AFRICA CENTER
FOR STRATEGIC STUDIES

CYBERSPACE SECURITY PRIORITIES FOR AFRICA'S NATIONAL SECURITY ACTORS VIRTUAL ACADEMIC PROGRAM

EXECUTIVE SUMMARY

August 3 – 25, 2021

From August 3-25, 2021, the Africa Center for Strategic Studies conducted an executive-level online program on the security sector's role in addressing Africa's cyber-related challenges and threats. This executive summary provides background, synthesizes participant perspectives, shares key insights, and identifies emerging trends discussed during the program. The insights explore how state, security sector, private, and civil society stakeholders in Africa can:

- Improve awareness of the most significant cyber-related threats and threat actors
- Implement multistakeholder approaches to cybersecurity
- Harness the benefits and limit the risks of security sector involvement in cybersecurity
- Align cybersecurity policy and strategy with human rights and respect for rule of law

Background

The seminar convened participants representing 30 African countries with civilian and military backgrounds as well as select representatives from the private sector, civil society, and regional organizations. The objectives were for participants to i) expand understanding of Africa's cyber-related threats and challenges, ii) to identify key priorities for national security and defense actors in responding to malicious cyber activity, and iii) discuss how to maximize the benefits of information technology while minimizing cybersecurity threats and vulnerabilities.

The convening of participants from varying backgrounds and across uniformed and civilian lines allowed for holistic, respectful, and informed dialogue on the security sector's role in cybersecurity in Africa. The first part of the program focused on understanding Africa's cyber threat landscape from a national security-oriented perspective. The remaining sessions discussed the key elements of a national cybersecurity response, focusing specifically on computer security incident response, critical infrastructure protection, and implementing national cybersecurity strategies.

Participant Perspectives on the Challenge

Participants discussed how the rapid spread of information technology is making their countries vulnerable to threats from cyber espionage, critical infrastructure sabotage, organized crime, and combat innovation. They discussed how the most significant threat actors have historically been from state-sponsored and transnational criminal actors external to Africa, but that there is growing concern at the rapid spread of strategic cyber threats from within the continent. In a poll conducted during the first

plenary session, participants ranked organized criminal networks and violent extremism as the cyber threat actors most concerning to them, closely paralleling traditional security concerns African officials have regarding these actors.

In addition, participants stressed the importance of the need to adopt a citizen-centric security lens when managing cyber threats and challenges. Because of the internal nature of most conflict in Africa, control over and access to the population often matters as much as physical violence. Since information technology is becoming increasingly central to how states inform, access, and provide services to their populations, governments should use information technology not only to directly address threats and vulnerabilities, but also to reinforce the social contract between governments and citizens.

How can African governments balance the necessity of security sector involvement in cyberspace while limiting the risks and reinforcing the social contract? Participants offered four key insights.

Key Insights

1. **Government, security sector, international, and private sector actors should work together to improve awareness of the most significant cyber-related threats and threat actors.** Virtually all African states now possess, at a minimum, a cyber unit responsible for monitoring and responding to cybercrime. However, awareness of how the most destabilizing threat actors such as organized criminal networks, violent extremist groups and nation states are leveraging cyberspace and for what purposes is more limited. Even more cyber mature African countries remain at a largely incipient stage in determining what, if any, role information technology should play in how the security sector monitors and responds to these threats, as well as the defense sector's role as part of a broader national cybersecurity response. Participants suggested that awareness of the continent's most significant cyber-related threats and challenges could be improved by:

    - *Basic cyber awareness and capacity building in less cyber mature countries*. Africa's least cyber mature countries should begin with basic cyber awareness training and capacity building. Capacity building should "be the foundation of digital transformation and be tailored to the importance of the threat." In countries where large swathes of the population lack internet access, these efforts will need to be conducted in tandem with efforts to improve internet penetration and basic digital literacy. For individuals with internet access, participants advised exploring ways to raise awareness and build capacity at little-to-no cost, through numerous free online courses and trainings.

    - *More concerted threat monitoring and reporting in more cyber mature countries*. For countries that have the capacity, participants suggested that more efforts were needed to monitor, track, and report on threats. Few countries, for example, regularly publish information about the type and volume of computer-based attacks they experience or monitor the online activities of the largest and most destabilizing threat actors. Often, it is third parties that identify and inform affected parties of a breach. In part, this is because cybersecurity is deemed a sensitive issue and both governments and the private sector are reluctant to report or disclose attacks. By raising continent-wide awareness of the cyber threat landscape, participants suggested that far more transparency and collaboration is needed to build trust across multiple groups of stakeholders, enabling them to monitor, deter and prevent

malicious cyber activity.

2. **Responses to even the most significant cyber-related threats and challenges need to be informed by a multistakeholder approach.** Unlike other technologies that are explicitly designed to cause physical harm, information technology has a broad array of uses, many if not most of which aim to derive economic and social benefits. Human capital, technical expertise, and defense capabilities in the private sector, especially in finance and technology sectors, usually exceed those of government actors. Moreover, because information technology is becoming more and more essential to how governments serve their citizens, both private industry and civil society stakeholders have a critical role to play in deciding how information technology is used. It was noted that cyber defense culture across Africa has to change, especially because in many cases civilians are more capable than security sector actors in their cyber awareness and level of training. Participants highlighted how the key ingredients to the successful design and implementation of multistakeholder cybersecurity strategy and policy included:

    - *Inclusivity and trust*. National cybersecurity strategy, legislation, and policy design and implementation should seek to include and incorporate the feedback of "all relevant stakeholders" into design, drafting and implementation. These include, minimally: the security sector, telecommunications, finance, energy, civil society, academia, and other sectors deemed essential for the protection of cyber-dependent critical infrastructure. Participants noted how inclusivity helps to build public trust in the national cyber authorities by allowing multi-stakeholder cooperation and the reporting of incidents. Without this public trust, efforts to counter cyber threats will be less successful.

    - *High-level political leadership.* Due to the range of stakeholders involved, cybersecurity strategy and policy processes are usually not effective without high-level political leadership to assign roles and responsibilities and mediate interagency disputes. In Ghana, this role was taken on with an inter-ministerial working group. In Nigeria and Burkina Faso, this was the responsibility the National Security Advisor and the National Information System Security Agency (Agence Nationale de Sécurité des Systèmes d'Information), respectively – two extra-ministerial entities that report directly to the president.

    - *Leveraging technical expertise*. The design and implementation of national cybersecurity strategies and policies need to be informed by technical expertise. In Niger, the National Agency for Information Networks (Agence Nationale pour la Société de l'Information) is playing a key role in developing a national cybersecurity strategy and will eventually host the nation's computer security incident response team (CSIRT). In Ghana, this role is played by a technical working group charged with implementing national cyber policies and making recommendations to the inter-ministerial committee. Ghana's national CSIRT has also played an important role in establishing and coordinating the efforts of regional and sectoral CSIRTs, which remain rare in Africa.

3. **The security sector has a crucial role to play in cyberspace security, but one that comes with risks as well as benefits.** While agreeing that there is no one-size-fits all approach**,** there was a consensus that the security sector in Africa had a critical role to play as part of broader national cybersecurity response. Participants highlighted the need for security sector actors to develop capacity to monitor and respond to cyber-enabled organized crime. They also suggested that the security sector can

play a lead role in responding to "external" or "extraterritorial" cyber aggression and help ensure the protection of critical national infrastructure from a major cyberattack. However, participants also highlighted numerous risks that stem from security sector involvement in cybersecurity, such as the imposition of needless costs if the security sector assumes responsibilities best left to technical experts in the private sector or other branches of government; or reductions in government accountability if security sector actors are given access to or use private information without adequate oversight. Participants suggested that these risks could be mitigated by:

- *Fostering public-private partnerships in securing critical national systems and infrastructure from attack.* Particularly when it comes to securing heavily technology dependent sectors such as banking, finance, and telecommunications, participants suggested that the private sector is often best suited to take a lead role in network security, threat monitoring, and recovery. In these sectors, private sector capabilities generally outpace those of government and security sector actors. But there is also an important role for government and security sector actors, who, as participants noted, can help identify critical information infrastructure, facilitate the exchange of information across sectors, and marshal resources to under-resourced sectors. In the event of a major attack, security sector actors can also conduct investigations, collect evidence, and charge those responsible in their country's jurisdiction.

- *Strengthening or creating vertical and horizontal accountability mechanisms.* Participants discussed how governments cannot rely on technical solutions to prevent the abuse of private or personal data by political or security sector actors. To a large extent, ensuring accountability necessities the existence, strengthening, or creation of legal and institutional oversight mechanisms. These include an independent judiciary and legislature; ombudsmen and inspector generals within the executive branch; and a robust civil society and media. Such actors are essential to ensuring that officials are held accountable, that abuses are reported and recorded, that existing laws are followed, and that laws or policies that decrease security sector transparency and accountability are modified or struck down.

4. **Cybersecurity policy and strategy in Africa needs to be aligned with human rights, the rule of law, and respect for citizen security.** As important as responding to the continent's rapidly evolving array of cyber threats is, participants agreed on the need to consider second- and third-order consequences of policies intended to give security sector actors tools to fight cyber-related organized crime, terrorism, or espionage. Participants pointed to the widespread adoption of vaguely - worded cybercrime and information security laws that have given security sector actors authority to censor, monitor and detain private citizens and opposition groups with limited oversight. The net result of many of these laws has been to decrease the trust between citizens and states and spread destabilizing, authoritarian forms of rule. In Mali, such laws went against the spirit of the country's constitution and may have helped contribute to the August 2020 coup d'état that ejected the country's elected government from power. Participants suggested that policymakers and security sector officials in Africa can help ensure that cybersecurity is aligned with citizen security by:

- *Avoiding ambiguity.* In many cases, terms such as "disinformation" and "terrorism" are vaguely defined or defined in ways that give governments discretion to effectively criminalize free expression, targeting non-violent protestors and political opposition. The broad use of such terms in criminal legislation should be avoided.

- *Elevating role of civil society in cybersecurity policy and strategy.* Plenary and discussion groups highlighted the role that organizations such as the Kenya ICT Action Network (KICTANet) have played in helping governments to understand the concerns of their people and pursue citizen-centric ICT policies. KICTANet's approach needs to be more widely replicated. For governments, this means more active efforts to incorporate civil society groups into the design and implementation of ICT policy. For civil society actors, it means leaning into a convening and coordinating role, vice one that focuses strictly on advocacy. Participants encouraged security forces to talk on equal footing with citizens, as opposed to hierarchically, can facilitate their work together.

Looking Over the Horizon on Cyberspace Security in Africa

Participant and panelist exchanges during the program also highlighted several elements of Africa's cyber threat landscape and state responses that warrant further analysis by researchers and additional discussion by local, regional and international policymakers.

Information technology as an enabling technology

The field of cybersecurity typically focuses on defending networks from attacks that compromise the confidentiality, integrity, or access to computer networks. The focus on cybersecurity is an important, but also narrow, frame for understanding how the spread of information technology is impacting national security in Africa and elsewhere. This is because the spread of information technology not only spreads computer-related vulnerabilities and exploits, but is also changing how state actors, organized criminal networks, and violent extremist groups organize, recruit, finance themselves, communicate, and deliver goods and services. Information technology is perhaps best conceived as an enabling technology that, like electricity or steam power, enables the growth and spread of other technologies, such as mobile payment networks, artificial intelligence, additive manufacturing, and unmanned aerial vehicles. Insofar as these technologies grow in sophistication, are low cost, and diffuse rapidly, they are likely to have profound consequences for peace, stability, and security in Africa and beyond.

Information technology and military strategy

African armed forces at times have attempted to model themselves off more technology-dependent armies in higher-income countries. Participants suggested it was time to rethink this approach, and to better understand the risks, vulnerabilities, and dependences that result from acquiring and using information and communications technology to collect intelligence, coordinate, and enable combat operations. The fact that African infantry, for example, tends to be less reliant information and communications technology than armed forces in other parts of the world is in one sense a strategic advantage, rendering them less vulnerable to cyberattack. Participants suggested that African armies need to be able to employ technology in ways that enable them to win in population-centric conflict, which could mean rethinking strategic approaches, operational doctrines, force structures, and roles for external actors. Moreover, to win in hybrid, information-based warfare, security forces need to establish cooperative relationships with citizens and private actors to leverage their capabilities and expertise.