistakeholder involvement is crucial to ensure accountability, inclusivity, and respect for citizen security.

Unfortunately, most African governments have yet to develop a national cybersecurity strategy. According to the most recent data available from the United Nations Information Technology Union, only 16 of Africa's 54 countries have completed national cybersecurity strategies. The strategies of four additional countries – Tunisia, Botswana, Ghana, and Zambia - remain in draft form.[9] Even in countries where internet penetration is low, the lack of a national cybersecurity strategy is a missed opportunity to maximize the benefits and minimize the risks of growing digitization.

[8] See Africa Center for Strategic Studies, "Toolkit for National Security Strategy Development," 2021. https://africacenter.org/wp-content/uploads/2021/01/National-Security-Strategy-Development-in-Africa-Toolkit-for-Drafting-and-Consultation-Africa-Center-for-Strategic-Studies.pdf

[9] See the ITU's Cybersecurity Strategy Repository: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

DISCUSSION QUESTIONS:

- For countries with a national cybersecurity strategy, what was the process through which your country's strategy was developed or implemented? For countries without a national cybersecurity strategy in place, what has your experience been with respect to developing and implementing sectoral strategies and policies on cyber issues?

- What role does or should the security sector have in cyberspace security strategy development process?

- What good practices, procedures, coordination mechanisms, or oversight are needed to ensure that national security actors play a productive role in formulating policies and strategies on cyber issues?

RECOMMENDED READINGS:

International Telecommunication Union (ITU), *Guide to Developing a National Cybersecurity Strategy*, 2018.
EN : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
FR : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-F.pdf

Africa Center for Strategic Studies, 2021, "National Security Strategy Development Toolkit," Section 1, pp. 1-9.
EN: https://africacenter.org/wp-content/uploads/2021/01/National-Security-Strategy-Development-in-Africa-Toolkit-for-Drafting-and-Consultation-Africa-Center-for-Strategic-Studies.pdf
FR : https://africacenter.org/wp-content/uploads/2021/01/Developpement-dune-strategie-de-securite-nationale-en-Afrique-outil-de-consultation-et-de-redaction-CESA.pdf
PO: https://africacenter.org/wp-content/uploads/2021/02/Desenvolvimento-da-Estrategias-de-Seguranca-Nacional-em-Africa-Um-kit-de-ferramentas-para-consulta-e-preparacao.pdf

Luka Kuol and Joel Amegboh, "Rethinking National Security Strategies in Africa," *International Relations and Diplomacy* 9 (01): 2021, 1-17.
http://www.davidpublisher.org/Public/uploads/Contribute/60a72058556ba.pdf

Gouvernement de Burkina Faso, « Strategie nationale de cybersécurité, » Janvier 2019.
https://anssi.bf/fileadmin/user_upload/SNCS_BF.pdf

Federal Republic of Nigeria, *National Cybersecurity Strategy and Policy,* February 2021.
https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

Claudia Almeida et al., "Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço," *Informação e Segurança no Ciberespaço,* September 2018.
https://www.researchgate.net/publication/327515395_A_Problematica_da_Ciberseguranca_o_Caso_da_Estrategia_Nacional_de_Seguranca_no_Ciberespaco