

**GLOBAL
INITIATIVE**

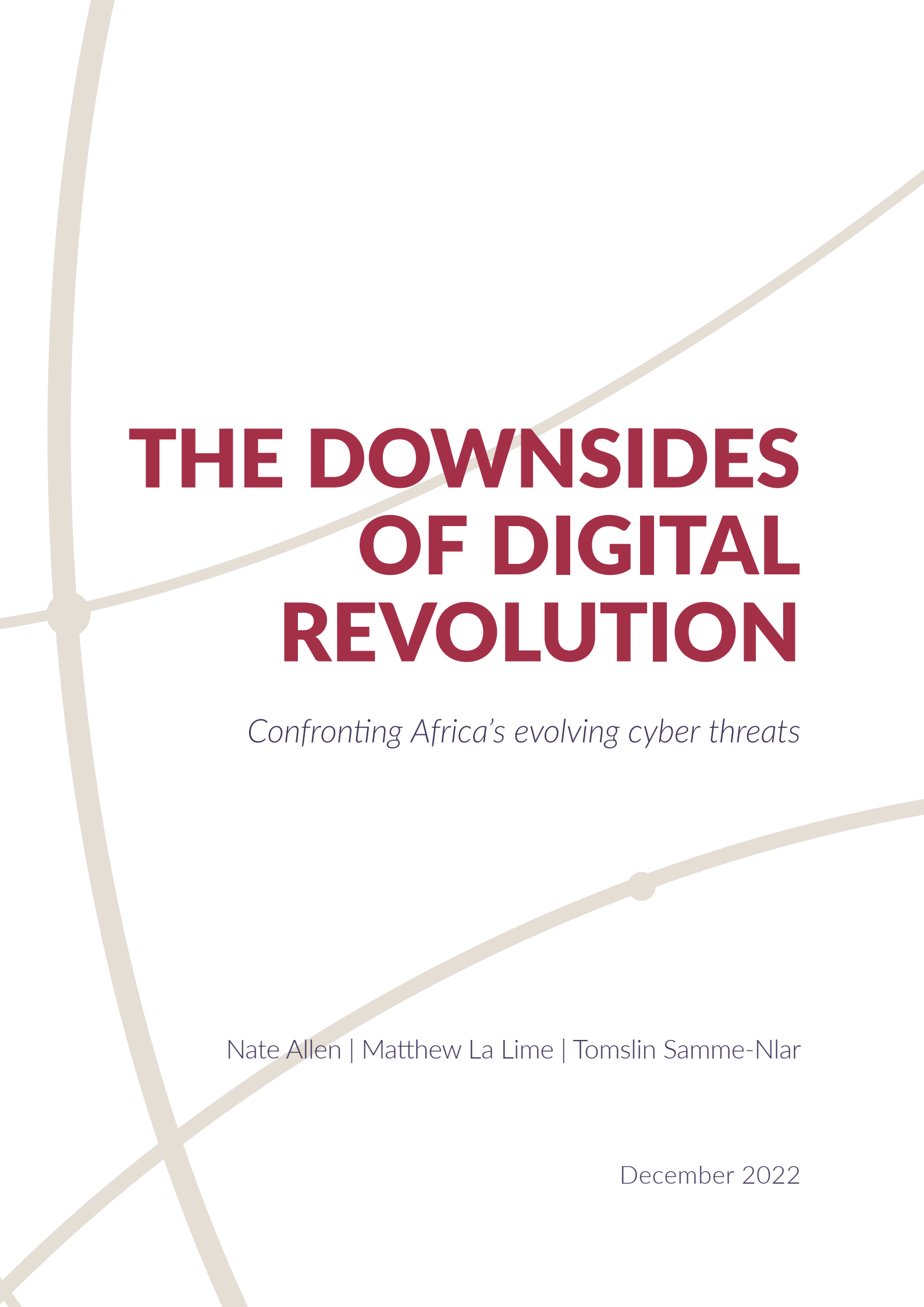
AGAINST TRANSNATIONAL
ORGANIZED CRIME

THE DOWNSIDES OF DIGITAL REVOLUTION

Confronting Africa's
evolving cyber threats

NATE ALLEN | MATTHEW LA LIME
AND TOMSLIN SAMME-NLAR





THE DOWNSIDES OF DIGITAL REVOLUTION

Confronting Africa's evolving cyber threats

Nate Allen | Matthew La Lime | Tomslin Samme-Nlar

December 2022

ACKNOWLEDGEMENTS

The authors would like to thank numerous individuals for feedback, advice and support they received while drafting this report. A big thank you to Matthew Herbert of the Global Initiative Against Transnational Organized Crime, who approached us about authorship, shepherded us through the editorial process, and provided extensive and detailed feedback. Without his support, this report would not have been possible. The authors would also like to acknowledge Joe Siegle, Elizabeth Vish, Yann Le Cloarec and Kenneth Adu-Amanfoh for providing excellent feedback and insight. As with all research projects, this was a collective endeavour, but any flaws in analysis are those of the authors. The opinions expressed in this report are those of the authors.

ABOUT THE AUTHORS

Nathaniel Allen is assistant professor of Security Studies at the Africa Center for Strategic Studies, a research fellow at the Security Institute for Leadership and Governance in Africa at Stellenbosch University, and term member with the Council on Foreign Relations. His expertise includes cyber issues, emerging technology, civil-military relations and regional security partnerships, primarily in North and West Africa.

Matthew La Lime is an academic associate at the Africa Center for Strategic Studies. He holds a PhD in African history from Georgetown University. His interests include development, the postcolonial state and emerging technology in Africa. His dissertation research in Guinea and Senegal was supported by the Fulbright and Boren programmes.

Tomslin Samme-Nlar is an engineer and independent researcher interested in issues where cyber-security and -strategy interact in Africa. He is a co-founder of Gefona Digital Foundation, a not-for-profit digital policy research organization in Cameroon, and the vice-chair of the Internet Corporation for Assigned Names and Numbers GNSO council.

© 2022 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Cover: © Ink Drop/Alamy Stock Vector; dan/Getty Images

Design and illustration: Ink Design Publishing Solutions

Cartography: Genevieve Hart

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

CONTENTS

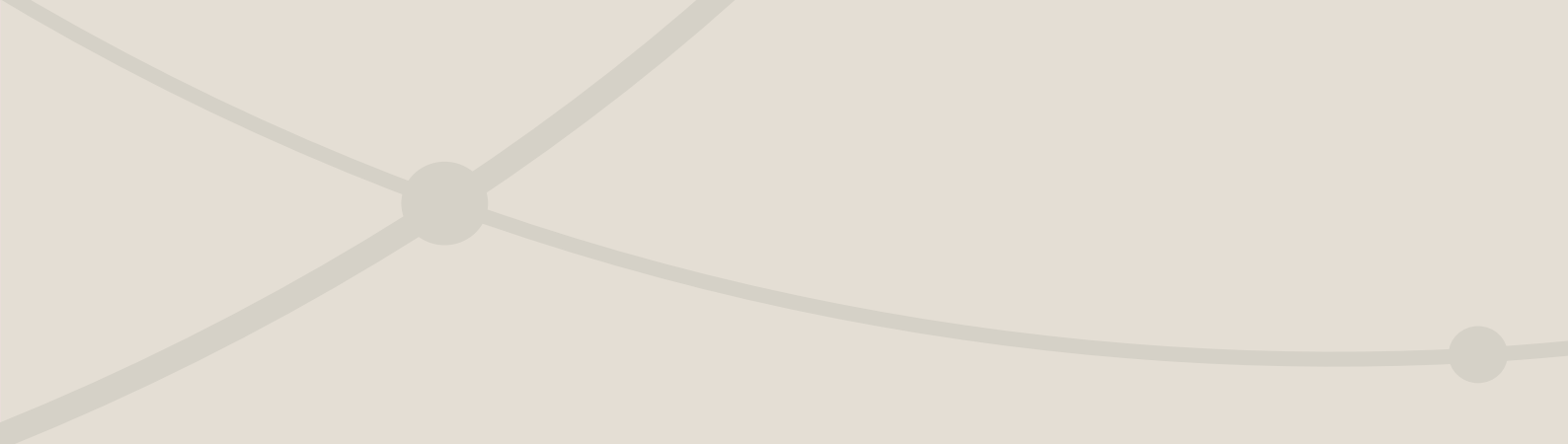
Executive summary.....	4
Methodology.....	7
The downsides of digital revolution	8
The digital revolution, cyberspace, and African peace and security	12
Definitions.....	13
The digital revolution and the changing nature of crime, conflict and coercion.....	14
Digital technology and organized crime	16
Cyberspace and the emergence of organized cybercrime	19
Information technology and traditional forms of organized crime	22
Cyberspace and financing organized crime	23
Critical infrastructure sabotage	25
Cyber-espionage.....	30
Armed conflict innovation.....	36
State and security sector responses.....	42
Conclusion and recommendations.....	46
Notes	55



EXECUTIVE SUMMARY

The harbour control tower of state-owned transport/logistics company Transnet.
Transnet was affected by a cyberattack on 27 July 2021.

© Rodger Bosch/AFP via Getty Images



To date, the dominant narrative of Africa's digital revolution has been one of techno-optimism. The spread of digital technology – from broadband internet to biometric identification systems – is frequently cast as a solution to all kinds of political, economic and social ills.

Unfortunately, such simplistic narratives belie a more complex reality. Over the past two decades, Africa has experienced an unprecedented wave of technological diffusion and innovation. At the same time, digitization has done little to enable the continent's leaders to address many of the core security and governance challenges – from rising conflict to declining democratic liberties – that their countries face.

This is because the impact of technology can never be divorced from the context in which it is used. Africa's digital revolution carries with it significant potential for benefit, but also enormous downsides, threats and challenges. This report is intended to help achieve a better understanding of these downsides, and to consider how African states, citizens and the international community can work together to address them.

Through the spread of computer-related vulnerabilities and falling communication costs, Africa's digital revolution is impacting and amplifying a broad array of security threats. This report offers a framework for categorizing these threats, highlighting the most significant ones and the actors involved. The framework, which constitutes the bulk of the report, details four primary threats.

The first is organized crime: the spread of information technology has driven the formation of highly organized and sophisticated cyber-dependent criminal enterprises. These groups, such as the Egypt-based Cyber Horus group and the Nigeria-based Silver Terrier (of which more later), are capable of conducting cyberattacks on behalf of state actors and employing advanced malware and phishing techniques to steal billions of dollars. In addition, online marketplaces and social media are altering the networks involved in more traditional organized crime networks, such as those behind human smuggling and drug smuggling. Finally, the rise of online banking, mobile payment networks and cryptocurrency is providing criminals across Africa with new targets and avenues of finance.

The second is critical infrastructure sabotage: Africa's government networks, military systems, banking, energy, transport and telecommunications industries are vulnerable to cyberattacks that seek to disrupt, disable or destroy them. The 2021 ransomware attacks against Transnet, the South African state-owned port, rail and pipeline operator, which disrupted shipping trafficking throughout southern Africa, is a leading indicator of what may follow if African nations fail to adequately protect increasingly digitized critical infrastructure systems.

The third is espionage: the digital revolution has fundamentally changed the methods and means through which states spy on one another and their citizens. Historically, the most significant cyber-espionage concerns in Africa have centred on external actors, like China. However, the rapid proliferation of state-of-the-art surveillance technology, methods and malware is leading to growth in the espionage and surveillance capabilities of African governments.

The fourth threat analyzed here is armed conflict innovation. The digital revolution is changing how both state and non-state actors organize, recruit, communicate and conduct their operations. Africa's insurgent groups have leveraged digital technology to catalyze their growth, and conflict theatres such as Libya and Ethiopia point to a future where algorithms and unmanned armed systems have become increasingly integrated into combat operations.

These threats will grow, evolve and become increasingly central to African security in the decades to come. Governments will play a decisive role in determining whether these threats are mitigated or whether they metastasize. They will face significant challenges. The African continent has greater deficits in cyber-capacity and resources than other regions. Many existing policies do not explicitly confront the threats mentioned above, or do so in ways that strengthen elites and undermine citizens. Fundamental questions exist about what role the African security sector should play in managing cyber-threats, with countries adopting widely differing approaches.

To manage Africa's growing array of cyber-threats, this report recommends that:

- **African governments** raise national awareness of cyber-risks and threats, implement multi-stakeholder national cybersecurity policies and strategies, identify and protect critical information infrastructure, adopt cybercrime legislation that prioritizes the protection of human rights, and improve international cooperation and engagement.
- **Security sector actors** increase capacity to investigate cyber-enabled and cyber-dependent organized crime, defend military information systems from external threats, coordinate critical infrastructure protection efforts, align information technology with population-centric military strategies and support cybersecurity policies that uphold the rule of law.

- **Regional organizations** support the creation of regional and continental computer security incident response teams (CSIRTs); create cross-disciplinary peace, security and emerging technology programmes; and provide additional opportunities for African countries to share good practices and lessons learned.
- **External actors** provide education and training opportunities for African cybersecurity professionals, invest in locally managed and driven efforts to build cyber-capacity, and limit the sale of sensitive surveillance technologies to regimes implicated in human rights abuses.
- **Private businesses** assess and grow their cybersecurity workforces, provide security as a service, and ensure the protection of critical information infrastructure they operate.
- **Civil society actors** support national cybersecurity policy, strategy and legislation through research, advocacy, monitoring and evaluation, and by convening dialogues to ensure that citizens' voices are heard on sensitive information and communications technology (ICT) issues.


Methodology

The approach to devising this framework was twofold. First, scholarship on the national security dimensions of cyberspace and the digital revolution was systematically reviewed. Secondly, a desk review of Africa-focused academic literature, news articles and grey literature sources was undertaken to assess the scope, scale and significance of these threats across the African continent. Due to the dearth of widely available or systematically collected information in the public domain on many of these threats, some of the conclusions drawn here are tentative. Therefore, this report relies where possible on illustrative case analyses to demonstrate the presence and significance of these threats across the African continent.

An aerial photograph of the Grand Ethiopian Renaissance Dam construction site. The image shows a large-scale construction project with multiple cranes, concrete structures, and a river in the background. A semi-transparent circuit board pattern is overlaid on the image, with yellow and blue lines connecting various points. The title 'THE DOWNSIDES OF DIGITAL REVOLUTION' is written in large, bold, white capital letters across the center of the image.

THE DOWNSIDES OF DIGITAL REVOLUTION

The construction of the Grand Ethiopian Renaissance Dam has raised considerable tensions with Egypt, leading to a cybercriminal attack by an Egypt-based network in June 2020. © Amanuel Sileshi/AFP via Getty Images



In June 2020, an Egypt-based cybercriminal network known as Cyber Horus hacked into the networks of the Ethiopian government, threatening war if Ethiopia began filling the Grand Renaissance Dam. The dam is a US\$4.6 billion hydroelectric project being built by Ethiopia on the Blue Nile and is highly contested by Egypt.¹ Over a dozen Ethiopian government websites were taken offline. State services to some regions halted. The Ethiopian Information Networks Security Agency alleged that Cyber Horus had intended to cause additional economic and political disruption but was unsuccessful.

The Horus group's attack was one of the first attempts to use offensive cyber-capabilities to coerce an African country over a high-profile political issue. The event illustrates how the effects of digital information technology on acts of coercion may be largely non-physical, yet highly disruptive. It also underscores the developing complexity and growth of African cyber-threat actors, a result of the continent's increasing digitization.

Rarely, however, are such developments reflected on in Africa's dominant discourse of techno-optimism. Instead, the effects of the rapid diffusion of ICT are framed predominantly in terms of their potential to transform daily life and deliver higher standards of living.

Despite these benefits, it is becoming increasingly evident that digitization poses new threats to African security and stability. Cyberspace has led to marked growth of organized criminal networks that either operate in or target Africa. It has exposed vulnerabilities in critical infrastructure systems, including government, military, telecommunications, finance, transport and energy sectors.² It is transforming the intelligence industry, making every phone a potential listening device.³ Digitally enabled technologies, like social media and drones, have influenced the contours of armed conflict by shaping the organization, strategies and tactics used by state and non-state actors.



Screenshot of computer compromised by Cyber Horus group. © Quartz

For African nations to harness the digital revolution's benefits, they must also limit its downsides.

The aim of this report is to help achieve a better understanding of how the global digital revolution is changing the African continent's national security threats and challenges, and to begin to consider how to address them. The central argument is that the spread of cyberspace in Africa has led to evolving digital threats, much as it has across the rest of the world. Today, Africa's cyber-vulnerabilities are exploited by a range of actors, and include organized crime, critical infrastructure sabotage, espionage and armed conflict innovation. Driven by rises in internet penetration, technological innovation and diffusion, cybersecurity actors and threats are likely to have an increasing effect on conflict, peace and security across Africa.

As mentioned, there are four broad categories of cyber-threats that African states face (see Figure 1). First is the threat from organized crime, or criminal enterprises that seek to profit through cyber-enabled means.⁴ The report shows how digital revolution has led to the formation of new kinds of criminal networks that operate in or target Africa; is impacting the market structure for more traditional forms of organized crime; and is changing how organized criminal networks across Africa secure financing and launder money. Africa-based organized cybercriminal networks, such as Silver Terrier and London Blue, have collectively stolen billions of dollars from individuals, business, governments and non-profit organizations around the world.

Second is critical infrastructure sabotage, which includes attempts to weaken or destroy national, government or military infrastructure, hardware or systems. This report shows how increasing internet penetration, reliance on foreign technologies and the existence of points of failure are leaving government and military systems, the financial sector, the energy sector and entry points across Africa vulnerable to critical infrastructure attacks. For example, a recent ransomware attack on Transnet, a South African state-owned infrastructure enterprise, caused billions of dollars in damages.⁵

Third, cyber-espionage entails attempts to penetrate a system to extract sensitive information. Rising digitization, rapid expansion in public and private sector surveillance capabilities, and advances in open-source intelligence are transforming and democratizing the

field of intelligence. Using recent revelations concerning the spread of spyware, such as the Israel-based NSO Group's Pegasus malware, to numerous African countries, the analysis shows that while African states remain vulnerable to espionage from abroad, they are simultaneously acquiring espionage and surveillance capabilities of their own.⁶

Finally, there is the threat posed by armed conflict innovation, or the use of digitally enabled technology to facilitate organized violence through external communications, internal organization and combat operations. The report demonstrates how advances in intelligence, surveillance and reconnaissance, the proliferation of social media networks and the deployment of unmanned aerial vehicles have affected armed conflict in Africa. Drone warfare, for example, played an important role in the 2019–2020 War for Tripoli in Libya.

Threat	Definition	Cases used
Organized crime	Criminal enterprises that profit from illicit activities through cyber-enabled means	Cyber Horus group's cyberattack on Ethiopia Silver Terrier Business Email Compromise Network Online marketplaces for East African human trafficking victims
Critical infrastructure sabotage	Attempts to weaken or destroy national, government or military infrastructure, hardware or systems	Cyber Horus group's cyberattack on Ethiopia Transnet ransomware attack
Espionage	Attempts to penetrate a system for the purposes of extracting sensitive or protected information	Pegasus malware
Armed conflict innovation	The use of cyber-enabled technology to facilitate organized violence through changes in external communications, international organization and combat operations	Libyan drone war


FIGURE 1 African cyber threat framework: definitions and cases.

SOURCES: UNODC, Module 1: Definitions of organized crime, Defining organized crime, April 2018, <https://www.unodc.org/en/organized-crime/module-1/key-issues/defining-organized-crime.html>; Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013; Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, Oxford University Press, 2019; UNODC, Use of the internet for terrorist purposes, 2012, <https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html>; Jacquelyn Schneider, The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war, *Journal of Strategic Studies*, 4, 2019.

A photograph of two young men, likely of African descent, looking down at their smartphones. They are outdoors, with a blurred background of trees and a building. The image is overlaid with a semi-transparent circuit board pattern in shades of green and blue. A large, bold, white title is centered over the image.

THE DIGITAL REVOLUTION, CYBERSPACE, AND AFRICAN PEACE AND SECURITY

Two brothers play Pokemon Go. The proliferation of mobile technology in Africa has made people more vulnerable to cyber attacks. © Stefan Heunis/AFP via Getty Images



Before discussing the impact of the digital revolution on Africa's security threats and challenges, it is important to begin with key definitions.

Definitions

While terms such as 'cyberspace' and 'digital revolution' are used ubiquitously, they have no universally accepted meaning. Following the Geneva Centre for Security Governance, this report defines cyberspace as 'an environment created by both physical and virtual components where data, information, or communication is stored, modified, or exchanged'. This definition captures the fact that while cyberspace is a largely virtual environment, it depends on physical systems such as fibre-optic cables and cellphone towers, and is designed to serve as a medium of communication and exchange between human users.

The digital revolution, by contrast, refers to growth of not just cyberspace but the digital technology that powers it. It can be defined as the development, advance, and spread of digital information and communications technologies. The digital revolution began in the immediate aftermath of World War II, when the invention of the transistor led to the emergence of modern computers and, eventually, the creation of the internet. Today, the digital revolution continues with increases in computing power and data storage, the spread of internet-connected devices (collectively referred to as the internet of things), and advances in artificial intelligence and automation.

Each of these concepts evokes different aspects of information technology and its vulnerabilities and risks. Rooted in, but distinct from, the physical world, cyberspace is exploitable using technical methods that arise from its digital nature. Reference to the digital revolution, by contrast, highlights the risks that stem from the rapid spread and acquisition of novel technologies that are becoming increasingly central to the functioning of society. Defining them is an important first step to understanding their significance for African peace and security.

The digital revolution and the changing nature of crime, conflict and coercion

The digital revolution is changing the nature of threat activities in at least two respects: by spreading vulnerabilities that arise from the technical nature of cyberspace, and by decreasing the costs of communication, which has, in turn, helped facilitate the rapid adoption of digitally enabled technology. Each of these factors has security implications for African governments, citizens and non-state actors, such as criminal networks and violent extremist organizations.

To begin with, there are technical vulnerabilities that affect all digital information systems. Computer security experts commonly identify three such vulnerabilities, which are targeted by virtually all forms of cyberattack.⁹ First, the confidentiality of a network can be compromised through exploits such as password theft or keylogging, allowing for unauthorized collection of information. Second, the integrity of an information system can be altered, misrepresented or deleted, at times causing damage to the system itself. The Stuxnet attack, which damaged Iran's nuclear programme by causing centrifuges to spin out of control, is an extreme example of an attack on information system integrity. Finally, legitimate users can be denied access to information, preventing them from using their applications, networks, accounts or devices. Distributed denial of service (DDoS) attacks, which can take a server offline by flooding it with traffic, are examples of cyberattacks that denies access. Some kinds of cyberattacks exploit multiple types of vulnerabilities – for example, ransomware, which alters a system's integrity by encrypting information, in the process denying users access to its content.

Confidentiality, integrity and access (CIA) vulnerabilities, commonly referred to as the 'CIA triad', form the basis of the field of cybersecurity (see Figure 2).

The implication of these technical vulnerabilities for African countries is straightforward. The more that African countries digitize, the more they become dependent on networks vulnerable to cyberattack. The African continent remains the world's least digitized region, which has insulated it from the worst effects of computer-based attacks in comparison to more technology-dependent regions of the world. This is changing rapidly, however, as broadband becomes more widely available and internet penetration rates rise. In the continent's more digitized regions, countries and cities – such as Nairobi, Lagos and Casablanca – cyberattacks have risen in tandem with growing internet access and, increasingly, dependence on innovations like mobile money.

The challenges posed by the spread of digital technology are not, however, purely technical in nature. They extend beyond the realm of computer security. A second means through which the digital revolution is influencing coercive activities and actors stems from changes in how governments, businesses, criminal networks, violent non-state actors and individuals communicate. The internet and other mobile technologies have drastically reduced the costs of producing and storing information. As a result, information can be produced by anyone and reach virtually anywhere, nearly instantaneously, enabling new forms of collective action.

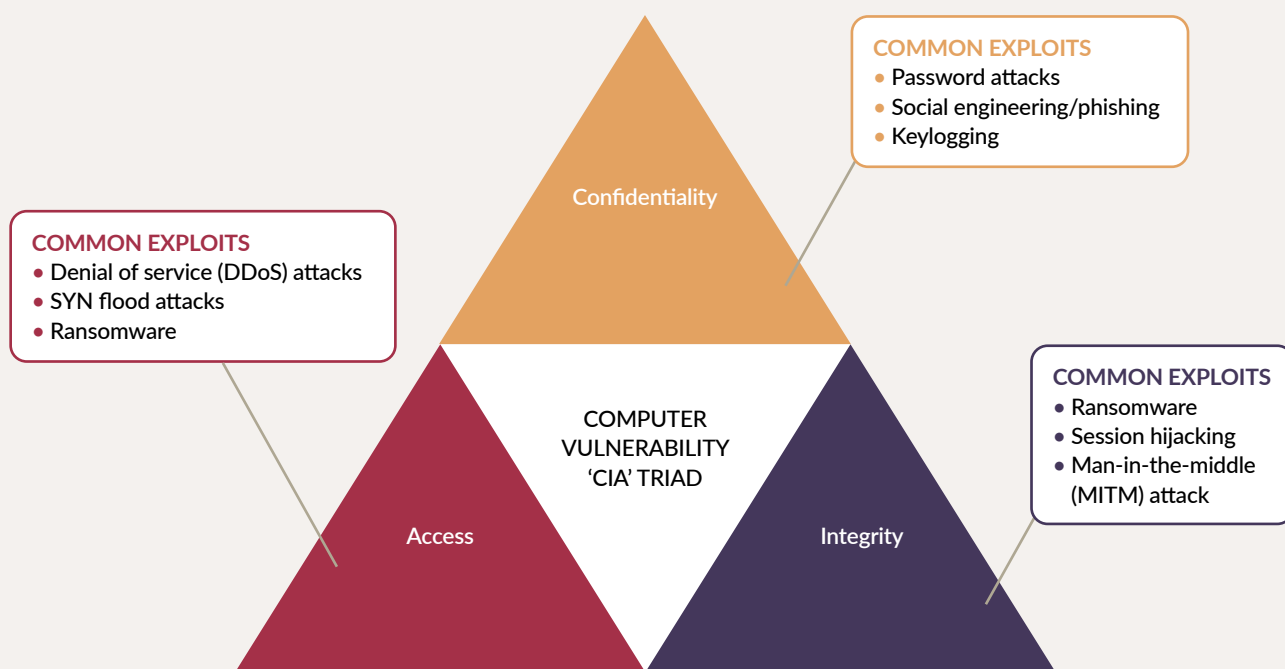


FIGURE 2 Computer exploits and vulnerabilities: the CIA triad.

One key implication is increased interconnectivity among malicious actors, and a globalized pool of victims. Digital technology has, for example, begun to transform organized criminal markets by facilitating globalized connections between buyers and sellers. Illicit goods, such as ivory poached in East Africa, motor vehicles stolen in West Africa or art looted in North Africa, are traded globally through online illicit marketplaces. Organized cybercriminal networks or state-sponsored actors – such as Scattered Canary, the Lazarus Group and Sandworm, to name but a few – deploy malware with the aim of committing fraud, stealing money or sabotaging the operations of African businesses, enterprises and governments.

A final consequence of the digital revolution stems from the fact that digital technology is an ‘enabling’ technology – one that enables other technologies. As an enabling technology, digital technology, like electricity or steam power, has led to a host of other inventions, from machine learning and artificial intelligence to additive manufacturing and cubic satellites. These are revolutionizing not only how we communicate, but also global distributions of wealth and power.

The key implication for African countries is that many forms of digital technology are cheap and rapidly diffusing. The cost to design a piece of malware is mostly an intellectual one – once created, it can be reproduced and transmitted with relative ease. The same is true of other digitally enabled technologies. Drones are no longer the limited domain of the world’s most sophisticated militaries, but are regularly used for surveillance, armed violence and to smuggle illicit goods. The proliferation of mobile phones and commercial satellite imagery allows for sophisticated analysts or non-profits to rival the information-gathering capabilities of nation-states.

As African states, citizens and criminal actors increasingly seek to harness disruptive new technologies, their significance for African peace and security will grow. More narrowly, however, the digital revolution has altered and amplified the nature of the threat from specific kinds of coercive activities and actors: from organized crime, espionage and critical infrastructure sabotage to armed conflict innovation. Though these threats are not unique to Africa and vary from country to country, they are of significant and increasing concern.



DIGITAL TECHNOLOGY AND ORGANIZED CRIME

Cybercriminals use a broad spectrum of attacks to compromise computer networks, including phishing, ransomware, man-in-the-middle attacks, denial of service attacks, zero-day exploits and cryptojacking. © AltumCode via Unsplash



The spread of digital technology has important implications for organized crime. Over the past decade, the proliferation of internet-enabled technologies, such as cryptocurrency and sophisticated malware, has provided tech-savvy crime groups with a range of new opportunities to steal, organize and extort. Common types of attacks that cybercriminals use to compromise computer networks are phishing, ransomware, man-in-the-middle attacks, denial of service attacks, zero-day exploits and cryptojacking, each of which can be accomplished with a wide array of tools (see Figure 3). Organized, cyber-enabled criminal networks are among the most rapidly growing and destabilizing criminal actors. In the past, a majority of such networks operated outside of Africa. Increasingly, however, African countries are becoming hubs for organized, cyber-enabled crime.

This section focuses on three main ways that cyberspace is transforming organized crime across Africa. First, cyberspace has led to the rise of novel organized cyber-criminal networks engaged in fraud, extortion or financial crime. Second, it is altering the way more traditional organized criminal economies, such as human smuggling and trafficking, and arms smuggling, operate. Finally, the rise of cryptocurrency and mobile money have afforded organized criminal networks across Africa novel means of financing.







Common types of attacks	Key tools used
 <p>Phishing: Sending emails purporting to be from reputable sources in order to induce individuals to reveal sensitive information.</p>	<p>Spear phishing: Malicious email spoofing attack that targets an organization or individual, seeking unauthorized access to sensitive information.</p> <p>Whaling: A highly targeted phishing attack – aimed at senior executives – masquerading as a legitimate email.</p> <p>Vishing: Phone calls or voice messages from criminals purporting to be from reputable companies with the aim of obtaining personal information, such as bank details and credit card numbers.</p> <p>Trojans (spyware, remote access tools, keyloggers): A type of malware that is often disguised as legitimate software that allows hackers to control a victim's device, gain backdoor access to a system, and obtain sensitive information.</p>
 <p>Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid.</p>	<p>Crypto ransomware: Encrypts valuable files on a computer so that they become unusable until ransom to hackers is paid.</p> <p>Locker ransomware: Locks the victim out of their device until ransom to hackers is paid.</p>
 <p>Man-in-the-middle (MITM) attacks: An attacker intercepts a two-party transaction, inserting themselves in the middle.</p>	<p>Packet sniffers: Software that monitors network traffic on wired or wireless networks and captures packets of data transmitted over the internet; typically used to gain unauthorized network access.</p> <p>Packet injection: A process whereby attackers inject malicious packets into data communication channels. Criminals use sniffing to identify how and when to send the malicious packets. The 'bad packets' then blend with the valid ones in the communication stream.</p> <p>Session hijacking: Access tokens theft allows hackers to make requests and impersonate legitimate service users.</p> <p>SSL stripping: Allows hackers to intercept legitimate data packets, modify the HTTPS-based requests and direct them to the insecure HTTP equivalent destination. This exposes sensitive data as plain text that is easy to steal.</p>
 <p>Distributed denial of service (DDoS) attacks: Sends multiple requests to websites with the aim of exceeding request capacity and shutting the site down.</p>	<p>Volume-based attacks: Include User Datagram Protocol (UDP) floods, Internet Control Message Protocol (ICMP) floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site.</p> <p>Protocol attacks: This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers.</p> <p>Application layer attacks: Comprise seemingly legitimate and innocent requests, the goal of which is to crash the web server.</p>
 <p>Zero-day exploit: A cyberattack targeting a software vulnerability that is unknown to the software vendor or to antivirus vendors.</p>	<p>Web browsers: Web browsers are common targets due to their ubiquity, as are email attachments that exploit vulnerabilities in the application opening the attachment.</p> <p>Zero-day malware: A computer virus for which specific antivirus software signatures are not yet available, so signature-based antivirus software cannot stop it.</p>
 <p>Cryptojacking: Malicious cryptomining that happens when cybercriminals gain access to digital devices and use malware to siphon funds.</p>	<p>File-based cryptojacking: Uses malicious emails to access the infrastructure of a computer.</p> <p>Browser-based cryptojacking: Hackers use programming languages to create a cryptomining script that is imbedded directly into the websites accessed from the corrupt browser, in outdated WordPress plugins and display ads.</p> <p>Cloud cryptojacking: Attackers search through the code or files of an organization in the hope of finding the application programming interface (API) keys to access the cloud service. Following this step, they can use CPU resources to mine cryptocurrency, leading to massive increases in electricity and computer power.</p>

FIGURE 3 The cybercriminal toolkit.

SOURCES: *Oxford English Dictionary*; Infocyte, Cybersecurity 101: Intro to the top 10 common types of cybersecurity attacks, 23 August 2021, <https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks>; Amos Kingatua, 6 HTTP MITM attack tools for security researchers, GeekFlare, 7 July 2021, <https://geekflare.com/mitm-attack-tools>; Kaspersky, What is a DDoS attack? – DDoS meaning, <https://usa.kaspersky.com/resource-center/threats/ddos-attacks>; Imperva, Distributed denial of service attack (DDoS) definition, <https://www.imperva.com/learn/ddos/ddos-attacks>; Ruslana Lishchuk, An overview of cryptojacking & useful tips on how to prevent cryptojacking, Clario Blog, 17 February 2021, <https://clario.co/blog/what-is-cryptojacking>.

Cyberspace and the emergence of organized cybercrime

The spread of digital technology has led to the formation of new organized cybercriminal networks, which now rank among the top threats to African enterprises and cost the region's economy billions of dollars per year.¹⁰ These networks commit a combination of cyber-dependent and cyber-enabled crimes. While the former category refers to crimes that can only be done with the use of a computer,¹¹ such as the cyberattacks listed in Figure 3, the latter refers to crimes whose scale has been increased through the expansion of digital technology. Examples of the latter include crimes such as extortion, fraud, money laundering, copyright infringement and the sale of illicit goods online.¹² Perpetrators of both sets of crimes encompass a wide variety of actors, including state-sponsored 'advanced persistent threat groups' who rob banks and steal sensitive information; hacktivist groups such as Anonymous, Legion of Doom, or Chaos Computer Club; and profit-seeking criminal organizations such as Magecart, RZEvil and Darkside.

African countries, governments, enterprises and organizations routinely fall victim to attacks by transnational organized cybercriminal groups who operate outside of Africa. At times, African governments, businesses and organizations are explicitly targeted. In 2018, for example, websites of the government of Gabon were defaced by the hacktivist group Anonymous in protest at the dictatorship of President Ali Bongo.¹³ African states and companies also fall victim to more indiscriminate global attacks. This was the case with the 2017 WannaCry ransomware attack, which affected public institutions and businesses in nine African countries as part of a broader operation that resulted in billions of dollars of damages around the world.¹⁴ The attack has been attributed to the North Korean-sponsored Lazarus Group.¹⁵

The threat from organized, cyber-enabled crime is also rapidly expanding within Africa. Organized African criminal networks who commit fraud, extortion, ransomware attacks, and online romance scams are increasing in scope and severity.¹⁶ These networks possess varying levels of skill. It is thought that the continent's most capable cybercriminals are based in West Africa, specifically in Nigeria. Some, such as the Black Axe Confraternity and London Blue, are long-standing criminal networks who also engage in more traditional types of crime alongside their cyber-dependent activities (see Figure 4). These organizations possess complex hierarchical structures, mafia-like indoctrination practices, and are generally transnational in nature, with members based in Africa, Europe and the United States.¹⁷ Other organizations, such as the fast-growing African malware and hacker groups, are more acephalous. Adherents work together on criminal operations, seek mentors and apprentices, share software and best practices with one another, but do not take orders from a centralized command structure or follow a supreme leader

Organized African criminal networks who commit cyber attacks and online scams are increasing in scope and severity.

Group name	Base of operations	Crime types	Tactics and malware used	Scope of the threat
SilverTerrier ¹⁸	Nigeria United States	Business email compromise (BEC)	Phishing Information stealers Remote access tools (RATs)	480-interrelated threat actors Over 2.1 million attacks At least US\$3 billion in losses
London Blue ¹⁹	Nigeria	Online scams Business email compromise (BEC)	Phishing Fake online ads Commercial data analysis	50 000 potential targets Members in three continents
Black Axe Confraternity ²⁰	Nigeria	Prostitution Human trafficking Narcotics trafficking Theft Money laundering Email fraud/ cybercrime	Phishing Spam campaigns Romance scams Document forgery	Hierarchical group structure Members in three continents US\$100s of millions stolen
Forkbombo ²¹	East Africa	Money laundering Cybercrime Online banking theft	Opensource malware tools Spyware and keyloggers	Constant threat to African banks Produce and distribute malware
Grapzone threat group ²²	Kenya	Cyber-enabled fraud Air tickets and Money Gram heists	Remote access tools (RATs) Spyware and keyloggers Hardware backdoors	Threat to Kenyan businesses Threat to money transfer firms
Silent Cards ²³	East, Southern, and Central Africa	Cyber-enabled fraud Cybercrime	Spyware and keyloggers Hardware backdoors	Targets banks, mobile banking service providers, ISPs, holding companies, hedge funds, betting firms, government, and financial sectors across East Africa.
The Sakawa Boys ²⁴	Ghana	Cyber-enabled fraud Romance scams	Phishing Social engineering	Frequently target men in Asia, Europe and America with romance scams
AnonGhost ²⁵	Northern Africa	Cyber-espionage	Manual hacking	Targets global governments to make classified information public Members in four continents
Scattered Canary ²⁶	Nigeria	Business email compromise (BEC)	Phishing Information stealers Remote access tools (RATs) Identity theft Social engineering	Attempted to defraud federal Cares Act of US\$5.4 million in COVID relief payments

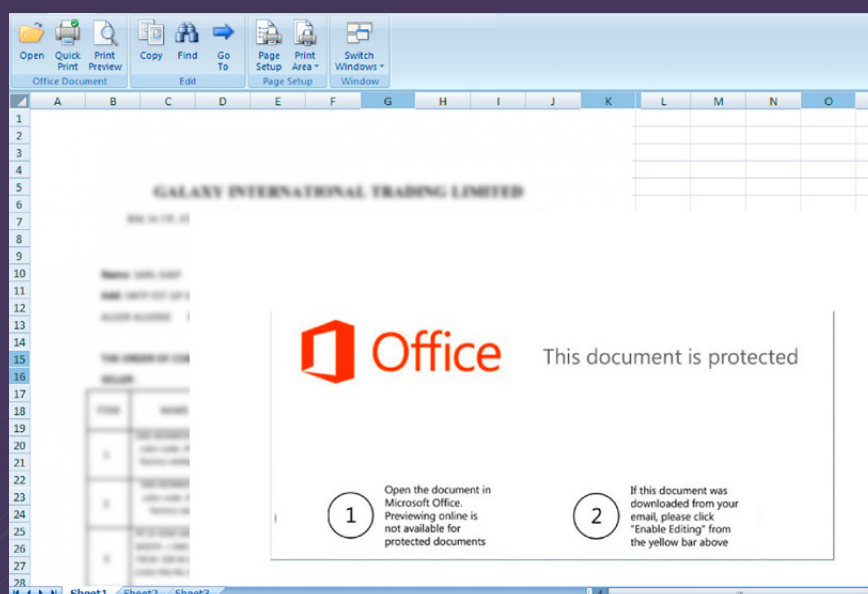
FIGURE 4 Major organized cybercriminal threat actors in Africa.

Africa-based cybercriminal networks and organizations have increasingly global reach. Little illustrates this better than the rise of the business email compromise (BEC) scam. BEC scam networks consist of loosely connected networks of criminals who use a combination of state-of-the-art malware and social engineering to deceive, infiltrate and extort money from wealthy businesses, organizations and individuals around the world. According to the Palo Alto-based Unit 42, approximately half of BEC actors are based in Nigeria and a quarter in the United States, with the rest scattered in other countries.²⁷ According to the United States Federal Bureau of Investigation, BEC has rapidly grown in recent years, resulting in as much as US\$43 billion in losses since 2016.²⁸

This figure would put annual BEC losses on par with, or greater than, major transnational organized crimes, such as small arms trafficking and the illegal wildlife trade.²⁹ One of the most prominent threat actors is SilverTerrier, which generated an estimated US\$3 billion dollars in revenue in 2019 (see box: 'The SilverTerrier business email compromise network').³⁰ More recently, a similar group, known as Scattered Canary, was suspected of attempting to steal hundreds of millions of dollars in unemployment insurance from state governments across the United States during the COVID-19 pandemic.³¹

The SilverTerrier business email compromise network

SilverTerrier is a constellation of over 480 Nigerian hacking groups that began to crystallize in 2014 when members of 419 'advance fee' cybergangs started to band together and search for new ways to conduct online crime. Today, the organization has become among the world's most successful perpetrators of internet fraud. SilverTerrier actors engage generally in BEC scams and combine high quality malware with sophisticated phishing tactics (see the screenshot). Much of SilverTerrier's effectiveness is attributable to their ability to develop and utilize newly emergent technological tools. In 2019, SilverTerrier actors created 81 300 malicious software samples, which allowed groups to conduct over 2.1 million targeted attacks in that year. Since then, actors' capacity to distribute attacks through email soared to 90 000 messages per month, with one cybersecurity firm experiencing 245 000 attacks.³²



Screenshot of SilverTerrier malware attachment. © Unit42

Social media, e-commerce websites and illicit dark web platforms are facilitating the sale of illicit goods to customers in Africa.

As internet penetration across Africa continues to increase, it is likely that transnational organized cybercriminal networks will expand. For one, the relative lack of cyber-awareness and cybersecurity precautions among businesses, enterprises and governments in Africa have rendered the continent's more digitized states an appealing target. In addition, a young, computer-literate population in many countries, coupled with the spread of new technologies, joblessness and mounting economic inequalities, offers a wealth of potential recruits. 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, growing networks of cybercriminals.³³

Information technology and traditional forms of organized crime

The spread of cyberspace is beginning to alter the markets and networks involved in more 'traditional' forms of organized crime in Africa, from human smuggling to drug trafficking. The main cause is the spread of online marketplaces and social media platforms, which ease communication and facilitate exchange between organized criminal networks, middlemen and customers of illicit goods.³⁴ As a result, organized criminal networks in Africa are becoming more integrated and globalized.

Social media, e-commerce websites and illicit dark web platforms are facilitating the sale of illicit goods to customers in Africa. This is particularly true with respect to organized criminal markets dealing in motor vehicles, illegal firearms, illicit drugs and counterfeit drugs. Fake pharmaceuticals, for example, which are increasingly distributed online, constitute between 30% and 60% of pharmaceuticals on the continent, and have been reportedly linked to around 100 000 deaths in Africa every year.³⁵ The issue is likely to worsen as e-commerce grows: in South Africa, it is estimated that 30% of online shoppers unknowingly buy fake goods.³⁶

The internet is also facilitating the growth and integration of African actors into organized criminal networks operating in the illegal wildlife, mineral, and human smuggling and trafficking markets. In 2017, a report from the International Fund for Animal Welfare determined that wild animals and their products were sold across 33 online marketplaces and on three social media platforms.³⁷ Poachers and smugglers are based mostly in countries with significant wildlife populations, such as Tanzania, Ethiopia, Côte d'Ivoire and Uganda, and use the internet to advertise endangered species and their products to buyers around the world.³⁸

Perhaps no singular criminal market in Africa has been more impacted by digitization than human smuggling and trafficking. Smugglers, for example, have made substantial use of Facebook Live and TikTok, in particular in North Africa, to reach potential clients and advertise services.

More problematically, online ads and social media platforms like Facebook, WhatsApp, Twitter and Instagram enable human traffickers to attain a victim's location and deceive them into seeking services for moving abroad. Traffickers first target victims and then send them tailored messages to exploit their interests, desires and vulnerabilities. Young women are often lured by

marriage proposals or the prospect of better paying jobs. Men are enticed by false job offers or with fake sports deals, contest offers or university acceptances.³⁹ Victims are then purchased from African sellers and delivered by organized crime networks to customers in Europe and the Middle East through other platforms, such as Haraj and 4Sales.⁴⁰ Upon arriving at their destination, however, both are sold into slavery or forced to reimburse their debt to smugglers, most often through forced labour or sex work.⁴¹

Despite this rise in cyber-trafficking, most migrants still seek out traffickers themselves and establish relationships through word of mouth or friends and family.⁴²

Cyberspace and financing organized crime

Deepening levels of online connectivity across Africa are altering the way in which both traditional and organized cybercriminal networks are financed. A wide array of criminal networks and organizations have begun to exploit the internet, online banking, mobile transfers and cryptocurrencies for the purposes of money laundering. INTERPOL warns that mobile money services like M-PESA, Orange Money and MTN Mobile Money could soon be used with greater frequency to launder ill-gotten funds.⁴³

The use of the internet and other mobile technologies is a concern in Africa in part because of financial innovation. Payment methods that allow individuals to remain unidentified, like cryptocurrency, are facilitating illicit financial flows between Africa and the world.⁴⁴ The number of Africans using cryptocurrency has grown exponentially in recent years. Between July 2020 and June 2021, Africa's cryptocurrency market grew by 1 200% to US\$105.6 billion worth of transactions.⁴⁵ Kenya, South Africa, Tanzania and Nigeria, where up to a third of individuals between the ages of 18 and 60 are invested in cryptocurrencies,⁴⁶ rank among the world's top 10 countries in terms of overall cryptocurrency adoption.⁴⁷ In 2022, South Africa was identified as

among the nations receiving the highest volume of cryptocurrency from illicit addresses and, in 2020, experienced the world's largest crypto-scam, resulting in hundreds of thousands of victims being swindled out of a total of US\$588 million in Bitcoin.⁴⁸

In recent years, Africa has evolved into a global centre for mobile money – a technology that Africans use to receive, store and spend funds using a mobile phone. More than 350 million people in sub-Saharan Africa use mobile money, and the total value of these exchanges was recently estimated at US\$300 billion.⁴⁹ The growth in mobile money among consumers has led to a rapid rise in organized criminal networks who exploit mobile money services to commit fraud and theft. Scams are carried out using several strategies, from 'vishing' schemes which see fraudsters gain access to users' accounts through phone calls and SMS, to advance-fee scams where users are tricked into sending money to criminals under false pretences.⁵⁰ Stephane Konan, a former senior official in Côte d'Ivoire's defence ministry, said that 'between 1990 and 2002, there were many attacks against banks by criminal groups by young people ... today, we no longer have bank robberies.'⁵¹

Mobile money has been used by kidnappers for the purposes of extortion.

Mobile money also provides organized criminal groups across the continent with new ways to launder money. Services such as M-PESA and Orange Money allow individuals to transfer money across borders and have grown explosively in recent years. At an individual level, the rise of mobile money is arguably a beneficial hedge against street crime, limiting the amount of cash an individual need carry at any given time.⁵² However, it also raises risks around the laundering of criminal proceeds and funding of illegal activity across multiple jurisdictions.⁵³ Some research has suggested that mobile money services, for example, are likely to already facilitate cross-border sex trafficking and human smuggling.⁵⁴ Mobile money has also been used by kidnappers for the purposes of extortion. In April 2019, for instance, Ugandan kidnappers demanded US\$500 000 be sent to their mobile money accounts in exchange for the release of an American citizen.⁵⁵ In 2020, kidnappers in Kenya intended to collect a ransom for abducting a Chinese man using M-PESA.⁵⁶

Despite significant anecdotal information on the role of the internet, cryptocurrencies and mobile money platforms in financing organized crime, their overall impact on the scope and scale of organized crime in Africa is difficult to assess – a challenge seen also at the global level.⁵⁷ The relative novelty of financial technologies and deficits in law enforcement capacity mean that a significant portion of illicit web-based financial transactions go unmonitored and general continent or country-wide statistics are hard to come by. Digitization also offers authorities tools to monitor and track financial flows. For now, most traditional criminal actors and networks in Africa appear to prefer to trade in hard cash and more familiar, localized revenue streams over mobile money, cryptocurrency or dark web markets.⁵⁸ Furthermore, the pressures of international law enforcement have forced many criminals to conduct sales, communications and financing using hidden platforms found in the darker corners of the internet.⁵⁹


Nevertheless, as the African continent becomes increasingly networked, it is inevitable that organized criminal networks across the continent will avail themselves of digital means of financing. So long as legal frameworks and law enforcement capacities lag behind criminal ingenuity, Africa's criminal organizations are likely to expand their efforts to leverage internet-enabled revenue streams.

A Transnet freight train is shown in the foreground, with the number 10140 visible on its side. The background features a large electrical pylon and power lines. The entire image is overlaid with a digital rain effect, consisting of vertical columns of green and blue characters and symbols. A white geometric line, resembling a stylized 'Y' or a network connection, is superimposed over the top left and center of the image.

CRITICAL INFRASTRUCTURE SABOTAGE

A Transnet freight train transports coal to Mpumalanga, South Africa. In July 2021, Transnet was the target of a cyberattack, which shut down key operating systems.

© Waldo Swiegers/Bloomberg via Getty Images



Another form of cyber-threat comes from critical infrastructure sabotage. Cyber-sabotage, or what cyber-experts often refer to as a computer network attack,⁶⁰ is the least common form of cyberattack,⁶¹ but potentially the most destructive. Unlike the purely criminal activities detailed in the previous section, cyber-sabotage is a tool used both by criminal organizations, to extract ransoms and financial gains, and by states, for whom acts of cyber-sabotage are employed for strategic, national security goals.

Critical infrastructure

Critical infrastructure can be defined 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'.⁶² They include systems in sectors such as energy grids, telecommunications networks, ports, banks, government functions and military systems. Cybersecurity experts often use the term 'critical information infrastructure' to refer specifically to interdependent, interconnected information systems necessary for the functioning of critical infrastructure across multiple sectors. These typically include telecommunications networks themselves, as well as controlling information systems like supervisory data control, and acquisition and incident command systems.⁶³

The threats to Africa's critical infrastructure from cyber-sabotage vary according to the capability and intent of the actors involved. The most damaging and sophisticated cyberattacks, such as Russia's attacks on Ukraine's energy grid and economic infrastructure,⁶⁴ Israel's 2007 attack on Syria's highly regarded air defence network,⁶⁵ and the Stuxnet worm attack on Iran's nuclear programme, were each state-sponsored acts of cyber-sabotage. In Africa, however, there have been few, if any, acts of cyber-sabotage targeting critical infrastructure confirmed to be the work of state-sponsored actors. In part, this may be due to limited offensive cyber-capabilities within African states, limited interest from external state actors with sophisticated offensive cyber-capabilities and Africa's relatively limited amount of cyber-dependent critical infrastructure.⁶⁶

However, lack of direct state attribution may result from the covert nature of many cyberattacks on critical infrastructure, which can be used as posturing and signalling below the threshold of armed conflict and often lead states to deny responsibility for an attack or work through proxies, including organized cyber-criminal networks or 'hactivist' organizations.⁶⁷ The Cyber Horus group's attack on Ethiopia's critical infrastructure described earlier in this report is one such example: the group has no confirmed linkages to state-sponsored actors. Another example can be found in 2020 denial of service attacks on

25 Algerian websites, including several owned and operated by the Algerian government, by a group known as MoroccoHackTeam. Algerian authorities accused the Moroccan government of sponsoring the attack, accusations that the Moroccan government denied.⁶⁸ Demonstrating increased vulnerabilities and increased capabilities, cyberattacks that disrupt, deface or compromise government networks are commonplace. Since 2020, cyberattacks have shut down government networks and infrastructure in Cape Verde, Algeria, Ethiopia, Kenya, South Africa, Gabon and Nigeria (see Figure 5).⁶⁹

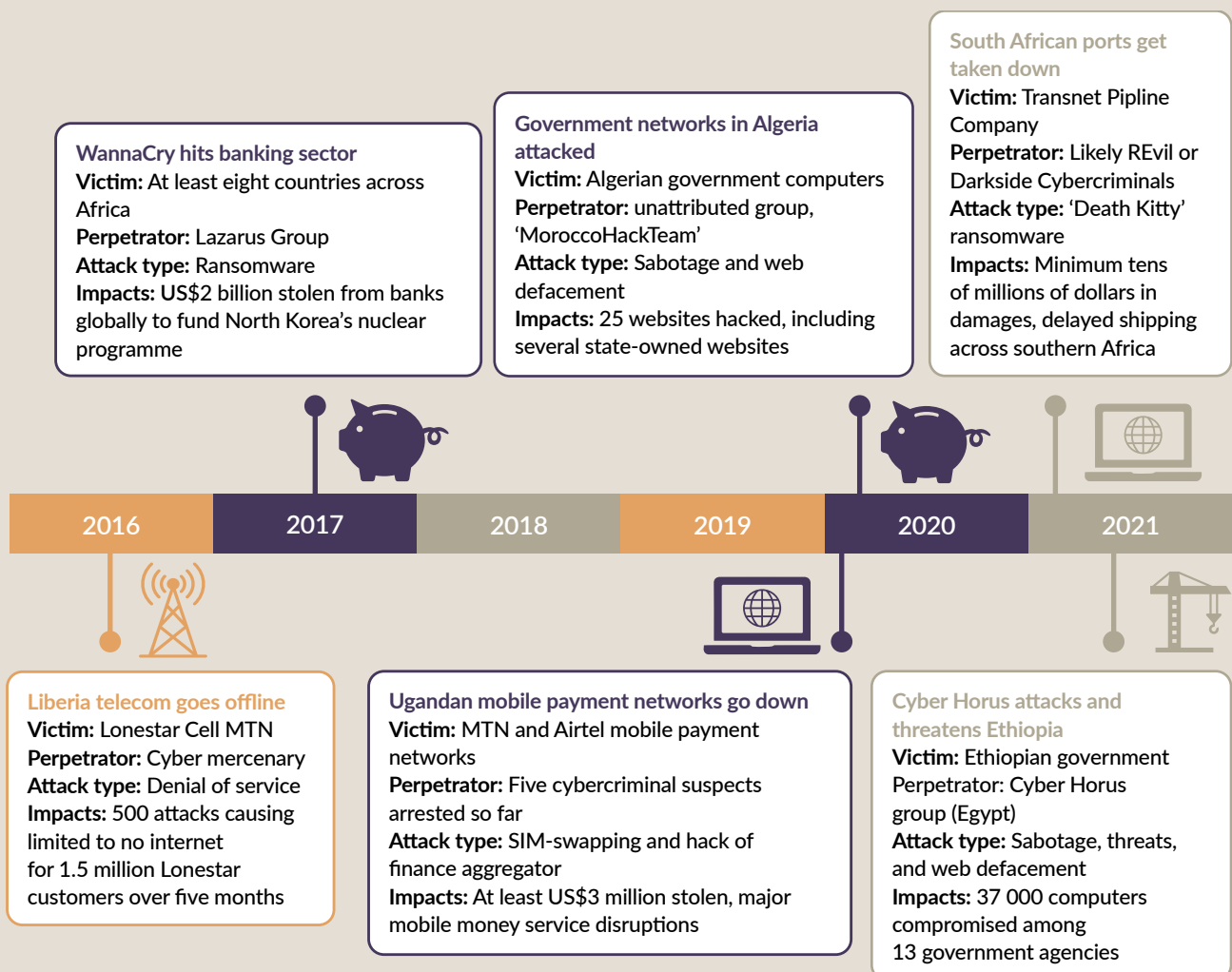


FIGURE 5 Major cyberattacks on African critical infrastructure.

SOURCES: Various sources cited in this section

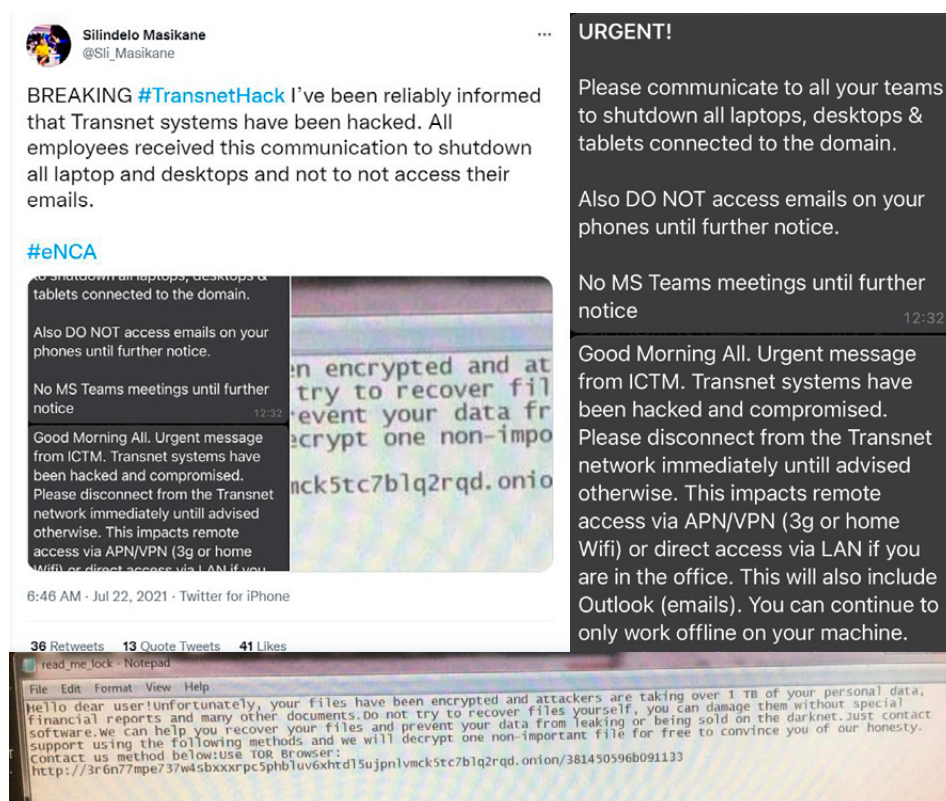
Driving this increase may be the proliferation, advancement and affordability of hacking tools like pay-to-use malware and ransomware, which are increasingly enabling cybercriminals to target critical infrastructure for financial gain. In October 2020, hackers compromised Uganda's mobile money network by using about 2 000 SIM cards to gain access to the MTN mobile money payment system. In addition to stealing US\$3.2 million, major service providers in Uganda were forced to suspend mobile money transactions because of the attack.⁷⁰ The most significant critical infrastructure attack in Africa was the result of a ransomware attack against Transnet, the South African state-owned infrastructure and port operator, which caused a significant slowdown in shipping at the ports of Cape Town and Durban, and threatened to disrupt the economy of the entire southern African region. The impact of the attack was concerning because the port operator constituted a 'single point of failure' – infrastructure that is not easily substituted or replaced, highlighting a need for more system redundancy and resilience (see box: 'Ransomware attack on Transnet').⁷¹

Ransomware attack on Transnet

In July 2021, Transnet notified its customers that it had 'experienced an act of cyberattack, security intrusion and sabotage'.⁷² Hackers had broken into the company's systems and used ransomware to encrypt over a terabyte of the company's files (see Figure 5).

In addition to compromising Transnet's online operations, the attack forced the shutdown of Transnet's Navis operating system, software the company relied on to coordinate the movement of shipping containers. As a result, shipping operations were brought to a crawl in all major South African ports, including Durban, which processes 60% of southern Africa's containerized trade. Unable to meet its contractual obligations, Transnet declared a force majeure, which lasted from the time the attack struck on 22 July until 2 August, at which point the Navis system was back online and most major systems had been restored. Though the perpetrator has not been definitively attributed, the Death Kitty strain of ransomware used to hack Transnet resembled that used in similar attacks by organized cybercrime syndicates based in Eastern Europe and Russia.

The fact that most major systems affected in the attack were restored within two weeks prevented a worst-case scenario. According to economist Mike Schussler, a longer delay could have had a 'domino effect on the rest of the economy ... [shaving] quite a few percentage points off the gross domestic product' of the entire southern African region.⁷³ The economic impact was still significant, however. Supply chains for animal products, fruit and vegetables, and other agricultural goods were severely disrupted. The attack also affected the manufacturing sector. BMW South Africa estimated that the disruptions stemming from the cyberattack, combined with protests, cost the car giant R200 million (US\$14 million) in lost sales.⁷⁴



Messages and posts at the time of the Transnet ransomware attack. Source: Twitter

It is not clear whether Transnet was deliberately targeted or its shutdown the product of a more indiscriminate ransomware attack, illustrating how cyber-operations are unpredictable, and, indeed, at times critical infrastructure sabotage can be the result of unintended consequences. This was the case between late 2016 and early 2017, when a corporate hacker hired by one of Liberia's two major telecommunications companies conducted hundreds of denial of service attacks against its main rival in a bid to get customers to switch. The attack, which used a Mirai botnet to hijack unsecured CCTV cameras, proved far more damaging than intended. According to one report, in the initial phases of the attack, 'half the country was cut off from bank transactions, farmers couldn't check crop prices, and students couldn't Google anything'.⁷⁵ It was not until the software used in the attack had been repurposed and used against Deutsche Telecom, a German telecommunications giant, that authorities outside of Liberia noticed and the hacker responsible, a British national who had never set foot in Liberia, was caught and arrested.⁷⁶


In short, in an era of increasingly sophisticated attacks, growing digital dependency, and port, energy and telecommunications systems that constitute single points of failure, critical infrastructure across Africa is vulnerable to cyber-sabotage. Government and private sector stakeholders need to build cybersecurity into critical infrastructure systems as the continent digitizes if they wish to stay ahead of the threat.



CYBER-ESPIONAGE

Artificial intelligence-enabled surveillance capabilities draw on technologies like CCTV cameras and facial recognition to predict and respond to crime.

© Luke Dray/Getty Images



Espionage broadly refers to attempts to penetrate an adversarial system in order to extract sensitive or protected information.⁷⁷ By stealing user credentials, tapping or engineering backdoors into cables or routers, installing malware, through legal or intelligence-sharing arrangements with service providers and, increasingly, through tools such as open source intelligence, attackers can collect intelligence about an adversary's capabilities or intentions, steal sensitive military secrets, or inform business deals or diplomatic negotiations.

Lack of threat detection capabilities and reliance on external actors for key ICT infrastructure make many African states highly vulnerable to cyber-espionage. To date, the main concerns around cyber-espionage in Africa have centred on China, whose investments in African ICT infrastructure most likely give it unique cyber-espionage capabilities. China has built 70% to 80% of Africa's telecommunications networks, provides services to more than 300 million African users and has set up government networks for over 20 of the continent's states.⁷⁸ As the continent's largest supplier of ICT infrastructure, China possesses the capability to install monitoring devices into physical infrastructure or backdoors into sensitive ICT platforms.

The threat is not theoretical. The most publicized instance of cyber-espionage in Africa concerns China's bugging of the African Union (AU) headquarters, which it built in 2012. In 2018, African systems engineers discovered that 'all the content on the AU building's servers was being routinely transmitted to Shanghai'.⁷⁹ Though the AU was reluctant to call out the Chinese publicly, Algerian and Ethiopian cyber-security experts replaced existing servers and installed a new video-conferencing system that operated independently of Chinese hardware.⁸⁰ Nevertheless, the threat persisted. Two years later, it was revealed that China had been extracting security footage from the headquarters' security cameras it had helped build.⁸¹ The case illustrates the difficulty of preventing cyber-espionage attempts of a determined state actor, particularly one that is responsible for supplying critical ICT infrastructure.

Going forward, increasing surveillance and espionage capabilities of states, criminal networks and armed groups in Africa are likely to be equally, if not more, important for security outcomes than those of external actors. This growth is being driven by the rapid diffusion of cheap digital surveillance technologies.

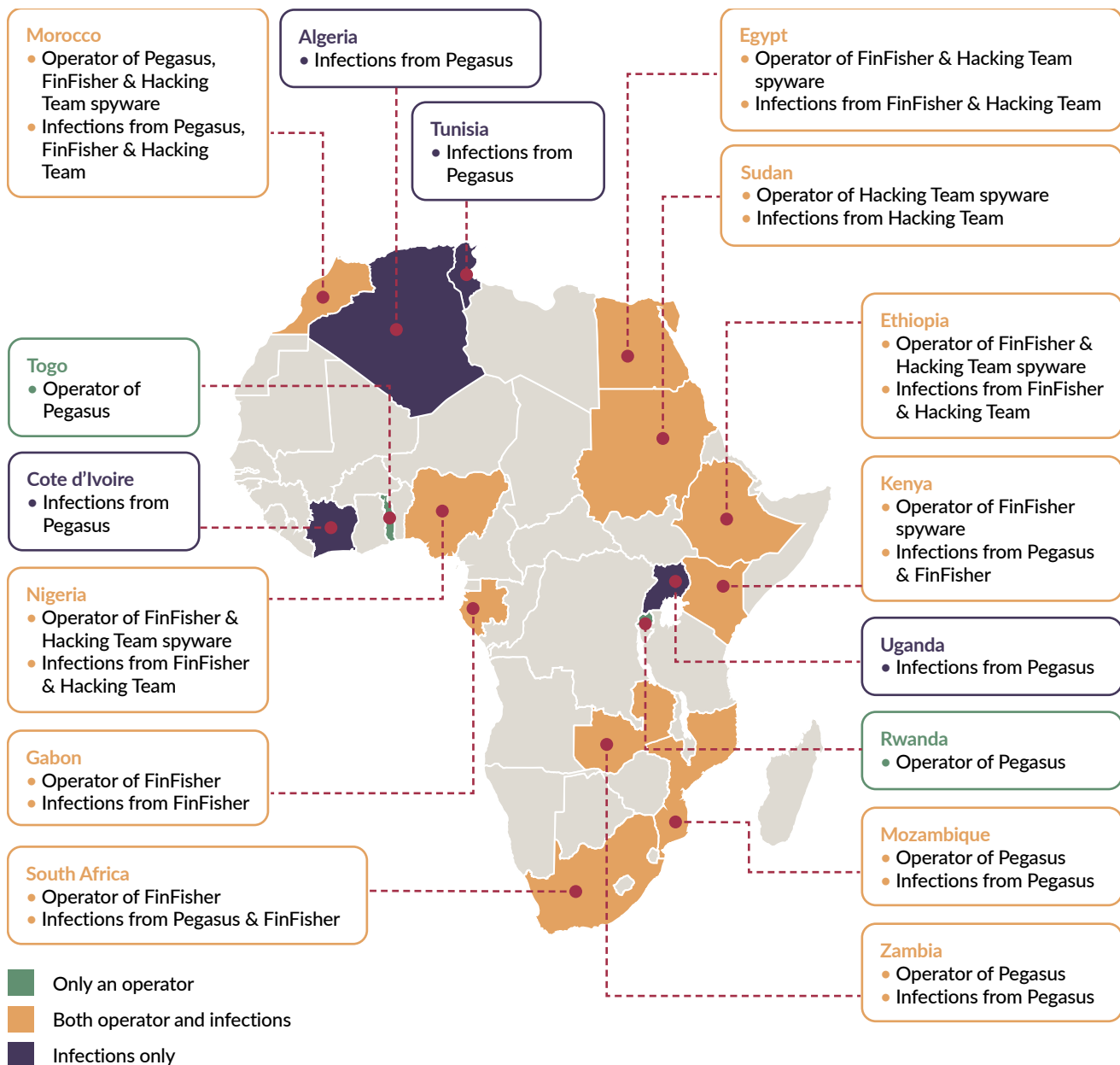


FIGURE 6 Spyware operations in Africa.

SOURCES: Bill Marczak et al, Mapping Hacking Team's 'untraceable' spyware, The Citizen Lab, 14 February 2014, <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware>; Bill Marczak et al, Pay no attention to the server behind the proxy: mapping FinFisher's continuing proliferation, The Citizen Lab, 15 October 2015, <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware>; Bill Marczak et al, Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries, The Citizen Lab, 18 September 2018, <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware>.

Using various forms of spyware, many African states are increasing their espionage and surveillance capabilities. Some suppliers, including Huawei, ZTE and Cloudwalk, are linked to state-based actors such as China, but others including SILAM, NSO Group, BAE Systems and Hacking Team are private companies with less overt affiliations to Western governments in France, Israel, Denmark, Britain and Italy (see Figure 6).⁸² This software is being used for interstate espionage. For example, infections from the NSO Group's Pegasus malware, which allows attackers to compromise mobile phones without any action by the user, have been found in at least 16 African countries to date. The software was used by the governments of Morocco and Rwanda to spy on the heads of state of France and South Africa, respectively.

In part, African states have rushed to embrace telecommunications networks monitoring, internet shutdowns, digital surveillance and biometrics in the name of limiting criminality and preventing attacks by armed groups. Fifteen African countries now possess artificial intelligence enabled surveillance capabilities that draw on technologies like CCTV cameras, facial recognition and advanced algorithms to predict and respond to crime.⁸³ To limit the ability of terrorist groups to use mobile devices to operate, Nigeria has attempted to ensure that all SIM cards in the country are tied to a biometrically backed national identification number.⁸⁴ Other African countries, including Benin, Liberia, Mozambique, Tanzania, Uganda and Zambia, have adopted or are in the process of adopting similar laws.⁸⁵

Despite the rush to adopt these capabilities, there is little to no evidence that information technology has been particularly effective in addressing the threats posed by non-state actors. The success of Nigeria's biometric ID laws has been limited, prompting pushback from those concerned about the exclusion of marginalized groups and lack of adequate privacy, association and freedom of speech protections.⁸⁶ Crime in Nairobi went down immediately following the installation of a Chinese-supplied 'smart' city surveillance system in 2014, but has risen since.⁸⁷

Pegasus malware and the diffusion of cyber-espionage

In July of 2021, the *Washington Post* reported that ‘military grade’ Pegasus spyware, licensed by the Israel-based NSO group, was used to perpetrate human rights abuses and spy on journalists, activists, political leaders and business executives in more than 50 countries. According to the report, up to seven African countries are clients of the NSO Group, with Morocco, Rwanda and Togo among the top users. On a list of 50 000 leaked phone numbers of interest to malware operators, Morocco is reported to have contributed 10 000 of them and Rwanda 3 500.

While the use of Pegasus and other surveillance software to target dissidents, opposition leaders and journalists has received the most press attention, the spyware appears to have been commonly used as a tool of interstate espionage. Some 600 of the 1 000 numbers identified by reporters as having been compromised by Pegasus included ‘politicians and government officials — including cabinet ministers, diplomats, and military and security officers.’⁸⁸ Morocco for example, reportedly installed the spyware on French President Emmanuel Macron’s phone and surveilled him, causing Macron to change his phone after the revelations and call on the Israeli prime minister to investigate the allegations. Rwanda is also reported to have spied on South African President Cyril Ramaphosa. King Mohammed VI of Morocco and the Moroccan prime minister also appear to have themselves been targets of the spyware, raising serious concerns about the degree to which they were informed about how their own security services were employing the malware.


The rapid proliferation of state-owned and -operated surveillance technology in Africa is, in many countries, coming at the cost of democratic freedoms, civil and political liberties and human rights. Authoritarian-leaning African governments now routinely employ a combination of internet shutdowns, mass surveillance tactics and overly broad information security laws to clamp down on dissent during contested elections, protests, or other events that may threaten the regime.⁸⁹ Uganda, for example, reportedly used its network of CCTV cameras to identify and arrest over 800 activists during 2020 anti-government protests.⁹⁰ Democracies are also leveraging surveillance technologies in ways that undermine democratic accountability and transparency. In Mali, a cybercrime bill passed in May 2019 gave defence actors expansive powers to copy private data and intercept in real-time communications of private citizens. According to US Institute of Peace Senior Expert Kamissa Camara, who served as the Minister of Digital Economy in the Malian government deposed by a 2020 coup, such laws ‘can very easily infringe on freedom of expression because the law can be interpreted any way the security sector wants to. Threats are not clearly defined, so anyone who speaks against the government can be tried.’⁹¹

Finally, advances in open-source intelligence (OSINT) – a practice that combines publicly available data from social media accounts, CCTV cameras, satellite imagery and other techniques commonly used by investigative journalists – is beginning to fundamentally transform intelligence collection and analysis. The major pioneer of OSINT is a non-profit organization called Bellingcat, which bills itself as ‘an intelligence agency for the people.’⁹² The capabilities demonstrated by organizations such as Bellingcat rival those of traditional intelligence agencies. Bellingcat has, for example, used open-source intelligence to demonstrate how school children are being used as pawns in Cameroon’s anglophone crisis,⁹³ to document a potential massacre by pro-government Ethiopian forces in the province of Tigray,⁹⁴ to monitor oil spills in South Sudan,⁹⁵ and to track the progress of a 2015 counterinsurgency operation in north-eastern Nigeria.⁹⁶

To date, there has been very little analysis on topics such as the use of advanced surveillance software or open-source intelligence by non-state armed actors operating in Africa. Nevertheless, the reductions in the cost of intelligence-gathering technology means that it is probably only a matter of time before they are used more regularly. Criminal actors and private companies, for example, already serve as middlemen for states and non-state actors in a global malware market worth billions of dollars, selling everything from simple software that cracks passwords to ‘exploit kits’ that include tailored malware payloads and user training.⁹⁷ Though states often have an advantage in that they set ICT regulations, own ICT infrastructure and contract with leading surveillance companies (who often do not work with terrorist organizations or known criminal groups), it is not out of the question that violent extremist groups or organized criminal networks operating in Africa could acquire digital espionage capabilities that rival those of state actors.


The reliance on ICT as a dominant tool of espionage is likely to grow as this technology continues to spread. Actors external to Africa may continue to possess the most sophisticated cyber-espionage capabilities. However, low costs have already driven a significant expansion of the cyber-espionage capabilities of African states. Non-state actors may soon follow.

*Reliance on ICT
as a tool of espionage
is likely to grow
as this technology
continues to spread.*



ARMED CONFLICT INNOVATION

Ugandan officers serving with the African Union Mission in Somalia film preparations for an advance on the Somali town of Buur-Hakba. The digital revolution has influenced many aspects of armed conflict. © Stuart Price/AFP via Getty Images



In the world's most technologically advanced militaries, satellites, remote sensors, telecommunications networks, aircraft and drones are influencing many aspects of armed conflict, from battlefield communications and target selection to the increasingly automated kinetic platforms. The digital revolution has had no less of a significant impact on armed conflict in Africa, where it has shaped the external communications, internal organization and combat operations of armed combatants. As one research study notes, ICT is a crucial 'enabling technology' that is changing the nature of combatants and the character of battlespaces across the continent.⁹⁸

The most widely discussed impact of digitization on armed conflict in Africa is the internet and social media's influence on the external communications, propaganda and recruitment efforts of armed actors. Virtually all of Africa's insurgent groups maintain an externally facing digital presence with the aim of gaining support and recognition. Amadou Kouffa, leader of central Mali's Macina Liberation Front, raised his group's profile by disseminating widely viewed videos on Facebook, WhatsApp and Telegram, calling for an uprising against the Malian armed forces and their international backers.⁹⁹ At a local level, citizen journalists and militia 'war influencers' helped shape discourse about the civil wars in Libya by streaming content directly from the front lines.¹⁰⁰ As far back as 2013, al-Qaeda in the Islamic Maghreb (AQIM) released a video game called 'Muslim Mali' on its website with the aim of recruiting youth. As recounted by Gabriel Weimman, in the game, 'military aircraft carrying AQIM's black flag attack French aircraft in the Sahara' and 'display the message "Congratulations, you have become martyrs!" in lieu of "game over" when a player loses all his/her lives.'¹⁰¹

*ICT is changing
the nature of
combatants and
the character
of battlespaces
across Africa.*

A second area in which digitization is influencing armed actors is with respect to internal organization. Internet-facilitated ‘franchising’ operations, whereby Africa-based militant groups, such as Boko Haram, al-Shabaab or Jama’at Nasr al-Islam wal Muslimin, pledge alliance to internationally recognized groups such as al-Qaeda and the Islamic State, have become the modus operandi for Africa’s largest Islamist militant groups. In each case, local groups retain significant autonomy, and the degree of financial, material and operational ties between the leadership of each entity and its Africa-based affiliates are the subject of contention. What is reasonably clear, however, is that the easy, instantaneous means of communication facilitates the observation and exchange of ideas, tactics and training manuals; allows for the sharing of communications platforms; raises the international profile of the Africa-based groups; and nominally extends the territorial reach of the ‘franchisor’, the international Islamist militant movement.¹⁰²

As ICT has become more widespread, it is becoming used for purposes of command, control and operational planning. Due to ease and accessibility, it is not uncommon for state militaries and insurgent groups to communicate and coordinate with one another through social media messaging apps such as Facebook or Telegram.

Though such apps can be convenient, they can also be a source of risk. For the Somalia-based al-Shabaab, digital communications have been a ‘double-edged sword [...] rendering it vulnerable to lethal security risks’.¹⁰³ Al-Shabaab was a pioneer with respect to the use of digital technology among Africa’s insurgent groups, widely integrating ICT into its recruitment, financing, international communications and operational planning. Between 2013 and 2014, however, many of the group’s leaders were killed in American drone strikes, which were probably executed by monitoring their mobile devices.¹⁰⁴ In response, al-Shabaab briefly banned internet use throughout its territories.

Telecommunications networks in Somalia have since become objects of contestation, with al-Shabaab targeting state-controlled ICT infrastructure for attack¹⁰⁵ and infiltrating Hormuud, the country’s largest telecommunications provider.¹⁰⁶

EXTERNAL COMMUNICATIONS



Al-Qaeda in the Islamic Maghreb's
'Muslim Mali' video game

INTERNAL ORGANIZATION



State targeting of al-Shabaab
mobile command and control networks

COMBAT OPERATIONS



Drone warfare in Libya

FIGURE 7 Examples of cyber-driven armed conflict innovation in Africa.

Finally, digital technology directly affects combat operations and battlefield tactics through its influence on battlefield surveillance, targeting and automation. Over the past 20 years, improvised explosive devices, many of which are detonated using a cellphone trigger, have become a weapon of choice for insurgent actors in Africa and beyond.

More recently, advanced sensors, digital connectivity and precision strike capabilities have led to a proliferation of drones, or unmanned aerial vehicles. Military drone technology has existed in Africa for some time. What is different about contemporary drone technology is its low cost, ability to loiter above a target of interest for extended periods, as well as the possibility of being retrofitted with advanced sensors and precision strike capabilities.

These factors make it possible for a wide range of actors to acquire and use drones. At least 19 African states have acquired drones for either surveillance or combat purposes (see Figure 8).¹⁰⁷ Armed drones have been used in nine states in North and West Africa alone: Algeria, Chad, Libya, Egypt, Mali, Morocco, Nigeria, Burkina Faso and Somalia.¹⁰⁸ In May 2019, Nigeria became the first sub-Saharan African state to use drones in combat against a terrorist group.¹⁰⁹ In Libya, the Turkish-made Bayraktar TB2 drone, deployed on behalf of the internationally recognized Government of National Accord (GNA), was decisive in shifting the course of the second civil war conflict, overwhelming air defence networks and armour supplied by Russia and the UAE to Khalifa Haftar's Libyan Arab Armed Forces.

The drone war in Libya

The degree to which digital technology is changing the face of modern armed conflict was nowhere more evident than in Libya's second civil war, which began in 2014 and ended in 2020. Ghassan Salamé, the former head of the UN mission in Libya, said that the country was 'possibly the largest drone war theatre' in the world, with hundreds of missions flown by each side.¹¹⁰ Drones were used for 'surveillance, long-range strategic strikes on arms depots and airports, and close-air support to units enmeshed in urban combat,' according to the Global Initiative Against Transnational Organized Crime.¹¹¹

Particularly crucial were mid-tier drones, including the Turkish-supplied Bayraktar TB2 and the Chinese Wing Loong II, supplied by the UAE. Beginning in mid-2018, the Wing Loong helped Haftar's forces dominate the skies around Tripoli, restricting the GNA's military movements.¹¹² The introduction of the TB2, along with more advanced air defence networks supplied by Turkish forces, helped repel the offensive by enabling the GNA to re-establish air superiority. Technical changes boosted the TB2's 'efficiency and reconnaissance capabilities', allowing the drone to loiter just beyond the reach of Russian-supplied air defences.¹¹³

The use of drones by non-state armed actors in Africa is also an area of potential concern (see Figure 8). Unmanned aerial systems appeal to violent non-state actors given that they are 'hard to detect and harder still to shoot down'.¹¹⁴ Commercial off-the-shelf drones can be acquired and weaponized for as little as US\$650,¹¹⁵ a tactic that the Islamic State used to attack coalition forces in Iraq. With African states such as Rwanda, Ghana, Uganda and Nigeria becoming leaders in the deployment of commercial drone technology, it is likely to be only a matter of time before they are weaponized by non-state actors in Africa. Surveillance drones have already been acquired and used by armed groups in Egypt and Algeria, by Boko Haram in Nigeria, the Islamic State in the Greater Sahara,¹¹⁶ and al-Shabaab, which used drone footage as propaganda in its attack on Kenyan and US security forces at Manda Bay.¹¹⁷

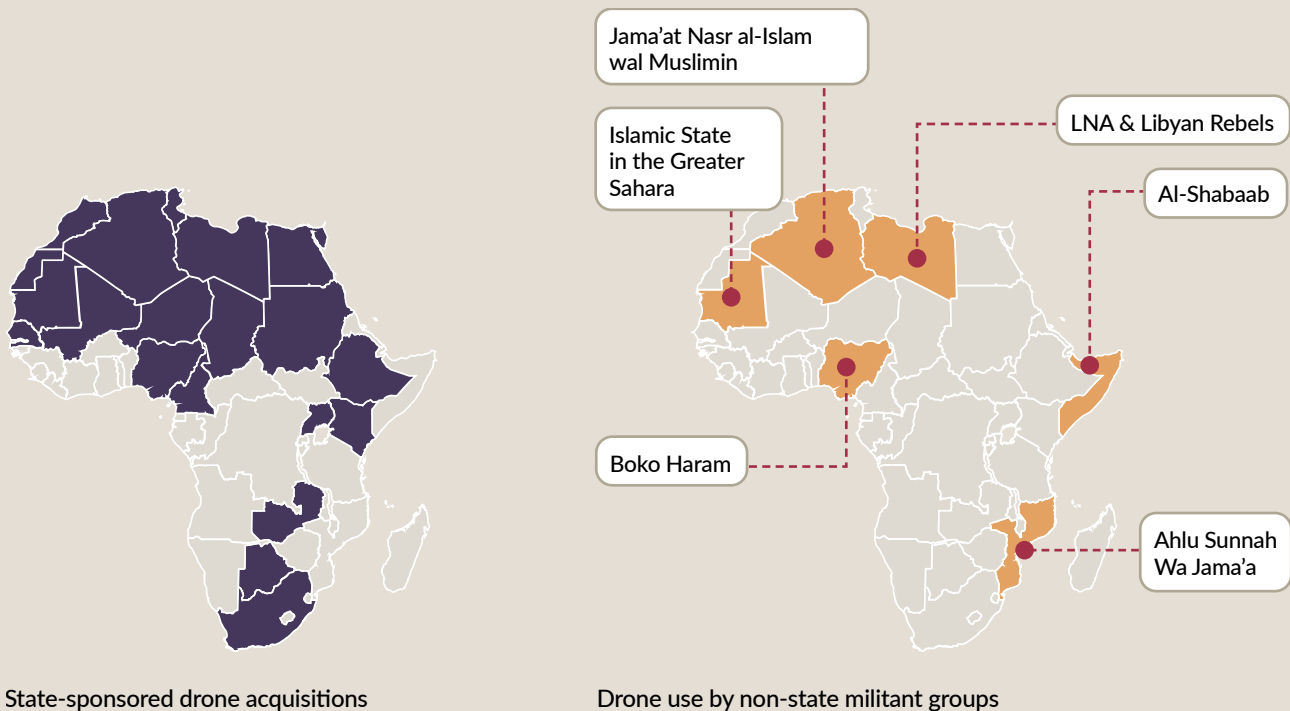


FIGURE 8 Drone proliferation in Africa.

SOURCES: Richtsje Kurpershoek, Alejandra Muñoz Valdez and Wim Zwijnenburg, Remote horizons: Expanding use and proliferation of military drones in Africa, Pax for Peace, February 2021, https://paxforpeace.nl/media/download/PAX_remote_horizons_FIN_lowres.pdf; Erwam de Chasey, Africa in the drone zone, African Aerospace Online News Service, 25 November 2019, <https://www.africanaerospace.aero/africa-in-the-drone-zone.html>; Dan Gettinger, The drone databook, Center for the Study of Drone at Bard College, 2019, <https://dronecenter.bard.edu/projects/drone-proliferation/databook>. Information on use of drones by non-state militant groups drawn from various news sources.

Thus, the implications of the digital revolution for armed conflict in Africa extend beyond the use of social media for propaganda purposes. Digital technologies have become integrated into the internal communications, organization and tactics of armed groups everywhere. Over the long term, digitization is likely to have as significant an impact on warfare as the gun or horse-mounted cavalry did. In the near term, the proliferation of unmanned systems in Africa signals the continuance of a broader trend towards reliance on digitized, automated systems in armed conflict.¹¹⁸



STATE AND SECURITY SECTOR RESPONSES

Control room of the African Union Mechanism for Police Cooperation (AFRIPOL), an organization created for better coordination among African police bodies.

© Andia/Universal Images Group via Getty Images



African nations face four key challenges in responding to the threats outlined above. First, Africa faces a deficit in cybersecurity knowledge and capacity. The most comprehensive data available comes from a 2017 report by the cybersecurity firm Serianu, which found that virtually all cybersecurity incidents go unresolved or unreported.¹¹⁹ Another study of cybersecurity awareness in six African countries found that, in most, 'the need for awareness of cybersecurity threats and vulnerabilities is not recognized, or is only at initial stages of discussion'.¹²⁰ According to Moctar Yedaly, former head of the AU's Information Society Department, many of the most strategically significant threats 'are not detected by [African] institutions themselves, but by a third party that notices the activity'.¹²¹

This lack of awareness is due in part to a dearth of digital skills and expertise: by 2030, over 230 million jobs in sub-Saharan Africa will require digital skills, with demand significantly exceeding supply.¹²² African cybersecurity experts have emphasized the need to build basic cyber-awareness and resilience, stating that capacity building should 'be the foundation of digital transformation and be tailored to the importance of the threat'.¹²³

Secondly, most African governments are behind the curve when it comes to the establishment of foundational cybersecurity policies. Only 18 out of 54 countries in Africa have completed national cybersecurity strategies, which are necessary to define the scale and scope of a country's cyber-related challenges, assign government-wide responsibilities for threat monitoring and response, and direct external support.¹²⁴ Only 22 African countries have national computer incident response teams (CIRTs) – groups of key stakeholders and experts who keep track of major threats and help countries recover from significant security incidents (see Figure 9). Challenges exist even for Africa's more cyber-mature countries, many of whose strategies are not updated regularly and often lack important elements such as threat assessments or dedicated resource allocations.¹²⁵

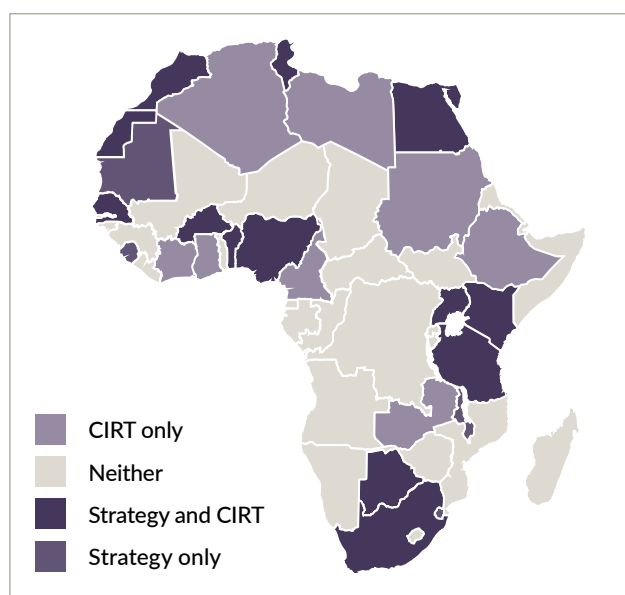


FIGURE 9 Computer incident response and cyber-strategy adoption in Africa.

SOURCE: Information Technology Union Global Cybersecurity Index, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.

Thirdly, there are significant obstacles to regional and international cyber-cooperation in Africa. Cybersecurity challenges in Africa and elsewhere cut across borders, and require the sharing of threat information, legal harmonization, and the capacity to extradite and prosecute criminals. The continent would also benefit from more consistent diplomatic engagement on issues such as norms of interstate behaviour in cyberspace and the use of lethal autonomous weapons. Only 15 African countries have ratified either one or both of the two existing major treaties that would do much to further international and regional cybersecurity cooperation: the Budapest Convention on Cybercrime¹²⁶ and the African Union Malabo Convention (see Figure 10).¹²⁷ Much of the cooperation that does exist appears to occur informally, as a result of contact between officials at regional forums hosted by organizations such as the UN Office on Drugs and Crime (UNODC) or AFRIPOL.¹²⁸

	RATIFIED BUDAPEST	RATIFIED MALABO	RATIFIED BOTH
Countries	Morocco Nigeria	Angola Congo Guinea Mozambique Namibia Niger Rwanda Togo Zambia	Cape Verde Ghana Mauritius Senegal
Total	2	9	4
Total ratifying countries	15		
Non- ratifying countries	39		

FIGURE 10 Adoption status of Malabo and Budapest conventions.

SOURCE: African Union (<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>) and Council of Europe (<https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#>).

Finally, perhaps the biggest challenge concerns the question of how to address the role of the African security sector in managing the downsides of Africa's digital revolution. There is a clear need for security sector actors to do more to address cyber-threats. However, they must recognize, in the words of AU Cyber Security Expert Group Chair Abdul Hakeem Ajijola, that if security sector actors mainly use technology as a means of surveillance and repression, they risk doing more harm than good.¹²⁹

Security sector leaders in Africa often lack basic understanding of the intersection between digital and national security. Cyber-threats are often viewed as issues to be addressed by software engineers or public affairs officers rather than state security officials. Narrowly, this has meant that the incorporation of information, communications and related technologies by African security forces into military strategies, operational plans and tactics are at a nascent stage. It has also meant poor and infrequent communication between information technology divisions and peace and security divisions of regional organizations like ECOWAS and the AU. This is unfortunate, because regional organizations could help develop threat monitoring guidance and coordinate regional responses on issues such as how African governments might respond to cyberattacks by external actors.

Which agencies are represented and who takes the lead is being determined more by political priorities, bureaucratic infighting and the relative influence of civilian, military and outside actors, and not necessarily by what is needed for governments to formulate and execute sound cyber-policy. Even in countries with robust cybersecurity policy frameworks, security sector actors have taken on vastly different roles. In Kenya, Ghana 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. Rwanda's National Cyber Security Agency is a part of the Office of the President of the Republic and oversees all other government agencies and ministries responsible for cyber-policy. Ajijola maintains that 'security sector actors should have a central role, but not exclusive role in cybersecurity policy and strategy development', and recognize that in many instances 'technical staff in a telecom or a service provider might be much more cost effective at identifying, addressing and resolving cybersecurity threats'.¹³⁰


Moreover, the concerns of civil society organizations are rarely taken into account when shaping cybersecurity policy and strategy. This is a grave oversight given that the main goal of cybersecurity policy should be to benefit the end users. The role of organizations such as Kenya's ICT Action Network provides a model for the part that civil society can play in shaping national ICT policy and strategy.

It is not that security sector actors should have no role in managing Africa's rising and diversifying array of cyber-threats. The growing spread of cyberspace and the increasing influence of emerging technology on virtually all aspects of daily life demands they must. But it is also important that the policy responses security sector officials support are clearly rooted in multi-stakeholder cooperation, follow the rule of law and respect citizen security. To address the continent's cyber-threats effectively, the government response must follow sound and established security sector governance principles.

A person is shown from the side, working at a computer. The image is overlaid with a complex network of glowing blue and orange digital circuit lines and icons, including stylized computer monitors and data flow symbols. The background is a blurred office setting.

CONCLUSION AND RECOMMENDATIONS

Internet was partially restored in Uganda on 18 January 2021 after a near-total blackout was imposed ahead of the country's elections. © Badru Katumba/AFP via Getty Images



In a continent where many citizens face real threats to their safety and security, it is tempting to overlook the cyber-domain. For many African citizens, the internet is an unaffordable luxury. For many African civil servants, cyber-threats are best left to the technical experts. After all, the thinking goes, damage to computer networks rarely results in loss of life. It is not possible to grow food, build roads or manufacture bullets using only pixels on a screen.

Nevertheless, as this report has shown, 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. These threats – from organized crime, critical infrastructure sabotage, espionage and armed conflict innovation – show few signs of abating. Indeed, they may accelerate as Africa continues to digitize; as existing digital technologies become increasingly integrated into the functioning of society; and as new technologies, such as artificial intelligence and quantum computing, mature. Over the long term, the impact of the digital revolution on African peace and security is likely to be every bit as significant as technological developments such as steam power, the firearm or the combustion engine.

African governments, citizens 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. It is, after all, impossible to take full advantage of information technology without basic literacy or access to a reliable power source.

Information technology is particularly crucial in part because, as an enabling technology, it has the capacity to fundamentally reshape the social contract between the state and its citizens. If African countries do not invest in information technology in a way that upholds this contract, the net effect of technology will be destabilizing.

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.

Recommendations for governments

National governments should focus on the following five areas:

- 1.** Raise national awareness of cyber-risks, challenges and threats. To respond effectively to cyber-threats, it is essential that these be defined and understood by all relevant stakeholders, from high-level government officials to civilians. Governments on the continent can raise awareness by:
 - Providing training to government officials to ensure basic awareness of key cybersecurity risks and cyber-hygiene. Many training courses are available online and at little to no cost. Countries in Africa with greater levels of cyber-maturity and risk should consider making such training courses mandatory and tailoring training courses to the specific cyber-threat environment in each sector.
 - Improving public and private sector capacity to monitor, share and publish information about key cyber-related threats and threat actors. State cybersecurity agencies should collect and publish information about national cybersecurity threats and attacks. Agencies should share relevant threat information with firms working in vulnerable sectors and require companies to disclose major cybersecurity incidents.
- 2.** Adopt, implement and update inclusive, multi-stakeholder national cybersecurity policies and strategies. National cybersecurity strategies are essential to assigning government-wide roles and responsibilities, and ensuring effective interagency cooperation. However, many do not follow established good practices. To maximize impact, governments drafting national cybersecurity policies and strategies should:
 - Ensure adequate political buy-in and financial support. To ensure effective interagency coordination and implementation, the strategy development process should have a fixed budget. High-level political buy-in is also needed to ensure a clear division of responsibility.

- Include a threat assessment, a clear specification of the strategy's key objectives and goals, the lines of effort intended to accomplish those goals, a specification of agencies and departments responsible, and a dedicated budget for implementation. The exact content of the strategy can vary but should, at a minimum, include an assessment of a country's cyber-threat landscape and the key goals and objectives that the government seeks to achieve through the adoption of a cybersecurity strategy, along with a division of tasks between various agencies and government entities responsible for the policy's implementation and allocation of resources to ensure that stakeholders are able to execute the strategy.
 - Include a broad range of government, security sector, private sector and academia/civil society stakeholders. The strategy should not be drafted by external actors or consultants, but by representatives from the key government agencies responsible for its implementation, in coordination and consultation with civil society and private sector stakeholders. A wide range of government, civil society and private sector stakeholders should inform every stage of the cybersecurity strategy development process. This includes the process of gathering basic inputs to the strategy, drafting, approval and implementation.
 - Be widely publicized and routinely updated. The effectiveness of a strategy depends on the document being read, internalized and acted upon. It is therefore essential to ensure the strategy is widely publicized. Strategy documents should also be routinely updated to ensure that they evolve along with the threats.
3. Protect critical information infrastructure. As Africa digitizes, governments and businesses have a unique opportunity to limit cyber-risks by ensuring national critical infrastructure is protected by the latest technologies and standards. Protecting critical information infrastructure requires efforts to define and identify it, prioritize the protection of vulnerable systems and create technical bodies, like computer incident response teams, to ensure resilience and recovery in the case of an attack. Therefore, governments should:
- Define critical information infrastructure in a manner consistent with local realities. States should define cyber-dependent critical information infrastructure in a manner consistent with their level of cyber-maturity and vulnerability. At a minimum, this categorization should include systems in the government, military, telecommunications, finance and transport sectors. It may also include other sectors critical to the economy and national security, such as agriculture, extraction or manufacturing.
 - Take a risk-based approach to national cyber-incident management and critical infrastructure protection. Cyber-risk measured at the national level will help states prioritize and direct scarce resources to secure those systems most critical to the state.

Some of the continent's biggest critical infrastructure vulnerabilities stem from the existence of single points of failure and reliance on external actors.

- Integrate cybersecurity emergency response with the rest of the nation's emergency response strategy and policy. The biggest cyber-risks to critical infrastructure remain physical in nature, resulting from the disablement or sabotage of critical systems and networks. Responses to these risks need to be incorporated into broader efforts to protect and recover from the loss of critical national infrastructure.
 - Prioritize the creation of national and sector-level computer incident response teams. CIRTs are groups of technical experts charged with monitoring threats and helping organizations recover from major cyberattacks. The African continent has made significant progress in recent years in establishing national CIRTs. Governments without a national CIRT should prioritize establishing one. Governments with national CIRTs should establish sectoral CIRTs covering the most vulnerable sectors and work together to support the establishment of regional and continent CIRTs.
 - Encourage competition and innovation in the critical infrastructure supply chain. Some of the continent's biggest critical infrastructure vulnerabilities stem from the existence of single points of failure and reliance on external actors who possess near monopolies on the provision of ICT infrastructure. Governments should prioritize the protection of the continent's most vulnerable power networks, ports and internet access points, diversify the suppliers of key technology infrastructure and, where possible, encourage the development of African enterprises capable of supplying, maintaining and protecting critical information infrastructure.
4. Adopt legislation to combat cybercrime and protect personal data that prioritizes government transparency and human rights. African governments have made laudable progress in their efforts to pass laws that protect personal data, respond to cybercrime and establish key national cybersecurity institutions and bodies. However, it is essential that these laws respect human rights and political liberties. Cybercrime laws and legislation in Africa should:
- Guarantee the protection of personal data. Government or security sector authorities should not have access to the personal data and communications of citizens without respect for due process or oversight from other branches of government.
 - Define terms such as 'hate speech', 'disinformation' and 'cyber-terrorism'. Often, such terms are vaguely defined and provide governments with powers that allow for arbitrary access to personal information and lead to detentions and arrests of peaceful dissidents and opposition figures. To be considered for law enforcement action, the use of the internet by dissident groups should be clearly identified as intending to provoke violence.
 - Consider de-platforming violent extremist groups and organized criminal networks on social media. A simple and effective approach to the use of the internet by violent extremist groups and other organized criminal networks is for government actors to work with technology companies to remove accounts and posts that advocate or facilitate violence. More punitive measures, such as criminalizing content, fines and arrests can create incentives for government overreach and disincentivize service providers from reporting incidents to authorities.

5. Improve international cooperation and engagement. Cyber-threat actors are not easily bound by physical borders. Addressing the challenges they pose requires African governments to work to improve international cooperation by:
 - Supporting regional and international efforts to monitor and respond to organized cybercrime. States need to adopt policies, procedures and treaties that allow them to collect and share digital evidence and extradite cybercriminals. Both the Budapest and Malabo conventions offer African countries avenues for responding to organized cybercrime in a manner consistent with respect for the rule of law and human rights.
 - Investing in cyber-diplomacy. African states need more active diplomatic engagement at major regional and international technology institutions. It is in the interest of African countries to foster international norms that discourage destabilizing uses of emerging technologies. To date, however, most African nations have played a limited role in these debates.
 - Sharing intelligence about key threats and threat actors. Zero-day vulnerabilities are more likely to be first exploited and reported in more technologically advanced countries. International cooperation and engagement will give the continent a chance to learn and respond to these threats.

Recommendations for security sector actors

The security sector in Africa has a crucial role to play in addressing the continent's cyber-threats and challenges. However, security sector actors need to align their involvement in cyberspace to ensure respect for citizen security and human rights. Security actors should avoid taking on roles and responsibilities that are best left to other branches of government or the private sector. Specifically, security sector actors should:

1. Increase capacity to collect digital forensic evidence and investigate cyber-enabled organized crime. Organized criminal networks across Africa depend on information technology to conduct their operations and African law enforcement needs digital tools to respond. Cybercrime units across Africa need expanded capacity, better reporting channels and clearer guidelines to ensure that digital evidence is collected and acted upon in an effective way.
2. Focus on defence of military and government information systems from external threats. African security forces should secure sensitive government and military communications networks. This will require adopting standard good practices from the private sector, such as two-factor authentication for government systems and layered network defences.
3. Play a convening and coordinating role in the protection of other key critical information infrastructure. The primary responsibility for network defence, resilience and recovery in key sectors, such as telecommunications, finance and energy, should rest with the private sector. However, the security sector should ensure that private actors are aware of major threats and work with companies to promote threat readiness.

4. Advocate for the adoption of cybersecurity laws and practices consistent with the rule of law. Since security forces are more likely to use and be used by political elites to collect citizens' personal information, it is incumbent on the security sector to insist that they collect and use personal information in a manner that does not infringe upon human rights and the rule of law. It is not in the interest of citizens, security forces or, ultimately, of political stability for information technology to be used as a means of political repression.
5. Adapt information technology into military strategies, tactics and combat doctrine. African security forces should adapt information technology into

their strategies, doctrine and combat operations, but do not necessarily need to use Western doctrine as a model. Rather, leaders should embrace limited technology dependence as a potential strategic advantage and acquire cheap, durable and secure technologies from multiple public and private sector suppliers. African security force institutions might, for example, make use of commercial off-the-shelf drones, buy their own cubic satellites or leverage commercially available satellite imagery, and use open-source-intelligence methods instead of acquiring higher-end drones or satellite-based intelligence from external actors.

Recommendations for regional organizations

To better help African countries foster consensus, share good practices and coordinate efforts to address cyber-related threats, regional organizations should:

1. Support the creation of regional and continental computer security incident response teams. A regional- or continental-level CSIRT could help African nations monitor and share information about external cyber-threats, improve multi-national response and recovery efforts, and support the development and growth of national and sectoral CSIRTs across Africa. An existing organization, AfricaCERT, is poised, with additional resources and expertise from regional and international organizations, to lead such efforts.
2. Improve coordination between security-focused and technology-focused divisions and directorates. Regional organizations, like the AU, should create peace, security and emerging technology programmes that are managed by or include the active participation of peace, security and political directorates. These programmes should focus on

managing cyber-threats from organized criminal networks and extremist groups, adapting emerging technology into regional peace operations and national security strategies, and increasing African engagement at the UN and other regional organizations.

3. Build a database of good practices and provide opportunities for African countries to share and disseminate good practices in responding to cyber-threats. African countries have received significant technical assistance and expertise from abroad in developing national cybersecurity capacity. However, with eight African countries among the top 51 countries of the UN Information Technology Union's cybersecurity commitment index, there are many internal lessons to be shared as well. Regional organizations are in an excellent position to provide Africa's more cyber-mature countries with a chance to learn from one another and inform the rest of the continent.

Recommendations for external actors

External actors will continue to play a major role in helping African governments and their citizens manage the downsides of the digital revolution. They should focus education, training and capacity building efforts on supporting existing initiatives and ensuring that the sale of sensitive surveillance technologies is not used to violate human rights and civil liberties. Specifically, external actors should:

- 1.** Provide educational opportunities and training for African cybersecurity and information technology professionals. Government, security sector and private sector workforces in Africa would benefit from a combination of basic digital literacy and more advanced training in cybersecurity. External actors should work with African governments and industry to provide such training at minimal cost, through study-abroad programmes or online certification courses.
- 2.** Invest in local efforts to build cyber-capacity. There are multiple, ongoing efforts at the national, regional and local levels aimed at building cyber-capacity. These include: the African Union Cybersecurity Expert Group, the Global Forum on Cyber Expertise, AfricaCERT and the Region Internet Registry for Africa. External actors should seek to invest and work through African-led, -managed and -run initiatives, particularly when they are seeking to build capacity and improve threat monitoring and information sharing across multiple countries.
- 3.** Limit the sale of sensitive surveillance technologies to regimes with a track record of human rights abuses. External actors should avoid selling sophisticated surveillance technologies to African countries with poor human rights records. Global governments should take action to limit the sale of such technologies by the private sector. External actors should invest more in efforts to build cyber-capacity and engage with security sectors in regimes with robust legal and policy frameworks that protect personal data and restrict the use of information technology for repressive purposes.

Recommendations for the private sector

Businesses in Africa have a responsibility to ensure a baseline level of cybersecurity of critical information infrastructure in sectors they tend to be responsible for. Even in the absence of government intervention, businesses can play a positive role in defending businesses and countries against strategic-level cyber-threats by:

- 1.** Ensuring the protection of critical information infrastructure. In countries that have clear critical information infrastructure protection policies and standards, businesses should align their definition of critical infrastructure with that of the government. In countries where critical infrastructure has yet to be defined, businesses should use international standards and good practices.
- 2.** Provide security as a service to small and medium enterprises. Large businesses and service providers should consider providing cybersecurity to small and medium enterprises, given that they often cannot afford to purchase their own dedicated cyber-defence systems.

3. Assess and grow a cybersecurity workforce. Many African enterprises lack basic awareness of their cyber-related vulnerabilities and threats, and cannot assess whether they need cybersecurity skills. This must change. As a first step, businesses need to assess whether cybersecurity skill shortages exist within their organizations and industries.

Recommendations for civil society

Civil society organizations (CSOs) are crucial to raising awareness about the broader social impact of cybersecurity policies and in ensuring that national efforts to address cyber-threats are compliant with human rights. Civil society's deep involvement in virtually all aspects of cybersecurity policy is essential to build trust between citizen, government and security sector stakeholders. Civil society actors should:

1. Support national cybersecurity efforts through research and guidance. CSOs, including think tanks, advocacy groups, the media and academia, have a crucial role to play in informing government policy through evidence-based research and public advocacy. Local CSO engagement is essential to ensure that cybersecurity policies are informed by local context and do not lead to unintended consequences.
2. Monitor the implementation of the government's cybersecurity policies, thereby providing accountability and public oversight. CSOs have an essential role to play in ensuring governments uphold the rule of law and are accountable to citizens. This accountability is essential in ensuring governments receive independent feedback and revisit policies that do not work.
3. Play a convening role to increase awareness about cybersecurity and conduct informed debates about sensitive ICT policy issues. CSOs play a crucial and under-recognized role in convening stakeholders from government, the security sector, the private sector and other CSOs to discuss and debate sensitive ICT issues. This convening role is essential to build trust and foster dialogue among all ICT stakeholders.

NOTES

- 1 Zecharias Zelalem, An Egyptian cyber attack on Ethiopia by hackers is the latest strike over the Grand Dam, Quartz Africa, 27 June 2020, <https://qz.com/africa/1874343/egypt-cyber-attack-on-ethiopia-is-strike-over-the-grand-dam/>.
- 2 Nathaniel Allen and Noelle van der Waag-Cowling, How African countries can tackle state-sponsored cyber threats, Brookings: Techstream, 15 July 2021, <https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/>.
- 3 Matthieu Olivier, Surveillance: The ultra-secure phones of Africa's presidents, The Africa Report, 3 February 2021, <https://www.theafricareport.com/22861/surveillance-the-ultra-secure-phones-of-africas-presidents/>.
- 4 UNODC, Module 1: Definitions of organized crime, defining organized crime, April 2018, <https://www.unodc.org/e4j/en/organized-crime/module-1/key-issues/defining-organized-crime.html>.
- 5 Makoma Makhopa et al, Cyber-attack cripples operations at the Port of Durban for the second time in a month, Foreign Agricultural Service, 13 August 2021, <https://www.fas.usda.gov/data/south-africa-cyber-attack-cripples-operations-port-durban-second-time-month>.
- 6 Nathaniel Allen and Matthew La Lime, How digital espionage tools exacerbate authoritarianism across Africa, Brookings: TechStream, 19 November 2021, <https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/>.
- 7 DCAF: Geneva Center for Security Sector Governance, Guide to good governance in cybersecurity, January 2021, https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021.pdf, p 27.
- 8 Some analysts refer to an emerging 'fourth industrial revolution' resulting from the convergence of digital technology with breakthroughs in material science and biology. See Klaus Schwab, *The Fourth Industrial Revolution*, New York: Currency, 2017; Njuguna Ndung'u and Landry Signé, The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse, Brookings: Foresight Africa, 8 January 2020, <https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/>.
- 9 Center for Internet Security, Election security spotlight—CIA triad, 2020, <https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/>.
- 10 Serianu, Africa Cyber Security Report 2017: Demystifying Africa's cyber security poverty line, 2017, <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>; PWC, Global Economic Crime and Fraud Survey: Pulling fraud out of the shadows, 13 April 2018, https://www.slideshare.net/Paperjam_redaction/global-economic-crime-and-fraude-survey-2018; Kayode Yusuf, Africa is leaving itself dangerously exposed to cyber-attacks, ACCA, 1 February 2019, <https://www.accaglobal.com/my/en/member/member/accounting-business/2019/02/insights/cyber-attacks.html>.
- 11 Merriam-Webster, Cybercrime, <https://www.merriam-webster.com/dictionary/cybercrime>.
- 12 Mike McGuire and Samantha Dowling, Cyber crime: A review of the evidence, Research Report 75, Home Office, 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf.
- 13 Gabon attacked by Anonymous, *IAfrikan*, 29 October 2018, <https://www.iafrikan.com/2018/10/29/gabon-websites-government-hacked-ddos-defaced/>.
- 14 Warwick Ashford, African bank foils suspected North Korean cyber attack, *ComputerWeekly.com*, 9 August 2019, <https://www.computerweekly.com/news/252467937/African-bank-foils-suspected-North-Korean-cyber-attack>.
- 15 United States of America vs. Park Jin Hyok, also known as ('aka') 'Jin Hyok Park,' aka 'Pak Jin Hek,' Criminal Complaint, United States District Court for the Central District of California, 8 June 2018.
- 16 See for instance: Youssef Igrouane, Moroccan police set up laboratories to fight sextortion, *Morocco World News*, 25 February 2017, <https://www.moroccoworldnews.com/2017/02/209454/moroccan-police-set-five-laboratories-fight-sex-tortion>; ENCA, Sextortion scams on the rise, 3 September 2019, <https://www.enca.com/life/cyber-criminals-blackmail-unsuspecting-victims>; BuinessTech, WhatsApp sextortion scam back on the rise in SA, 13 August 2018, <https://businesstech.co.za/news/mobile/264357/whatsapp-sextortion-scam-back-on-the-rise-in-sa/>; Trésor Kalonji, *La cybercriminalité en RDC en chiffres*, Trésor Kalonji Blog, 24 September 2018, <http://tresorkalonji.pro/2018/09/la-cybercriminalite-en-rdc-en-chiffres.html>; Digital Business Africa, *Sextorsion et chantage à la Webcam: la triste histoire de la Camerounaise Christelle N.*, 28 April 2016, <https://www.digitalbusiness.africa/chantage-et-arnaque-a-la-webcam-la-triste-histoire-de-la-camerounaise-christelle-n>.

- 17 US Department of Justice, 281 arrested worldwide in coordinated international enforcement operation targeting hundreds of individuals in Business Email Compromise schemes, 10 September 2019, <https://www.justice.gov/opa/pr/281-arrested-worldwidecoordinated-international-enforcement-operation-targeting-hundreds>; Crowdstrike, Intelligence Report: Nigerian confraternities emerge as Business Email Compromise threat, 3 May 2018, <https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf>.
- 18 Peter Renals, SilverTerrier: 2019 Nigerian Business Email Compromise update, Unit 42: Palo Alto Networks, 31 March 2020, <https://unit42.paloaltonetworks.com/silverterrier-2019-update/>; Peter Renals, SilverTerrier: The rise of Nigerian Business Email compromise, Palo Alto Networks, 18 May 2020, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise.
- 19 ENACT, Online African organized crime from surface to dark web, INTERPOL, July 2020, <https://www.interpol.int/en/content/download/15525/file/Online%20African%20Organized%20Crime%20from%20Surface%20to%20Darkweb-17.08.2020.pdf>.
- 20 Crowdstrike, Intelligence report: Nigerian confraternities emerge as business email compromise threat, 20 March 2018, <https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf>.
- 21 CTI Team, Understanding the adversaries: The Forkbombo group, OnNet, 2 April 2019, <http://blog.onnetservices.io/?p=20>.
- 22 CTI Team, Loan Wipers–The Grapzone threat group, OnNet, 20 August 2019, <https://blog.onnetservices.io/?p=220>.
- 23 CTI Team, SilentCards threat group expands around East and Central Africa with an offshoot group born due to internal rivalry, OnNet, 10 October 2019, <http://blog.onnetservices.io/?p=279>.
- 24 Sammy Darko, Inside the world of Ghana's internet fraudsters, BBC News, 10 May 2015, <https://www.bbc.com/news/world-africa-32583161>.
- 25 Abhishek Kumar Jha, An interview with hacker group Anonghost, from the world of Anonymous hacking, Techworm, 30 July 2020, <https://www.techworm.net/2013/06/an-interview-with-hacker-group.html>.
- 26 Lily Hay Newman, The Nigerian fraudsters ripping off the unemployment system, *Wired*, 19 May 2020, <https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>; Brian Krebs, U.S. Secret Service: 'Massive fraud' against state unemployment insurance programs, KrebsonSecurity, 16 May 2020, <https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/>.
- 27 Unit 42, Infographic: Overview of BEC schemes, Palo Alto Networks, 15 October 2019, <https://www.paloaltonetworks.com/resources/infographics/overview-of-bec-schemes>.
- 28 Federal Bureau of Investigation, Business email compromise: The \$43 billion scam, Alert# I-050422-PSA, 4 May 2022, <https://www.ic3.gov/Media/Y2022/PSA220504>.
- 29 UNODC, Transnational organized crime: the globalized illegal economy, 2022, <https://www.unodc.org/toc/en/crimes/organized-crime.html>.
- 30 Federal Bureau of Investigation, Internet crime report, 2019, https://pdf.ic3.gov/2019_IC3Report.pdf.
- 31 Brian Krebs, U.S. Secret Service: 'Massive fraud' against state unemployment insurance programs, KrebsonSecurity, 16 May 2020, <https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/>.
- 32 Peter Renals, SilverTerrier: 2019 Nigerian Business Email Compromise Update, Unit 42: Palo Alto Networks, 31 March 2020, <https://unit42.paloaltonetworks.com/silverterrier-2019-update/>.
- 33 U. Kadri, 'Inside the world of 'Apprentice Yahoo Boys', *The Moment*, 24 February 2019, <https://themomentng.com/index.php/2019/02/24/inside-theworld-of-apprentice-yahoo-boys/>.
- 34 ENACT, Online African organized crime from surface to dark web, INTERPOL, July 2020, <https://www.interpol.int/en/content/download/15525/file/Online%20African%20Organized%20Crime%20from%20Surface%20to%20Darkweb-17.08.2020.pdf>.
- 35 Chris Walters, Africa steps up fight against counterfeits, Managing Intellectual Property, March 2017, <https://spoor.com/docs/4549/Feature%20Africa.pdf>; ENACT, Strategic assessment: Overview of serious and organized crime in Africa, INTERPOL, 2018.
- 36 Paul Ramara, South Africa: High online counterfeit goods risk, says survey, Mondaq, 22 January 2019, <https://www.mondaq.com/southafrica/dodd-frank-consumer-protection-act/773528/high-online-counterfeit-goods-risk-says-survey>.
- 37 Today, the main online platforms for coordinating the illicit wildlife trade are Facebook, Instagram, WhatsApp and Twitter, with goods being sold on e-commerce platforms such as Jiji.ng and Nairaland.
- 38 Important trades include ivory, rhinoceros' horn and pangolin scales sold mostly to customers living in Asia.
- 39 ENACT, Mobile money and organized crime in Africa, INTERPOL, June 2020, <https://www.interpol.int/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf>, pp 39-40; ENACT, Online African organized crime from surface to dark web, INTERPOL, July 2020, <https://www.interpol.int/en/content/download/15525/file/Online%20African%20Organized%20Crime%20from%20Surface%20to%20Darkweb-17.08.2020.pdf>.
- 40 O. Pinnell and J. Kelly, Slave markets found on Instagram and other apps, BBC News, 31 October 2019, <https://www.bbc.com/news/technology-50228549>; M. Vidal, 'Discounted maids!': How ads trap women in modern-day slavery in Jordan, *The World*, 14 June 2019, <https://www.pri.org/stories/2019-06-14/maids-sale-how-ads-trap-women-modern-day-slavery-jordan>.

- 41 Centre Français de Recherche sur le Renseignement, *Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée*, <https://cf2r.org/travailler-dans-le-renseignement/au-service-de-letat/ministere-de-linterieur/service-dinformation-de-renseignement-et-danalyse-strategique-sur-la-criminalite-organisee-sirasco/>; Sertan Sanderson, More Ivorian women smuggled into slavery and sexual abuse, Infomigrants, 21 October 2019, <https://www.infomigrants.net/en/post/20273/more-ivorian-women-smuggled-into-slavery-and-sexual-abuse>.
- 42 Frontex, Western Mediterranean route: Frontex in Spain, European Union, 2018, <https://frontex.europa.eu/we-know/migratory-routes/western-mediterranean-route/>.
- 43 ENACT, Analytical report: overview of serious and organized crime in Africa, INTERPOL, 28 October 2018, <https://enact-africa.s3.amazonaws.com/site/uploads/2018-12-12-interpol-continental-001.pdf>.
- 44 Pavritha Rao, Africa could be the next frontier for cryptocurrency, *Africa Renewal*, April–July 2018, <https://www.un.org/africarenewal/magazine/april-2018-july-2018/africa-could-be-next-frontier-cryptocurrency>.
- 45 Chainalysis, P2P platforms, remittances, and savings needs power Africa's grassroots cryptocurrency adoption, 14 October 2021, <https://blog.chainalysis.com/reports/africas-grassroots-cryptocurrency-adoption/>.
- 46 KuCoin, Into the Cryptoverse report: Nigeria edition 2022, 12 April 2022, <https://www.kucoin.com/blog/kucoin-is-into-the-cryptoverse-report-reveals-35-percent-of-nigerian-adults-are-crypto-investors>.
- 47 Chainalysis, P2P platforms, remittances, and savings needs power Africa's grassroots cryptocurrency adoption, 14 October 2021, <https://blog.chainalysis.com/reports/africas-grassroots-cryptocurrency-adoption/>.
- 48 Ibid.
- 49 Nano B&K, Criminal infiltrating Africa's booming mobile money industry, 12 February 2021, <http://www.nanobnk.com/criminal-infiltrating-africas-booming-mobile-money-industry/>.
- 50 Ibid.
- 51 Quoted in Africa Center for Strategic Studies, Cyber dimensions of transnational organized crime, Webinar series video, 8 July 2021, <https://youtu.be/QgmqfpC8vj8?t=1743>.
- 52 Matt Herbert, Mobile finance and citizen security in East Africa, STATT Synapse No. 9, July 2012.
- 53 Susie Lonie, Fraud risk management for mobile money: An overview, Consult Hyperion and FSDafrica, August 2017, <https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf>.
- 54 ENACT, Mobile money and organized crime in Africa, INTERPOL, June 2020, <https://www.interpol.int/es/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf>.
- 55 Elias Biryabarema, American kidnapped on Ugandan safari, \$500,000 ransom demanded, Reuters, 3 April 2019, <https://www.reuters.com/article/us-uganda-usa-kidnapping-idUSKCN1RF1LU>.
- 56 International SOS, Security Alert: Kenya: Nairobi: Abduction of foreign national underscores HIGH crime risk, 3 February 2020; Capital News, Police officer among 4 kidnappers killed As Chinese national rescued, 29 February 2020, <https://www.capitalfm.co.ke/news/2020/02/police-officer-among-4-kidnappers-killed-as-chinese-national-rescued/>.
- 57 John Collins, Crypto, crime and control: Cryptocurrencies as an enabler of organized crime, GI-TOC, June 2022, <https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-crypto-crime-and-control-cryptocurrencies-as-an-enabler-of-organized-crime.pdf>.
- 58 Katharine Petrich, Cows, charcoal, and cocaine: Al-Shabaab's criminal activities in the Horn of Africa, *Studies in Conflict & Terrorism*, 17 October 2019; FATF, Terrorist financing in West and Central Africa, October 2016, <https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-West-Central-Africa.pdf>.
- 59 ENACT, Mobile money and organized crime in Africa, INTERPOL, June 2020, <https://www.interpol.int/es/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report%20-Mobile%20Money%20in%20Africa%202020.pdf>.
- 60 Joseph S. Nye Jr., Deterrence and dissuasion in cyberspace, *International Security*, 41, 2016/17; National Research Council, *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*, Washington D.C., National Academies Press, 2009.
- 61 Ibid.
- 62 ITU Study Group Q.22/1, Report on best practices for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts, International Telecommunications Union, January 2008, <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>.
- 63 Leandros Maglaras et al, Threats, countermeasures, and attribution of cyberattacks on critical infrastructures, *EAI Endorsed Transactions on Security and Safety*, 5, 2018.
- 64 One particular piece of malware the Russians used, known as NotPetya, was based off a stolen US National Security Agency exploit and is estimated to have resulted in at least US\$10 billion in damages, making it the costliest cyberattack to date. Laurens Cerelus, How Ukraine became a test bed for cyberweapons, Politico, 14 February, 2019, <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks>; Mike McQuade, The untold story of NotPetya, the most devastating cyberattack in history, *Wired*, 22 August 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- 65 Sharon Weinberger, How Israel spoofed Syria's air defense system, *Wired*, 10 April 2007, <https://www.wired.com/2007/10/how-israel-spoof/>.
- 66 Nathaniel Allen and Noëlle van de Waag-Cowling, How African states can tackle state-backed cyber threats, Brookings: Tech Stream, 15 July 2021, <https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/>.

- 67 Erica D. Borghard and Shawn W. Lonergan, Cyber operations as imperfect tools of escalation, *Strategic Studies Quarterly*, 13, 3, 2019, 122-145; Jacquelyn Schneider, The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war, *Journal of Strategic Studies*, 4, 2019; Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Cambridge, MA: Harvard University Press, 2020.
- 68 Yahia Hatem, Algerian media accuse Morocco of hacking state-owned websites, *Morocco World News*, 18 December 2020, <https://www.moroccoworldnews.com/2020/12/329277/algerian-media-accuse-morocco-of-hacking-state-owned-websites>.
- 69 For Cape Verde, see Inforpress, NOSI starts today replacement of suspended services due to cyber attack on the state network, 30 November 2020, <https://inforpress.cv/nosi-starts-today-replacement-of-suspended-services-due-to-cyber-attack-on-the-state-network/>; for Algeria, Yahia Hatem, Algerian media accuse Morocco of hacking state-owned websites, *Morocco World News*, 18 December 2020, <https://www.moroccoworldnews.com/2020/12/329277/algerian-media-accuse-morocco-of-hacking-state-owned-websites>; for Kenya, Africa Tech Digest, Kenyan government website hacked, 5 June 2019, <https://africatechdigest.com/2019/06/05/kenyan-government-website-hacked/>; for Gabon, IAFRIK, Gabon attacked by Anonymous, 29 October 2018, <https://www.iafrikan.com/2018/10/29/gabon-websites-government-hacked-ddos-defaced/>; for Nigeria, Alfred Olufemi, Anonymous attacks CBN website, *Premium Times*, 16 October 2020, <https://www.premiumtimesng.com/news/headlines/421284-updated-endsars-anonymous-attacks-cbn-website.html>; for Ethiopia, see Cyber Horus group case study, and for South Africa, see later in this section.
- 70 Stephen Kafeero, Uganda's banks have been plunged into chaos by a mobile money fraud hack, *Quartz Africa*, 10 October 2020, <https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/>.
- 71 Nathaniel Allen and Noëlle van de Waag-Cowling, How African states can tackle state-backed cyber threats, Brookings: Tech Stream, 15 July 2021, <https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/>.
- 72 The Maritime Executive, Second force majeure at South African ports following cyberattack, 28 July 2021, <https://maritime-executive.com/article/second-force-majeure-at-south-african-ports-following-cyberattack>.
- 73 Felix Njini and Prinesha Naidoo, South Africa port operator declares force majeure over cyber attack, Bloomberg, 27 July 2021, <https://www.bloomberg.com/news/articles/2021-07-27/s-africa-port-operator-declares-force-majeure-over-cyber-attack-krln4ku6>.
- 74 Irma Venter, Unrest, Transnet cyberattack cost BMW SA R200m in lost sales, Creamer Media's Engineering News, 13 August 2021, <https://www.engineeringnews.co.za/article/unrest-transnet-cyberattack-cost-bmw-sa-r200m-in-lost-sales-2021-08-13>.
- 75 Kit Chellel, The hacker who took down a country, Bloomberg, 20 December 2019, <https://www.bloomberg.com/news/features/2019-12-20/spiderman-hacker-daniel-kaye-took-down-liberia-s-internet>.
- 76 Ibid.
- 77 Thomas Rid, Cyber war will not take pace, *Journal of Strategic Studies*, 35, 2012, p 20.
- 78 Andrea Marshall, China's mighty telecom footprint in Africa, New Security Learning, 14 February 2011, <http://www.newsecuritylearning.com/index.php/archive/75-chinas-mighty-telecom-footprint-in-africa>; Daouda Cissé, 'Going global' in growth markets—Chinese investments in telecommunications in Africa, Centre for Chinese Studies at Stellenbosch University, South Africa, April 2012, http://www.ccs.org.za/wp-content/uploads/2012/04/Telecom_Policy-Briefing_final.pdf.
- 79 Ghalia Kadiri and Joan Tilouine, À Addis-Abeba, le siège de l'Union africaine espionné par Pékin, *Le Monde*, 26 January 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.
- 80 Ibid.
- 81 CSIS, Significant cyber incidents, https://csis-website-prod.s3.amazonaws.com/s3fs-public/210708_Significant_Cyber_Events_0.pdf?X14jARKPqPZgya1nQlOkntCQaHp6HzAc.
- 82 Mathieu Olivier, Inside Africa's increasingly lucrative surveillance market, *The Africa Report*, 21 July 2021, <https://www.theafricareport.com/22841/inside-africas-increasingly-lucrative-surveillance-market/>.
- 83 Steven Feldstein, The global expansion of AI surveillance, Carnegie Endowment for International Peace, 19 September 2019, <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>.
- 84 Reuters, UPDATE 1-Nigeria gives telecoms providers two weeks to add ID numbers to SIM cards -statement, 15 December 2020, <https://www.reuters.com/article/nigeria-telecoms/update-1-nigeria-gives-telecoms-providers-two-weeks-to-add-id-numbers-to-sim-cards-statement-idUKL1N2IV2D1>.
- 85 Luana Pascu, Comparitech report shows 17 countries collecting biometric data for SIM card registration, Biometric Update, 9 January 2020, <https://www.biometricupdate.com/202001/comparitech-report-shows-17-countries-collecting-biometric-data-for-sim-card-registration>.
- 86 Yusuf Akinpelu, As Nigeria advances quest for national database, concerns remain, *Premium Times*, 25 May 2021, <https://www.premiumtimesng.com/features-and-interviews/463715-analysis-as-nigeria-advances-quest-for-national-database-concerns-remain.html>.
- 87 Jonathan E. Hillman and Maesea McCalpin, Watching Huawei's 'safe cities', CSIS Briefs, November 2019, <https://www.csis.org/analysis/watching-huaweis-safe-cities>.
- 88 Dana Priest, Craig Timberg and Souad Mekennet, Private Israeli spyware used to hack cellphones of journalists, activists worldwide, *The Washington Post*, 18 July 2021, <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones>.
- 89 Nathaniel Allen and Catherine Lena Kelly, Deluge of digital repression threatens African security, Africa Center for Strategic Studies, 4 January 2022, <https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/>.
- 90 Stephen Kafeero, Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests, *Quartz Africa*, 17 November 2020, <https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/?msclkid=928cf561cfa311ec973734519d2240e6>.

- 91 Quoted in Africa Center for Strategic Studies, Key elements of a national cybersecurity response, Virtual Academic Program Video, 10 August 2021, <https://youtu.be/rDeadSoU3Gg?t=2736>.
- 92 Eliot Higgins, *We are Bellingcat: An Intelligence Agency for the People*, Bloomsbury, 2021.
- 93 Bellingcat, How schoolchildren became pawns in Cameroon's Anglophone crisis, 16 July 2021, <https://www.bellingcat.com/news/africa/2021/07/16/how-schoolchildren-became-pawns-in-cameroots-anglophone-crisis/>.
- 94 Bellingcat, Tigray conflict: Videos provide new details of Mahbere dego massacre, 24 June 2021, <https://www.bellingcat.com/news/2021/06/24/tigray-conflict-videos-provide-new-details-of-mahbere-dego-massacre/>.
- 95 Bellingcat, Black gold burning: In search of South Sudan's oil pollution, 23 January 2020, <https://www.bellingcat.com/news/africa/2020/01/23/black-gold-burning-in-search-of-south-sudans-oil-pollution/>.
- 96 Bellingcat, Tracking the Nigerian Armed Forces' COIN offensive in north-east Nigeria, 20 February 2017, <https://www.bellingcat.com/news/africa/2017/02/20/tracking-nigerian-armed-forces-coin-offensive-north-east-nigeria/>.
- 97 New America Foundation, The malware markets: a graphic exploitation, <https://www.newamerica.org/in-depth/malware-markets/what-products-are-available-malware-markets/>.
- 98 Quoted in Africa Center for Strategic Studies, State responses to the use of information technology by Africa's violent extremist groups,' Webinar Series Video, 2 December 2021, <https://youtu.be/rzRIHY79-d4?t=464>.
- 99 Elise Vermeersch, Julie Coleman, Méryl Demuyne and Elena Dal Santo, The role of social media in Mali and its relation to violent extremism: A youth perspective, International Centre for Counter-Terrorism, 18 March 2020, <https://icct.nl/publication/social-media-in-mali-and-its-relation-to-violent-extremism-a-youth-perspective/>.
- 100 Khadeja Ramali, quoted in Africa Center for Strategic Studies, A light in Libya's fog of disinformation, 9 October 2020, <https://africacenter.org/spotlight/light-libya-fog-disinformation/>.
- 101 Gabriel Weimann, The emerging role of social media in the recruitment of foreign fighters, in Andrea de Guttery, Francesca Capone and Christophe Paulussen (eds), *Foreign Fighters under International Law and Beyond*, TMC Asser Press, 2016.
- 102 See, for example, Jason Warner, *The Islamic State in Africa: The Emergence, Evolution and Future of the Next Jihadist Battlefield*, Hurst, 2021; Nathaniel Allen, The Islamic State, Boko Haram, and the evolution of international jihad, *The Washington Post*, 15 May 2015, <https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/27/the-islamic-state-boko-haram-and-the-evolution-of-international-jihad/>.
- 103 Ken Menkhaus, Al-Shabaab and social media: A double-edged Sword, *The Brown Journal of World Affairs*, 20, 2014. The details here are highly under-researched and somewhat murky, but perceived government/foreign advantages in exploiting ICT to track it might have been what has led al-Shabaab to take a more forceful hand in attempting to co-opt Somalia's ICT infrastructure, potentially aiding in its resurgence.
- 104 Ibid.
- 105 Moulid Hujale, Schools close in north-east Kenya after al-Shabaab targets teachers, *The Guardian*, 20 March 2020, <https://www.theguardian.com/global-development/2020/mar/10/schools-close-in-north-east-kenya-after-al-shabaab-targets-teachers>.
- 106 United Nations Security Council, United Nations monitoring group on Somalia and Eritrea report, 9 November 2018, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_1002.pdf.
- 107 Dan Gettinger, Drone databook update: March 2020, Center for the Study of the Drone, March 2020, <https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/>.
- 108 Richtsje Kurpershoek, Alejandra Muñoz Valdez and Wim Zwijnenburg, Remote horizons: Expanding use and proliferation of military drones in Africa, Pax for Peace, February 2021, https://paxforpeace.nl/media/download/PAX_remote_horizons_FIN_lowres.pdf; Hamza Guessous, Moroccan Armed Forces strike two Polisario SUVs, *Morocco World News*, 16 May 2021, <https://www.moroccoworldnews.com/2021/05/342209/moroccan-armed-forces-strike-two-polisario-suvs>.
- 109 Kelsey D. Atherton, Watch Nigeria's first confirmed drone strike — against Boko Haram, *Popular Science*, 4 February 2016, <https://www.popsoci.com/watch-nigerias-first-confirmed-drone-strike/>. Christopher Soelistyo, Death from the Skies of Libya, Part III: The largest drone war in the world, Pi Media, 28 January 2021, <https://uclpimedia.com/online/death-from-the-skies-of-libya-part-iii-the-largest-drone-war-in-the-world>.
- 110 BBC, UAE implicated in lethal drone strike in Libya, 28 August 2020, <https://www.bbc.com/news/world-africa-53917791>.
- 111 Matt Herbert, Libya's war becomes a tech battleground, ISS Africa, 8 October 2019, <https://issafrica.org/iss-today/libyas-war-becomes-a-tech-battleground>.
- 112 Christopher Soelistyo, Death from the skies of Libya, Part III: The largest drone war in the world, Pi Media, 28 January 2021, <https://uclpimedia.com/online/death-from-the-skies-of-libya-part-iii-the-largest-drone-war-in-the-world>.
- 113 Tom Kingston, Libya is turning into a battle lab for air warfare, *Defense News*, 6 August 2020, <https://www.defensenews.com/smr/nato-air-power/2020/08/06/libya-is-turning-into-a-battle-lab-for-air-warfare/>.
- 114 BBC, UAE implicated in lethal drone strike in Libya, 28 August 2020, <https://www.bbc.com/news/world-africa-53917791>. Matt Herbert, Libya's war becomes a tech battleground, ISS Africa, 8 October 2019, <https://issafrica.org/iss-today/libyas-war-becomes-a-tech-battleground>. Karen Allen, Drones and violent nonstate actors in Africa, Africa Center for Strategic Studies, 6 August 2021, <https://africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/>.
- 115 Mark Pamereau, How \$650 drones are creating a problem in Iraq and Syria, C4ISRNET, 5 January 2018, <https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/>.

- 116 Richtsje Kurpershoek, Alejandra Muñoz Valdez and Wim Zwijnenburg, Remote horizons: Expanding use and proliferation of military drones in Africa, Pax for Peace, February 2021, https://paxforpeace.nl/media/download/PAX_remote_horizons_FIN_lowres.pdf.
- 117 Southfront, Al-Shabab shares never-before-seen footage of its attack on US Camp Simba in Kenya, 4 February 2021, <https://maps.southfront.org/al-shabab-shares-never-before-seen-footage-of-its-attack-on-us-camp-simba-in-kenya/>.
- 118 Nathaniel Allen and Ify Okpali, Artificial intelligence creeps onto the African battlefield, Brookings Institution, 2 February 2022, <https://www.brookings.edu/techstream/artificial-intelligence-creeps-on-to-the-african-battlefield/>.
- 119 Brencil Kaimba, Africa Cyber Security Report 2017, Serianu Ltd, 2017, <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>.
- 120 Maria Bada, Basie Von Solms and Ioannis Agrafiotis, Reviewing national cybersecurity awareness in Africa: An empirical study, *International Journal on Advances in Security*, 12, 2019.
- 121 Quoted in Africa Center for Strategic Studies, Key elements of a national cybersecurity response, Virtual Academic Program video, 10 August 2021, <https://youtu.be/rDeadSoU3Gg?t=700>.
- 122 International Financial Corporation, Digital skills in sub-Saharan Africa: Spotlight on Ghana, May 2019, https://www.ifc.org/wps/wcm/connect/ed6362b3-aa34-42ac-ae9f-c739904951b1/Digital+Skills_Final_WEB_5-7-19.pdf?MOD=AJPERES.
- 123 Quoted in Africa Center for Strategic Studies, Executive summary: Cyberspace security priorities for Africa's national security actors, Virtual Academic Program, 3–25 August 2021, <https://africacenter.org/wp-content/uploads/2022/01/2021-08-Cyberspace-Security-vap-Executive-Summary-EN-1-14.pdf>.
- 124 ITU, National cybersecurity strategy repository, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>.
- 125 Nate Allen and Abdul-Hakeem Ajijola, African lessons in cyber strategy, Africa Center for Strategic Studies, 8 March 2022, <https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/>.
- 126 List of the signatories of the Budapest Convention on Cybercrime is available here: Council of Europe, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, 7 January 2004, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?module=signatures-by-treaty&treatynum=185>.
- 127 For a list of signatories see African Union, List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection, 18 June 2020, <https://au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf>.
- 128 Africa Center for Strategic Studies, The African security sector's response to cyber-enabled organized crime, Webinar series video, 17 February 2022, https://youtu.be/2rbP4g_ngZ0?t=2092.
- 129 Quoted in Africa Center for Strategic Studies, National cybersecurity strategy, Virtual Academic Program video, 24 August 2021, <https://youtu.be/Rlf6AVYuSns?t=619>.
- 130 Ibid.



GLOBAL INITIATIVE

AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 600 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net