RESEARCH BRIEF 2/2023
Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Author: Tomslin Samme-Nlar (SIGLA) **Series Editor:** Professor F. Vreÿ (SIGLA)

The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats[1]

Introduction

The dominant narrative of Africa's digital revolution has been one of techno-optimism. The spread of digital technology is frequently cast as a solution to all kinds of political, economic and social ills. Unfortunately, such simplistic narratives belie a more complex reality. The unprecedented wave of technological diffusion and innovation over the past two decades does indeed have the potential to transform lives and deliver higher standards of living. However, despite these benefits, digitization poses new threats and opportunities for cybercriminals to exploit vulnerabilities in the system. It has exposed vulnerabilities in critical infrastructure systems, introduced new challenges for the intelligence industry, and is influencing the contours of armed conflict on the continent. Below follows a brief overview of the four primary threats.

Discussion

The first threat is organized cybercrime. An increase in Internet penetration and the proliferation of technology is enabling rapid expansion of both cyber-dependent and cyber-enabled crime on the continent, perpetrated by organized cybercriminal networks. Organized cybercrime ranks among the top threats to Africa's enterprises and costs the region billions of dollars per year. The actors involved are wide-ranging including profit-seeking criminal organizations such as SilverTerrier, Black Axe Confraternity, Forkbombo, etc.; hacktivist groups such as Anonymous and Legion of Doom; and state-sponsored 'advanced persistent threat groups' who rob banks and steal sensitive information. Many of the profit-seeking organizations are also involved in 'traditional' forms of organized crime in Africa, taking advantage of technological innovations like social media, e-commerce websites and illicit dark web platforms to facilitate the sale of illicit goods and grow their activities in areas like illegal wildlife and human trafficking. The actors are located both in Africa and outside the continent with Africa-based actors increasingly growing in number, capability and influence. This increase is attributed to a

[1] See further reading below reference to the research paper that the author co-authored with Nate Allen and Matthew La Lime that serves as the primary source for this SIGLA Research Brief.

young, computer-literate population, coupled with joblessness and mounting economic inequalities, offering a wealth of potential recruits to criminal organizations. Without more licit forms of employment opportunities readily available, a generation of young hackers will be taught 'the business' of cybercrime by apprenticing with established cybercriminals. From a financing perspective, mobile money and cryptocurrencies have been noted as already enabling organized criminal groups across the continent to launder money and facilitate cross-border sex trafficking and human smuggling. In response, proactive legal and regulatory frameworks and better law enforcement capacity will be required to address and stop the expansion of organized cybercriminal networks on the continent. In addition, cross-boundary information sharing, legal harmonization and the capacity to extradite and prosecute criminals need to be developed. A deficit in cyber security knowledge and capacity is identified as one of the major challenges facing the continent.

The second category of cyber threat stemming from digital revolution is critical infrastructure sabotage. Globally, this form of threat is often perpetrated by states for strategic, national security goals and by criminal organizations to extract ransom and financial gains. In Africa, the majority of critical infrastructure attacks have been attributed to groups and individuals either seeking financial gain or activism purposes. They include the Cyber Horus group's attack on Ethiopia's critical infrastructure, a 2016 denial of service attack on Liberia's Lonestar Cell MTN network by a mercenary reportedly hired by Orange, a 2020 denial of service attacks on several Algerian government-owned websites, a 2020 attack on Uganda's MTN and Airtel mobile payment networks, and the 2021 ransomware attack on South Africa's Transnet possibly by either REvil or Darkside Cybercriminals. Only one record of attack – the WannaCry ransomware attack – has been positively attributed to a state-sponsored group. The lack of clarity on whether the Transnet attack was a targeted attack or was a result of an indiscriminate attack illustrates how Africa's critical cyber infrastructure can be vulnerable even to activities not intended for the continent. To stay ahead of the threat as the continent digitizes, African governments and private sector stakeholders, in consultation with civil society need to build cybersecurity into critical infrastructure systems and develop local skills because today, most significant threats are not detected by African institutions themselves, but by third parties.

The third category is cyber espionage. This is a growing threat to Africa, as the continent continues to rapidly develop its technological infrastructure. Many African countries lack the resources and expertise to effectively defend against cyber espionage, making them vulnerable to attacks. State-sponsored hackers and criminal groups are known to target African nations for various forms of sensitive information, such as national security secrets, trade secrets, and personal information of government officials and business leaders. The threat has predominantly been from state actors outside the continent. Publicized instances such as China's bugging of the African Union (AU) headquarters which they built illustrate this. However, the threat from local actors, including states, criminal networks, and armed groups within the continent is also growing rapidly because of the rapid diffusion of cheap digital surveillance technologies. Many African states are growing their inter-state digital espionage capabilities using spyware from various vendors such as NSO Group, SILAM, Huawei, ZTE, BAE Systems, Cloudwalk and Hacking Team. Authoritarian-leaning African governments also routinely employ mass surveillance tactics to clamp down on dissent and there is also the possibility of non-state armed actors on the continent acquiring similar advanced surveillance technologies and open-source intelligence (OSINT) that rival those of state actors. Because the reliance on ICT as a dominant tool of espionage is likely to grow, it is therefore important for African nations to increase their cybersecurity capabilities and invest in the development of their own talent to mitigate the threat of cyber espionage.

The fourth category is armed conflict innovation. Digital revolution has had a significant impact on armed conflict in Africa, where it has shaped the external communications, internal organization and combat operations of armed combatants. The influence of the Internet and social media cannot be overstated. Insurgent groups all use it to maintain an external presence and gain support like the case of Mali's Macina Liberation Front. The medium also facilitates 'franchising' of insurgent operations in Africa. Africa-based militant groups, such as Boko Haram, al-Shabaab or Jama'at Nasr al-Islam wal Muslimin are known to pledge alliance to internationally recognized groups such as al-Qaeda and the Islamic State over the Internet. The proliferation and the use of low cost drones is another way digital technology is affecting combat operations and tactics in Africa, evident in the heavy use of drones in Libya's second civil war. At least 19 African states have already acquired drones for either surveillance or combat purposes and six non-state militant groups are known to have used drones in combat operations. It is also common for both state and insurgent groups to use social media messaging apps such as Telegram and Facebook for command, control and operational planning. Though using digital technology for combat communication has proven to be a double-edged sword. Al-Shabaab found this out the hard way when many of its leaders were killed by American drone strikes, probably executed by monitoring their mobile devices.

Conclusions

The spread of digital technology across the African continent over the past two decades has already led to a fast-evolving array of security threats. The threats show few signs of abating and may indeed accelerate as Africa continues to digitize, as existing digital technologies become increasingly integrated into the functioning of society and as new technologies mature.

As observed in the above discussion, African governments, civil society and security sector actors will have to act with speed and foresight if they are to harness the benefits and limit the downsides of Africa's digital revolution. Addressing Africa's digital threats and challenges demands investments in cyber capabilities, policies, strategies, and legal frameworks. It necessitates reducing reliance on external actors to supply technology and ICT infrastructure, and to leverage multiple public and private sector partners to cultivate African-owned technologies. It requires investments in education, digital literacy and power infrastructure.

Many African countries are at a critical juncture in their journey towards cyber maturity. The decisions their leaders make about how their countries use information technology will have repercussions for decades. They must anticipate and respond to the cyber-threats their countries face. But they also must ensure information technology is used above all else as a tool to promote peace within their nations and the security of their citizens. Only then will Africa's digital revolution leave a different legacy from the industrial one.

Further Reading

Allen, N. La Lime, M. & Tomslin Samme-Nlar. '*The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats*'. Geneva, Switzerland: Global Initiative Against Transnational Organized Crime, December 2022. https://globalinitiative.net/analysis/digital-revolution-africa-cyber-threats/

Tomslin Samme-Nlar is an independent researcher from Cameroon and a member of the panel of experts at SIGLA, Faculty of Military Science, Stellenbosch University.

Email: mesumbeslin@gmail.com