CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

MARCH 2024

Security and Trust in Africa's Digital Financial Inclusion Landscape

Aubra Anthony, Nanjira Sambuli, and Lakshmee Sharma

Security and Trust in Africa's Digital Financial Inclusion Landscape

Aubra Anthony, Nanjira Sambuli, and Lakshmee Sharma

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction 1

Insights on Capacities and Challenges in Securing Digital Financial Inclusion 5

How Donors and National Actors Can Work Together Toward Securing Financial Inclusion 14

Conclusions 26

About the Authors 27

Notes 29

Carnegie Endowment for International Peace 37

Introduction

To promote financial inclusion, innovators and policymakers across Africa have encouraged the adoption of financial technologies like mobile banking and mobile money, as well as more emergent technologies such as artificial intelligence and distributed ledgers. This is especially the case in sub-Saharan Africa, where there are an estimated 400 million financially unserved or underserved people. Digital finance is characterized as a catalyst for poverty reduction, as it provides low-income households with access to affordable and convenient tools to support their economic activities. Kenya's M-PESA mobile money system, for example, is famously purported to have lifted households out of poverty.[1] Such tools can facilitate digital payments from governments or businesses to people and vice versa—providing quicker transmission of pensions or welfare, for instance. And these payments are generally considered more efficient and less vulnerable to fraud or theft than cash payments and can help consumers establish a financial history that enables access to loans and other financial services.[2]

Digital financial inclusion is thus a priority across Africa, as evidenced by the uptake of digital technologies in most African markets. According to the Global Findex Database, Africa leads the world in mobile money adoption, the primary driver of digital financial inclusion.[3] Additionally, mobile money accounts have enabled users to save formally, borrow money, make or receive digital payments, receive remittances, and even raise emergency funds. The potential of digital financial services has spurred innovations in the sector of financial technology (fintech), thus creating options for businesses looking to reach new markets or more effectively serve their customers. Between 2020 and 2021, over 2,000 of the estimated 5,200 tech start-ups in Africa were in the fintech sector,[4] a testament to the push to deepen financial sector services and to the indispensable role of digital technologies in driving financial inclusion.

Digital financial services (DFS), however, are not without significant challenges. Consumers less familiar with digital technology, or who have limited literacy, can find DFS difficult to navigate. And consumers in rural or poorly connected regions often have inequitable access to mobile phones and the mobile internet. Access rates for Africa's total population remain stubbornly low. In 2023, among the continent's 1.18 billion people, the mobile phone penetration rate stood at 43 percent, with 489 million unique subscribers, and the mobile internet penetration rate stood at 25 percent, with 287 million users.[5] In addition, the introduction of digital services has created new avenues for criminality to take hold, fraud to transpire, and security to be compromised, with real-world impacts on the businesses driving African economies and the people who are often not afforded adequate protections by law or current-day practice.

Between January 2022 and July 2023, the main sectoral targets for cyber attacks across the continent were financial sector organizations, followed by telecommunications companies and government agencies.[6] Africa reportedly loses about $4 billion (gross[7]) a year to cyber crime, resulting in a 10 percent reduction to gross domestic product (GDP) across the continent,[8] a number that is likely to have increased since 2021. In South Africa, SIM-swap frauds registered a spike that cost a victim an average of more than $900 per incident in 2021;[9] and online banking fraud incidents cost an average of $1,131 per incident in 2022.[10]

About the CyberFI Project

Several years ago, the Cybersecurity and the Financial System (FinCyber) project—implemented under Carnegie's umbrella Cyber Policy Initiative—revealed that more attention should be paid to the relationship between cybersecurity and financial inclusion in Africa.[11] The findings pinpointed the need to incorporate cybersecurity into the technologies driving financial inclusion from the start, rather than as an afterthought. Therefore, in 2021, as part of the initiative, Carnegie launched the Cybersecurity, Capacity Development, and Financial Inclusion (CyberFI) project to examine the potential impacts of Africa's significant digital transformation and how to promote inclusion while mitigating the negative side-effects.

Carnegie worked with African scholars to explore the intersection of digital transformation, financial inclusion, and cybersecurity.[12] The thematic and country-specific perspectives portrayed in the resulting CyberFI papers elucidate how societies can establish trust in digital financial services that serve individuals and communities throughout Africa. This synthesis paper offers key insights and recommendations for the development community based on the papers published and convenings held. It is intended to inform the understanding and actions of those seeking to expand the inclusiveness of digital financial ecosystems across the continent. The insights presented underscore that the security and resilience of those interacting with these systems is important; consumer experience is defined less by the technology involved and more by the socioeconomic effects of using it.

Countries Featured in the CyberFi Project

Table 1 outlines the most persistent threats facing DFS consumers throughout Africa.[13] The range and reach of these threats are broad. Threat actors exploit points of weakness in technology, in its management, and in its administration. They also prey on points of weakness arising from how different individuals may (mistakenly) trust the technology and its administrators. This work offers a more comprehensive framing of both where these weaknesses manifest in practice as well as how different stakeholders can play a more significant role in addressing them to ensure a more secure and resilient digital financial ecosystem across the continent.

Table 1. Common Types of Consumer-Facing DFS Cyber Threats

Types	Definition
Social engineering	Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cyber crime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in person, and via other interactions.[14]
SIM swaps	SIM-swap fraud occurs when scammers exploit weaknesses in two-factor authentication and verification that allow them to use a phone to access personal accounts. A scammer contacts a victim's mobile phone carrier and tricks them into activating a SIM card that the scammer has; this then gives the scammer control over the victim's phone number, enabling them to reroute calls and texts to their device and not the victim's phone.[15]
Denial-of-service attacks	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.[16]
False promotion fraud	Prompts are sent under the guise of a telco promotion, and the recipient is asked to input their PIN as a verification measure to claim their "prize." The fraudster gains access to the recipient's mobile money account with the PIN that was inputted.[17]
Ransomware and malware	Ransomware is a type of malware, or malicious software, that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.[18]
Mobile network operator fraud	This type of fraud involves employees of telcos and occurs in different forms. For example, employees can steal from customers' mobile money wallets, transfer customers' money unauthorized, and collude with other fraudsters to swap SIM cards. It generally involves a telco employee manipulating a customer's account without authorization.[19]
Scam messages/reversal of erroneous transactions	A fake SMS is sent that indicates a deposit into a customer's account. The fraudster then calls the customer to tell them the deposit was a mistake and to send that amount back.[20]
Fortuitous scam	Fraudsters pose as delivery companies and call customers under the pretext of delivering goods to them from relatives abroad. Customers are then instructed to make a deposit to a mobile money account in exchange for delivering the goods.[21]
Third-party vulnerabilities	A third-party data breach refers to a breach that has occurred through a third-party company. The vendor or supplier's system is compromised and used to steal data that belong to the consumer.[22]

Insights on Capacities and Challenges in Securing Digital Financial Inclusion

The following insights on the capacities and challenges identified during the CyberFI project's country case studies are categorized by four main stakeholder groups: governments, firms and businesses, consumers, and donors and the digital development support community.

Governments

Digital financial services span multiple sectors that are developing concurrently, and as a result, governments are adopting experimental policy postures. Multiple sectors in Africa provide digital financial services (DFS): traditional finance (primarily banking services); telecommunications (primarily mobile money services); and emerging technology (such as artificial intelligence and cryptocurrency services). Most African markets have regulatory and legislative frameworks in place to govern the traditional financial sector, dominated by banks, and the telecommunications sector. However, the markets are each handling the introduction of mobile money differently.

For instance, Kenya's financial sector regulator, the Central Bank of Kenya—in coordination with the telecommunications sector regulator, the Communications Authority of Kenya—adopted a receptive "test and learn" approach. The approach enabled the renowned mobile money service M-PESA to grow from a pilot test to a full-scale financial technology behemoth that underpins Kenya's digital financial landscape.[23]

By comparison, the Central Bank of Nigeria (CBN) first established a policy framework that prohibited mobile network operators from operating in mobile money services provision. But then in late 2021, it issued an approval to lift the prohibition in principle, enabling telecommunications companies to participate as long as they set up subsidiaries that operate under rules akin to those regulating banks. In this way, mobile money services in Africa's largest economy still operate according to a banking-led model.[24] Also in 2021, the CBN introduced a central bank digital currency (CBDC), the eNaira, to among other things, drive financial inclusion. Thus, in part, the Nigerian government has also taken a "test and learn" approach; however, its experimentation has so far led to mixed results in improving digital financial inclusion.[25]

In Ghana, an interoperable system facilitating transactions across telecommunications service providers has contributed to the astronomical growth of mobile money in the country. Ghana's telecommunications service providers have gone from only being able to offer their services as agents of banks to being permitted to operate mobile money accounts without linking them to bank accounts.

Meanwhile, although the Central African Republic has very limited financial and digital systems—in part due to its status as a postconflict nation—it has nonetheless embarked on an ambitious digitalization project that aims to develop a national cryptocurrency based on the Bitcoin blockchain. The endeavor to make the resulting Sango Coin legal tender is intended to "modernize and uplift the economy, increase the general population's access to finance and infrastructure, and address financial exclusion."[26] However, the nation's controversial crypto ambitions have been tempered by resistance from several corners, including from the regional banking regulatory authority—which the nation's financial sector is party to—and from actors like the International Monetary Fund.

And in Zimbabwe, trials of a financial technology (fintech) regulatory sandbox have proven uniquely beneficial for entrepreneurs seeking to understand how new regulatory requirements may impact their digital solutions and their bottom line.[27] Sandboxes offer a structured experimental approach to allow fintech businesses to learn about and respond to regulatory advances before their formal adoption—ideally helping fintech businesses' evolution to include addressing associated vulnerabilities in the local regulatory context.

Yet governments struggle to keep up with the rapid pace of digital financial services. Traditional financial services—those provided by formal financial institutions like banks—have long been governed by time-tested policy and regulatory approaches that need relatively infrequent updating thanks to the relatively slow rate of the field's evolution. The intersection of these services with digital technology, however, has greatly accelerated this evolution and introduced serious cyber-enabled risks into the financial domain. Such a rapid pace necessitates far more timely policy responses, but governments are finding it exceedingly difficult to keep up.

Shockingly, South Africa—which has one of the most advanced and digitally dependent financial markets on the continent—has not yet updated its regulatory cybersecurity protections to secure DFS. The country lacks a national cyber strategy, leaving a decade-old national cybersecurity policy framework in place. The resulting effect is a "disjointed and reactive national cyber posture" that has led indirectly to cyber threat escalations and degraded services due to cyber crime, affecting already financially strained individuals and communities.[28] Furthermore, the posture has allowed fast-growing financial technology services to operate within a less regulated space than the formal banking sector.

Namibia, meanwhile, tends to follow a "cut and paste" approach, taking cues from South Africa given the dominance of South African banks and insurance companies. This approach offers some efficiencies, but it also brings policy vulnerabilities into a far more nascent cyberspace.[29]

Cameroon's only national cybersecurity law is from 2010, and as fintech innovation has ballooned nationally in recent years, these regulations are now outdated. The policy environment reactively addresses, rather than anticipates, the needs of a rapidly evolving, innovation-driven sector.[30]

In the Central African Republic, efforts to embrace newer DFS technologies have outpaced the infrastructure needed to allow domestic markets to keep pace. DFS require significant hard and soft infrastructure to operate—for example, internet connectivity and electricity, as well as user access and affordability of services. But given its postconflict status, the country's government faces unique difficulties in establishing the policies and investments needed to rapidly build these components and enable DFS advances to take root domestically.[31]

In Tanzania, digital connectivity through mobile phones and social media is unlocking DFS access to traditional savings and lending groups, such as village community banks and lending associations. DFS are becoming popular, because they mean that physical proximity is no longer necessary to form such groups across interest areas. However, existing regulations for these groups do not adequately account for the resulting expanded linkages brought about by digital connectivity.[32] Furthermore, the regulatory framework currently categorizes financial services by institutional categories rather than service type, which invariably excludes some service providers and stifles product innovation and financial inclusion.

Governments lose citizens' trust when policies and practices do not deliver on stated goals. Having laws, regulations, and policies in place is only part of the equation; it is equally important to implement them with fidelity.

Countries such as Ghana, Kenya, and Nigeria arguably have adequate cybersecurity policies in place, but poor enforcement and/or coordination between relevant sectors impedes effective consumer protection and undermines trust in digital financial services. For instance, Nigeria's regulatory landscape is relatively robust; the Nigerian Payments System Risk and Information Security Management Framework promotes best practices for ensuring strong system protections in DFS (for example, systematic vulnerability assessments and compliance with standards set by the International Organization for Standardization). Nigeria also seeks to build consumer trust through the Central Bank's Consumer Protection Regulations. Yet the existence of these frameworks alone is not sufficient to establish a fully protective environment; many Nigerian consumers reportedly prefer to engage private firms to resolve banking disputes.[33] Even when regulation is strong, implementation has often proven to be a weak link in securing the country's digital financial services landscape.[34]

Approaches that overemphasize process at the expense of impact also undermine confidence. In South Africa, a compliance-based regulatory approach mires organizations and individuals in red tape.[35] Prioritizing compliance means companies expend substantial resources to meet the government's regulatory requirements—usually leading to costly overheads—at the expense of adequately addressing what is happening to customers. A risk-based approach, on the other hand, enables companies to prioritize consumer security and adaptability to varied risks.

In Ghana, regulation has steadily improved in recent years, thanks largely to a 2017 overhaul of the financial sector that addressed many issues of illegality or noncompliance.[36] But this overhaul also caused frustration with formal institutions, and disparate efforts have at times

eroded gains in inclusion. For instance, Ghana's government instituted a single national ID document, the GhanaCard, to avoid onerous verification processes, decrease friction, and promote financial inclusion. However, it caused all telcos to require that customers reregister SIM cards using their GhanaCard. The rollout did not sufficiently consider the time nor the logistical and administrative efforts required for the reregistration process, resulting in backlogs and leading to potential SIM deactivation for those customers unable to comply with the requirements. Such poorly implemented policies undermine consumer trust in formal institutions and digital financial solutions.

When regulatory responsibility is shared or unclear, accountability can fall short. Because digital financial services often straddle traditionally siloed sectors like banking and telecommunications, regulatory responsibility ends up divided across different regulatory bodies. This is especially true across markets where mobile money plays a significant role, such as in Ghana, Kenya, and Nigeria. In these countries, the majority of relevant financial regulation comes from central banks: the Bank of Ghana, the Central Bank of Kenya, and the Central Bank of Nigeria. The interplay between national and regional governance efforts can also blur the lines of responsibility and authority among regulatory bodies. More centralization and clarity in terms of sectoral "ownership" could help streamline processes for drafting regulations and establishing clear requirements for their enforcement. But accountability could still be elusive, given the wide-ranging nature of DFS-borne harms and difficulties inherent in implementing interoperable regulatory approaches.

In South Africa, the financial sector's cybersecurity regulation (and importantly, its enforcement) is far stronger than that for the telecommunications sector. For firms whose products and services span these two sectors, determining which regulations and laws apply—and which will be enforced—is anything but a simple task. The surge in South Africa's banking app fraud illustrates the effects of such unevenness in regulation strength (and implementation) between the telecommunications and financial sectors. [37]

Cameroon's banking and financial policy and regulatory guidelines are set at a regional level, with the Ministry of Finance playing a supervisory role. As such, capacity constraints or a laxity in national-level oversight of domestic digital finance players contributes to enforcement challenges, leading to a situation wherein fintech innovators are largely unaware of whether and which cybersecurity regulations even apply to their work. Against this backdrop, it is perhaps unsurprising that a paltry 16 percent of fintech firms surveyed report safeguarding their apps, and just half of that figure conduct protective measures like penetration testing.[38]

Governments' approaches will naturally vary, so the key to establishing a cohesive regulatory environment is clarity around responsibility within different sectors and regions—for actors both within and outside the government. At present, this clarity is often lacking.

In some contexts, regulation is frail or nonexistent due to underdevelopment of the local technology ecosystem. In postconflict states like the Central African Republic, where digital infrastructure is nascent, governments embrace technology to try to stimulate rapid growth and leapfrog development. But rushing digitization before regulation and protective measures are adopted can compromise the health and sustainability of growth.

Many countries also do not have formalized approaches to information sharing, a centralized cybersecurity emergency response body, or a financial sector-specific incidence response support body. Numerous countries have struggled to appropriately set incident response mechanisms or processes, which further inhibits their capacity to share information across relevant parties when cybersecurity incidents occur. In Ghana, sectoral computer emergency response teams (CERTs) must coordinate with the main Cyber Security Authority, and this process has reportedly resulted in operational confusion and inefficiencies.[39] Similarly, the Tanzania Communications Regulatory Authority oversees the country's central CERT, but it does not have sector-specific CERTs, which could help drive accountability.

Micro-, Small-, and Medium-Sized Enterprises (MSMEs)

MSMEs are the economic backbone of Africa but are often not sufficiently supported. Cybersecurity is critical for any firm providing or using digital financial services, large or small. In Africa, MSMEs make up the lion's share of businesses—a whopping 90 percent.[40] In Cameroon, more than 99 percent of enterprises are MSMEs;[41] and in Ghana, MSMEs account for more than 70 percent of the country's GDP.[42] But MSMEs' influence on African (and international) economies—and therefore their influence on the *security* of these economies—is often underappreciated.[43] Despite their central role, these enterprises often face unique challenges in ensuring the cybersecurity of systems underpinning their services and offerings.

MSMEs face distinctive cybersecurity resource challenges. Smaller businesses that incorporate digital financial services may lack the technical expertise or resources to ensure that products are secure, especially if the businesses are not directly operating in the fintech domain. An MSME's structure generally requires making do with lean teams that specialize in the product or service underpinning their business model—meaning staff often lack the specialized skills necessary to provide sufficient cybersecurity protections for their products and services. To enhance security, businesses need to be adequately staffed to (1) identify and mitigate incoming threats, (2) align these possible threats with cybersecurity standards and best practices, and (3) conduct necessary testing to identify how best to continuously bolster systems' security as financial technologies and external threats evolve. Unfortunately, the capacity of smaller financial firms or businesses to detect and respond to emerging cyber threats is widely insufficient; for example, they might have less access than larger, established players to digital security resources. Firms depend on critical resources like hardware and software to effectively stymie attacks or breaches. MSMEs' budgets generally do not accommodate these important resources, even secure alternatives such as cloud services that

offer more specialized infrastructure, software, and platform-as-a-service.[44] Contracting out cybersecurity-related tasks to third-party providers is often not possible for those businesses already operating at the edges of their profit margins—a common reality for many MSMEs.

Navigating how and whether cybersecurity regulations impact MSMEs is especially difficult. Financial sector regulators naturally focus security efforts on the largest financial institutions, because that is where the money seems to be. Less attention is given to how MSMEs can be expected (or helped) to secure their digital clients and foster cyber resilience—a harder, if less dramatic challenge. Regulations built primarily with larger firms in mind likely discount the unique needs and constraints of MSMEs and therefore effectively ignore the needs of a majority of African firms and individuals. Moreover, requiring MSMEs to adhere to these regulations places a disproportionate burden on them. With limited in-house legal and technical expertise to help navigate complex or evolving regulatory environments, MSMEs often struggle to identify which cybersecurity requirements apply to them and must be complied with. When small firms want to align with cyber resilience best practices or regulations, they sometimes do not know where to turn for answers about cybersecurity expectations and requirements. Ultimately, given these and other issues, innovators are left to function in an ineffective, inapplicable, or altogether absent regulatory environment.

Firms evolve their practices to stay current, but rapid change demands rapid response from support and oversight bodies. The rapid evolvement of fintech, and how firms can leverage fintech to support their growth, creates vulnerabilities that can be easily exploited and that can undermine the benefit of shifting from analog to digital systems.

Digitization can introduce dynamics that either disrupt or enhance long-standing trust frameworks that play a critical role in many African countries and communities. For instance, rapidly implementing digitization efforts and associated policies that do not account for MSMEs' specific needs and a banking sector's current practices and products can lead to harmful outcomes. In Tanzania, efforts to link long-standing community-led savings and lending groups to banks did not lead to better consumer experiences, but rather to greater risk of indebtedness owing to poorly designed products and the banks' aggressive marketing of credit facilities.[45] Policy development approaches need to adequately account for fundamental behavioral and trust dynamics between business communities, financial service providers, and other central actors leading or affected by digitization. Kenyan regulators, for instance, eventually rolled out guidelines on data processing compliance requirements (Data Protection Commissioner)[46] and licensing requirements for fintechs operating in digital credit service provision (Central Bank of Kenya)[47] to address the growing concern of data breaches and fraud concerns that were undermining trust in the digital financial service.

Bright spots emerging across the continent offer insights for stronger risk awareness. In Nigeria, awareness of cybersecurity risks and requirements is relatively strong among a diverse range of organizations, from large banks to small-scale digital financial service

providers. Savvy customers have even managed to circumvent poorly implemented policy: the act of a customer simply including the Consumer Protection Department on complaint correspondence has helped motivate banks to address security grievances. Even when the department has failed to directly address a complaint, this consumer practice has been enough to compel the bank to act; the Central Bank of Nigeria claims it resolved over 94 percent of complaints in 2021.[48] In Cameroon, even though fintech start-ups lack awareness of how national and regional cybersecurity policy should guide their operations, a majority still claim to prioritize security in their products. And in Kenya, mobile money users have occasionally taken cyber awareness-raising matters into their own hands; for instance, in 2023, customers shared tips via social media on mitigating SIM-swap threats, as service providers had been slacking on widely disseminating the existing information on preventive measures despite a surge in the cyber threat.[49]

Innovative partnerships between diverse private sector actors are paving the way to increase cybersecurity awareness among the South African public as well. The South African Banking Risk Information Centre, a nonprofit company formed by four major banks to assist banking and cash transit industries combat cyber crime, launched an online campaign called #TakeACloserLook to encourage people to build awareness about online threats and develop cyber hygiene practices.[50]

Consumers

A lack of digital literacy compounds a lack of basic literacy, numeracy, and/or financial literacy. For individuals navigating the digital financial ecosystem, cyber capacity is often broadly defined to include fundamentals like digital literacy or familiarity with and ability to carry out cyber hygiene best practices. In much of Africa, though, levels of basic literacy, numeracy, and/or financial literacy must also be factored into how resilience is built into products and services meant to safely serve African consumers. Individual users often prove to be the "weakest link" in securing financial systems—a fact that malicious actors all too readily exploit. Fraudulent schemes throughout Africa often prey on those already living at and below the poverty line.

After malware use, social engineering—techniques that exploit human interactions, human behavior, and psychological manipulation to trick users into divulging sensitive information and making security mistakes[51]—emerges as the second-leading threat in the African region. Social engineering accounts for 52 percent of successful attacks on organizations and 91 percent on individuals.[52] In 2021, the Interpol's cyber threat assessment report found that key cyber threats in the region, particularly in Ghana, Kenya, Nigeria, and South Africa, include phishing scams, digital extortion, and business email compromise.[53]

Cultivating security and resilience (in other words, being able to rebound from cyber harm when it does occur) is thus crucially important as formerly unbanked, underbanked, or unconnected people become DFS users. Despite this, however, resilience is often only

framed around technical systems, not individuals. This suggests that resilience measures such as consumer protection practices and regulations have been insufficiently prioritized so far.[54]

The lack of clear accountability channels and low broad public awareness of cyber harms means there is limited to no visibility of how criminals are attempting and getting away with cyber crime. Unfortunately, this means harms are often likely to go unaddressed and unimpeded: In Cameroon, many people do not know where to report cyber crime, and as a result, very few incidents are reported.[55] This is the case even though cyber crime remains a pressing concern; according to the National Agency for Information and Communication Technologies, more than 90 percent of software and operating systems in the country have been hacked.[56] In Ghana, firms' fear of bad publicity leads to a general underreporting of incidents as well.[57] Nigeria also struggles with underreporting (or nonreporting) of incidents, despite strong regulations and relatively high awareness of both the risks and reporting channels available.[58]

Awareness and capacity constraints in identifying and reporting cyber crime contribute to "digital deprivation," where existing socioeconomic disparities exacerbate gaps in access and usage of information and communication technologies (ICTs).[59] In the context of cybersecurity, digital deprivation creates a host of constraints that further limit the cyber resilience of vulnerable populations. These constraints include low digital literacy, suboptimal hardware platforms without adequate security patches, unaffordable data costs, reduced access to security software and technical support, and inherently low-security legacy authentication methods like SMS one-time-passwords. These constraints often directly contribute to compromised cybersecurity for vulnerable people; for instance, in South Africa, "the net effect of data unaffordability is that low-income users sacrifice cybersecurity hygiene when they prioritize data usage."[60]

Thanks to increased reporting of cyber incidents in the media, consumers are becoming more aware of the risks that accompany DFS. But as criminals find novel ways to exploit DFS, consumers' trust will continue to be eroded. DFS-borne risks like fraud are harming service reputation across the continent as protections and mitigations continue to lag. A World Bank report on cyber threats in Africa's financial sector notes the difficulty in quantifying such reputational harms but cites profit losses after major incidents as a barometer.[61]

Donors

Foreign donors and international organizations are carrying out important capacity-building efforts to fortify cyber protections, but these efforts often overlook needs specific to the continent. The donor community recognizes the need for stronger capacity to consistently achieve adequate security protections and the shortage of domestic support to get there—often providing trainings or workshops to upskill government and private sector institutions' staffs around fundamental cybersecurity practices. But these cyber

capacity-building efforts are often based on how cybersecurity has been most commonly threatened and addressed in Western economies. Capacity building thus aligns to a predetermined model of what cyber capacities should be prioritized, as well as how—without sufficient appreciation for the degree of demand for these types of capacity—a more thorough triaging effort might surface.

Donors and organizations tend to produce general capacity-building toolkits for MSMEs to implement, as well as awareness-raising programs tailored toward specific demographics, such as women.[62] While these are useful first steps in orienting these actors toward cyber awareness and resilience, additional targeted support is scarce. In many cases, African countries need direct funding to hire financial cybersecurity specialists; support for acquiring, updating, and maintaining hardware and software licenses and subscriptions; and/or access to contract specialist services such as those offered by cloud service providers. Such support is necessary to secure digital financial services themselves, as well as their integration into MSMEs.

Donors and governments risk undermining trust in DFS when pushing digital financial interventions that fail to deliver on goals of improved resilience, agency, or economic mobility. To drive financial inclusion at scale, governments in Africa have pursued digitalization without an appropriate appraisal of the structural drivers of digital exclusion. In some cases, the rush to digitalize financial inclusion and the policies aimed at securing DFS may counterintuitively create new modes of exclusion, leaving people doubly vulnerable and potentially undermining financial health.

For example, in Nigeria, citing security, policymakers made biometric IDs a requirement for DFS users. This created not only another barrier to entry for vulnerable users, but also failed to adequately protect them from cyber risks given the inadequate legal consequences for cyber criminals. Furthermore, the cost and inefficiencies in the collection and deployment of biometric systems led to high failure rates and data leaks, eroding consumer trust.[63]

In Ghana, efforts to tax electronic transactions, as well as to protect against fraud, ultimately led to erosion of consumer trust and greater resistance to the use of mobile money. An empirical study published by the nonprofit Consultative Group to Assist the Poor in 2022 presents a taxonomy of perceived and encountered risks experienced by DFS consumers that can create a trust deficit and decrease uptake.[64] Even just the perception of these risks' existence—such as inability to transact due to network/service downtime, fraud, insufficient agent liquidity, and complex user interfaces—contribute to consumers adopting "self-protection" steps that include limited or no DFS use.

Governments and policymakers must consider the negative ramifications of advancing digitalization for financial inclusion without a focus on fostering financial health. Furthermore, policies that do not consider unique vulnerabilities at the national, regional, and subregional levels may fail on both financial inclusion and cyber risk prevention.[65]

How Donors and National Actors Can Work Together Toward Securing Financial Inclusion

Cybersecurity requires not only technical tools and practices but also informed behavior by customers and service providers. Secure digital financial inclusion requires even more, including, for example:

- User-centric, secure technology
- More informed decisionmaking by both consumers and providers of fintech
- Improvement, and more effective implementation, of regulations
- Better staffing and oversight of regulatory bodies
- Increased education, awareness, and trust among consumers

Of course, even if shifts occur across all these necessary dimensions, there will still inevitably be breaches, and institutions and consumers will be exposed to harm. This is the reality of a rapidly evolving, dynamic threat environment. No approach to improving the security of financial services across the continent will be impermeable. But concrete actions can (and must) be taken to improve trust and the trustworthiness of digital financial ecosystems across Africa. In much of the world, businesses contract with specialized firms that rely on cloud service providers' security support. But this approach currently appears less feasible in Africa due to infrastructural barriers (for example, a patchwork of data localization laws and variation in connectivity and compute resources) (see Box 1); therefore, alternative approaches to creating financial security are needed.

Necessary steps toward securing financial inclusion

Both international and domestic actors must take steps to improve the security and resilience of digital financial services aimed at deepening inclusion throughout Africa. Each stakeholder group's steps may be unique—national governments will have a different path than external funders, for example—but it's important that stakeholders work in concert toward shared goals.

Box 1. Cloud Computing for Secure Digital Financial Inclusion in Africa

Cloud computing offers cost savings for banking and financial services by reducing the need for local resources and infrastructure. It can improve performance by offering better processing speeds, reliability, and greater security. For fintech firms and digital banks, cloud computing can bring strategic advantages by enabling them to leapfrog legacy infrastructure and in-house technical personnel investments through outsourcing ICT services to third-party providers who specialize in offering software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). Furthermore, regulatory compliance support is increasingly being built into cloud solutions. Combined, these solutions allow start-ups and MSMEs to focus on core business operations and innovation.[66]

The prospects of cloud computing for Africa's digital financial services are increasing; investments in connectivity infrastructure (subsea cables) are driving the expansion, while demand for cloud services is growing by an estimated 25 to 30 percent annually.[67] The number of data centers is proliferating in tech hubs such as Kenya, Nigeria, and South Africa, while strategic efforts targeting smaller African countries are also underway.[68] Primary target clients for cloud solutions are currently big enterprises like banks and governments, but start-ups in the financial sector and rapidly digitizing MSME players will be central drivers of sustained growth. Currently, notable tech sector players like Microsoft, Amazon Web Services, Oracle, Google Cloud, and Huawei are all in a race to grab the cloud market share in Africa's fintech sector.[69] And across many African markets, financial sector regulators have issued cloud computing guidelines to steer adoption and compliance with relevant legal and regulatory instruments.

However, for cloud computing to drive the inclusion of new entrants to formal financial systems, cloud-based solutions need to be adaptable to operate in areas of low connectivity internet access—especially in Africa's more rural areas where a majority of un/underserved financial customers are likely to be—as well as to navigate power/energy challenges that remain salient. Other challenges that must be overcome include data localization requirements in some jurisdictions and lack of clear cloud adoption guidelines, which are particularly valuable to those actors making decisions at the intersection of cloud computing and digital sovereignty.[70] Presently, due to these factors, the costs of cloud services may be unaffordable for MSMEs, but creative partnerships between the public and private sectors and the donor community could catalyze cloud computing's potential to sustainably, reliably, and securely serve Africa's digital economies.

Acknowledge and Reinforce the Strength of Africa's Economic Backbone

Donors must reorient cybersecurity support to better match the reality of digital financial services ecosystems across Africa. Capacity-building support and technical assistance will be critical to help smaller firms handle the scope of cyber threats and to help governments develop or improve policies to better contend with how a majority of financial transactions occurs. But donors should not assume that broadly applied training and financing support models will suffice. Instead, they should provide support that explicitly prioritizes context-oriented tactics, starting with, for example, a realistic needs assessment and risk profile for the country or region as well as the sector, as appropriate. Among other benefits, this effort could increase understanding of the degree to which domestic policy accounts for transactions taking place (and therefore cyber attack targets arising) in the informal economy or with MSMEs. Large financial institutions will of course be the first line of defense. But ensuring that security efforts focus on the entire range of financial activity on the continent will be crucial for realizing financial inclusion.

Given the importance of consumer trust in the system, donors and national policymakers must prioritize understanding where people face the greatest threats of financial loss in the local context. This learning process will neither be straightforward, nor will it be static. For example, in Nigeria, the dominant channel of loss is through mobile banking, whereas in Kenya and Uganda, mobile money carries greater risk. Such realities will reveal where cybersecurity programming—trainings, policy support, and technical assistance—could be of the greatest benefit and therefore must inform how and where donor programming is directed.[71] They should also inform national policy development efforts. Policymakers must begin with an honest assessment of the national (and subnational) strengths and weaknesses rather than effectively copy and paste other countries' or communities' efforts.[72] Governments look to neighbors for helpful policy "blueprints" and assessments of likely threat trends, but each country's financial ecosystem differs; policies and practices must reflect that.

Policy can best support local realities—for example, fintech trends, ecosystem limitations, and strengths and challenges of entrepreneurs—by embracing practice-oriented testing to ensure flexibility and adaptation. Embracing sandboxes with a policy-minded learning mentality can go a long way toward building flexible and robust policy. These sorts of test beds can do more than just enable entrepreneurs and firms to learn rules of the road with proposed regulations; they can also let policymakers understand the interplay of regulations with different technologies and business models. Relying on these kinds of approaches can lead to development of more tailored, practical guidance for interpreting common challenges.

In many countries, including Ghana, Kenya, Nigeria, Rwanda, South Africa, and Zimbabwe, policymakers have used regulatory sandboxes to ease the growing pains associated with both fostering rapid innovation and holding it in check. When done well, the sandboxes create a "cordoned-off" testing area that allows regulators to base their recommendations on live experiments, pressure-test the efficacy of proposed regulations, and make faster and better-informed decisions on how to regulate new products or services in the market before fully releasing them in a way that may cause disruption.[73]

For instance, South Africa—through the Intergovernmental Fintech Working Group[74]—has instituted a regulatory sandbox to allow fintech firms to assess the impact of regulatory compliance on innovations before they hit the market. In Zimbabwe, the National Fintech Steering Committee, under the aegis of the Reserve Bank of Zimbabwe, established a fintech regulatory sandbox to facilitate testing.[75] The process enabled innovation, collaboration among participants, the monitoring of financial technology developments, and research support for innovators. Sandbox approaches could be leveraged to greater potential; for example, in South Africa, both regulatory sandboxes and technical sandboxes could be used for dedicated security testing of beta versions, helping to substantially improve the strength of protections that fintech firms enjoy.

Agent banking is an underutilized conduit for amplifying end users' cybersecurity awareness. Agent banking uses authorized agents to deliver financial services in person to customers beyond the reach of the traditional banking branch network.[76] It has been a significant catalyst in driving both analog and digital financial inclusion in Africa.[77] In Kenya, DFS facilitated by agent banking has surged since 2021, in part due to the COVID-19 pandemic; the Central Bank of Kenya has noted a 36-percent jump in cash transacted by mobile money agents. In Ghana, agent banking facilitated access to previously unreached populations, with 1.5 million people—30 percent of them women—accessing mobile-based savings.[78]

Beyond just facilitating transactions, agents play a crucial role in enhancing financial literacy in new digital modalities.[79] Agent banking also offers an overlooked "trusted" avenue to raise cybersecurity awareness among vulnerable populations. Trust plays a vital role in the success of financial inclusion efforts pursued through agent banking.[80] Because agents are embedded in communities, can draw on large networks, and have a long history of supporting financial capacity building, they are potentially well positioned to bolster cybersecurity reporting capabilities and regulatory awareness.

Over the long term, regulation must be flexible and resilient in responding to the steady evolution of DFS technologies and their inherent vulnerabilities. Many stakeholders in Africa complain that overly broad or restrictive regulations risk stifling growth of an innovation-filled sector that supports financial inclusion and economic activity. As a result, policymakers sometimes remove or limit regulations to avoid the appearance of slowing local growth. But they cannot afford to eschew protections of large vulnerable populations—including MSME owners and consumers—for the sake of short-term economic gains. Flexible policies that are explicitly tailored to the needs of key drivers of the economy (like MSMEs) will go a long way toward achieving sustained growth.

Build Sustainable Capacity Where It Is Most Needed

Bolstering cybersecurity will demand more—and sustained—support in the financial sector across Africa. The financial sector includes not only traditional banks but also fintech firms, mobile money operators, and other financial institutions such as microfinance institutions. It is imperative to appreciate how much digital financial services are driving digitalization, especially for businesses and consumers. As concepts like Digital Public Infrastructure (DPI) take root in driving digitalization investment, the lessons from securing digital finance will be invaluable in advancing other foundational DPI pillars, like digital identity and data exchange. Donors can prioritize funding activities that both strengthen cybersecurity capacity for the financial sector today and support countries in their efforts to sustain capacity for the long term.

Build the capacity of consumers

As both the first and sometimes last line-of-defense, DFS users must be a priority for capacity-building and awareness-raising efforts**.** Donors must better orient their cybersecurity support to meet the needs of local consumers. For example, they should deliver trainings that account for the local policy environment and the most relevant local cybersecurity risks. Importantly, they should also recognize that local firms and organizations might need their capacities built in a very different way than larger or multinational companies and organizations. By starting with practical, locally led consultations—with a locally based organization (such as a civil society research group or a university group)—to map relevant capacity needs,[81] donors can ensure that their efforts focus on the most relevant cybersecurity risks (rather than simply check a box*).* Assessing these risks and tailoring trainings accordingly can help ensure that locally actionable (rather than standard) cybersecurity recommendations are put forward.

Capacity-building efforts should also include helping to fund and potentially deliver awareness-raising campaigns. Broad awareness of cyber risks is critical, but increasing consumers' and small businesses' awareness of the implications of a shifting policy environment or evolving practices regarding digital financial services is just as important. In Ghana, an e-levy program meant to tax electronic transactions was hastily rolled out, creating an opportunity for scammers to leverage resulting confusion and launch a wide-scale fraud campaign.[82] By raising consumers' awareness of both the nature of risks and the various ways to protect themselves in the digital ecosystem, this sort of consumer exploitation can be mitigated.

Build the capacity of financial service providers and MSMEs leveraging DFS

In particular, the capacity building of financial service providers to protect against cybersecurity threats is critically needed—whether in the form of locally tailored guidance or more creative models of support like public-private partnerships or sustained financial support for the hiring or retention of skilled (and ideally local) tech talent. MSMEs in the financial services domain will benefit from activities that address common limitations in

both legal and cybersecurity expertise on their teams. Training could be provided, but given many firms' constraints in both staffing and time, it may be more practical to deliver technical support (financial or in-kind) to bolster systems or ensure compliance of products or processes with given regulations. In-kind support could also involve help with establishing public-private partnerships that better align resources with MSMEs' cybersecurity needs. Start-ups will also benefit from ongoing help with specialized but rote tasks, like penetration testing. Capacity building should also include pursuing other ways of forging longer-term security support for small, stretched-thin teams, such as using pooled ecosystem resources for strengthening cybersecurity capacity (for example, technical experts housed in research institutions could provide free vulnerability assessments).[83] Capacity-building assessments that do not seek to probe those gaps and challenges specifically related to the target actors (such as MSMEs or established sector players) will result in capacity building efforts missing their mark.

It is widely known that many businesses lack coordination mechanisms to share information, including with national governments. When appropriately structured, information sharing can alert different DFS actors to vulnerabilities that could be exploited. It can allow actors to share successful approaches in mitigating risk across public-private barriers and between different sectors. Unfortunately, there is currently limited information sharing in Africa on successful attacks or even common threats—often because businesses believe (perhaps rightly so) that their reputations will be damaged if their cybersecurity is shown to be lacking. This perception can and should be addressed, as information sharing is often highly beneficial.

Strengthen information sharing

As information sharing is a key need across contexts, it should be a priority issue in donor funding streams, especially as a component of capacity building. But donors should support convenings or collaborative efforts to allow local actors to self-organize and address the issue (for example, by aiming for shared protocols and standards)—as (in)formal modalities with stakeholder buy-in could emerge and have a more lasting impact than externally imposed directives. While many aspects of information sharing will need to reflect specific local trust frameworks and procedural or societal realities, some of the fundamental issues needing to be addressed are universal. For example, enterprises resist sharing details on how they are, or have been, vulnerable to hacking or ransom attacks; they worry about the erosion of consumer trust once their brand has been linked with a cyber breach.

Organizations like AfricaCERT and the Africa Cybersecurity Resource Centre (ACRC) have been set up to facilitate coordination and information sharing among computer incident response teams (CIRTs) on the continent. International funders should explore how their agencies (for example, the United States Cybersecurity and Infrastructure Security Agency [CISA] or the European Union Agency for Cybersecurity [ENISA]) could partner with national and regional peers in Africa to offer lessons and insights from their experiences

standing up information sharing efforts and public-private information-exchange mechanisms. American and European companies operating in African markets can also lead by example by setting up local or regional versions of their information-exchange modalities and invite their peers to engage, observe, and participate.

The international community should also continue to prioritize the hard work of destigmatizing cybersecurity breaches. This might include working with key investors to ensure that firms are protected against blowback if/when they share details about cybersecurity incidents, or creating space by establishing the types of fora that allow for candid, ongoing exchanges between the public and private sectors. Awareness-raising campaigns can also drive information sharing by leveraging existing risk mitigation architectures like CERTs/CIRTs. After the hacker group Anonymous Sudan conducted a cyber attack on MTN Nigeria, Nigeria's CERT (ngCERT) took proactive measures to limit harm by distributing guidelines on how organizations in the country can protect themselves against cyber risks. ngCERT released advisories that promoted protection measures against distributed denial-of-service (DDoS) attacks and implored organizations to educate employees on cybersecurity best practices.[84]

National and regional policymakers can greatly improve information exchange by establishing frameworks to incentivize or support the practice and to protect against associated concerns (for example, private sector firms' fear of reputational risk). Exploring how best to establish intersectoral processes for information exchange would also be beneficial; malicious actors recycle similar techniques/approaches across domains, and information silos only help those efforts. Additionally, establishing regional-level coordination bodies or public-private partnerships for cross-national information exchange on threat actors and threats could also help improve information exchange. The African Union (AU)—under the auspices of the AU Convention on Cyber Security and Personal Data Protection (also referred to as the Malabo Convention), which entered into force in 2023—could potentially provide coordination mechanisms and support.

Beyond international cooperation, national policymakers can work to establish fora (or identify existing platforms) that encourage increased public-private information exchange in-country. By creating appropriate space for public-private dialog and establishing the parameters for candor, governments and corporations alike will be better positioned to explore both time-tested approaches (such as developing shared standards for public-private information exchange) and novel approaches (such as automating real-time information sharing for certain types of security incidents).[85] The government of Kenya, in light of recent nationwide cyber attacks, has acknowledged the need for such engagements and has initiated a multistakeholder cybersecurity roundtable to discuss the management of cyber threats in an ever-evolving landscape.[86]

Build capacity in the public sector

Support for the public sector should focus on deepening and sustaining its ability to respond to cyber incidents, for example through CERTs at the institutional level. More countries should establish national-level CERTs, as well as sector-specific response teams, such as for the financial sector. Regional organizations like Smart Africa could be well positioned to draw from a continent-wide network of CERT teams and relevant expertise to offer capacity building and support. Among other countries, Ghana and Nigeria have instituted a robust response to addressing cyber threats through their national CERT coordination centers and/or sector-specific CERT efforts and legally mandated incident reporting (see Table 2). Most recently, in May 2023, Ghana launched the Financial Industry Command Security Operations Centre, a platform for sharing threat intelligence among regulated financial institutions; twenty-three banks are currently directly connected.[87]

Table 2. CERT/CIRT Status of Select Countries

Country	CERT/CIRT	Sector-Specific CERTs/CIRTs as of February 2024
Cameroon[88]	Cameroon's National Agency for Information and Communication has a national-level CIRT.	There are no sector-specific CERTs/CIRTs in Cameroon.
Central African Republic[89]	There is currently no CERT/CIRT in the CAR.	There are no sector-specific CERTs/CIRTs in the CAR.
Ghana[90]	A national- level CERT was established pursuant to the Cybersecurity Act of 2020.	The Bank of Ghana Security Operations Centre, the National Communications Authority's CERT, and the National Information Technology Agency-Security Operations Centre are responsible for the financial, telecommunications, and government sectors, respectively.
Kenya[91]	The KE-CIRT coordination center operates nationally with local and international collaboration.	There are no sector-specific CERTs/CIRTs in Kenya with information-sharing protocols.[92] The Central Bank of Kenya, however, has a set of cybersecurity guidelines intended for payment service providers.[93]
Namibia[94]	The Communications Regulatory Authority of Namibia established a national cyber incident response team.	Namibia does not have sector-specific CERTs/CIRTs, but the national team has been tasked to develop frameworks for sector-specific CIRTs.
Nigeria[95]	ngCERT is the national-level computer emergency response team, and the National Information Technology Development Agency's CERT is the government team. The lateral government team is tasked with coordinating and facilitating information sharing; providing mitigation strategies and recommendations for incident response and recovery; and researching and analyzing trends and patterns of incident activity for government ministries, departments and agencies and the private sector.	There are no sector-specific CERTs/CIRTs; however, the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers has outlined the respective responsibilities held by incident response teams. [96]
South Africa[97]	The Cybersecurity Hub is South Africa's national computer security incident response team.	The Cybersecurity Hub's incident response portal allows for reporting sector-specific cyber incidents and the type of cyber incident as well (such as malware, ransomware, or DDoS,).
Tanzania[98]	Tanzania's Communications Regulatory Authority currently steers a national-level CERT.	There are no sector-specific CERTs/CIRTs in Tanzania, but the Communications Regulatory Authority has issued a framework to set up CERTs tailored to specific sectors.[99]
Zimbabwe[100]	The Postal and Telecommunications Regulatory Authority of Zimbabwe, in cooperation with the International Telecommunication Union had planned to set up a CIRT by 2021.[101] However, it has not yet happened.[102]	There are no sector-specific CERTs/CIRTs in Zimbabwe.

Increasing cybersecurity familiarity among policymakers and regulators will help strengthen the protections and incentives driving cybersecurity compliance today. Groups like the Global Forum on Cyber Expertise and the Toronto Centre are leading promising work. With a more cyber-aware workforce, governments can right-size policies to better meet the needs that arise from an ever-evolving risk profile and can fine-tune policy instruments for local priorities (for example, those faced by MSMEs). In countries with more established tech ecosystems—for example, Kenya, Nigeria, and South Africa—donors could work creatively with governments to onboard ready local cyber talent, in addition to upskilling or reskilling people already within government. In addition, regulators and businesses could explore public-private partnership models that allow for secondments and on-the-spot support for standing up and overseeing helpful innovations like regulatory sandboxes. In countries with less established tech ecosystems or a less cyber-aware workforce, governments and the private sector may need to develop contracting relationships that strengthen local tech ecosystems rather than foster dependencies (see Box 2).

Box 2. Capacity Building and Digital Dependence

When businesses and governments leverage digital technology to improve financial services, they face decisions about whether to develop in-house cybersecurity capacity and infrastructure or contract with external providers based in-country or internationally. Costs of building in-house capacity are often high—sometimes prohibitively so for MSMEs whose main business offerings depend on staff having the skills necessary to deliver their business products, not ensure cybersecurity. External providers based in-country can offer expediency and complementary skills; in other words, the skills of firms with expertise in cybersecurity or digital transformation complement the skills of financial firms operating in more analog spaces. They can also offer short-term ways to fill gaps in cybersecurity expertise. But relying on local providers may be impractical if necessary cybersecurity skills are in low supply. In less digitally developed markets especially, international firms are often best equipped to provide cybersecurity support, so building a DFS business model that depends on these skills may mean that international linkages are largely unavoidable. But how these linkages are structured matters: contracting decisions can implicate dependencies, and relying on short-term support from external actors may set organizations (and countries) up for a less sustainable digital transformation if contracting arrangements undermine longer-term growth or security of the local digital ecosystem. As digital markets develop globally, governments must make choices about how best to reconcile growth with autonomy—and these choices will impact how both large and small firms interact with cyber threats.

Decisions around how best to address cybersecurity capacity gaps should account for both financial and geopolitical considerations, and they require balancing the sometimes different priorities of stakeholders. For example, firms may prioritize minimizing costs while governments may prioritize cultivating strategic autonomy. Governments and donors can make it easier for smaller firms and businesses to fill cybersecurity gaps by investing in skills capacity building at the local level, tailoring support efforts to bolster the most in-demand skills, and/or establishing partnership models that prioritize long-term sustainability. For example, while Brazilian and Indian markets long relied on foreign digital payments providers to help solidify e-payments capacity in-country, the sizable profits extracted by foreign corporations motivated investment in more home-grown alternatives (such as Pix, the instant payments platform managed by the Central Bank of Brazil[105]; and the instant Unified Payments Interface managed by the National Payments Corporation of India[106]). These systems now support lower-cost financial operations in-country and serve as models for digital public infrastructure elsewhere.[107] On the other hand, in Kenya, the government and the leading DFS provider (M-PESA) have managed to successfully navigate external partnerships by letting market forces entice competition in cloud services, allowing private sector actors to shift from and to international corporations as their needs dictate.[108]

Address Regulatory Fragmentation

Donors and other international organizations with influence on the continent (for example, global nongovernmental organizations targeting cybersecurity) can help ease the burden of fragmentation by providing support for MSMEs and other firms seeking to navigate complicated legal landscapes. Even in countries where regulations are in place (or are strong), fragmentation leads to confusion and lack of clarity around what applies to whom and what are the appropriate channels for harm redress. For larger institutions with adequate internal legal support, fragmentation is navigable, but for MSMEs, a fractured regulatory landscape can overwhelm already underresourced actors. Depending on country-specific challenges, having access to resources would help local start-ups translate regulatory requirements into actionable advice based on local constraints. Cloud service providers increasingly offer built-in security, regulatory, and compliance controls that can benefit financial sector MSMEs and fintech firms. Donors working to secure digital financial inclusion could help foster creative partnerships to drive down the cost of accessing such cloud services. Even in environments where regulatory reform is needed, donors and other international actors could partner with local technical centers (for example, in academia, civil society, or local industry associations) to deliver tailored guidance to MSMEs for navigating gaps or contradictions in local regulation.

Additionally, in cases where it is appropriate given country priorities and contextual needs, donors could work with governments to identify areas where increased regulatory clarity is required to support effective implementation and adherence by impacted groups and

across regional or sectoral lines. Donors could support regulatory bodies with landscaping studies, legal analyses, or on-the-spot support to streamline existing or pending policies and regulations. They could also encourage stronger regional coordination through, for example, supporting workshops or convenings to bring together policymakers from neighboring countries to encourage regional engagement and/or alignment as appropriate.

While international actors can help address the impacts of fragmentation, national policymakers are the only actors who can realistically address fragmentation or contradictions in policy. If the policy and regulatory environments function as enablers, not deterrents, of coherent digital transformation, everyone benefits. Whenever revisiting contradictions in existing policy is impractical, policymakers should explicitly conduct analyses to understand points of friction that arise from policies or regulations—for instance, those governing telecoms versus banks—and develop guidance for how to weigh relevant directives coming from competing legislation.

The AU has provided national policymakers with valuable guiding resources. Policymakers could leverage the stated focus of the union's Digital Transformation Strategy for Africa (2020–2030); in response to the threats of digital transformation, "The Commission in collaboration with other Continental Institutions and Regional Economic Communities will work with Member States to identify and address barriers to harmonization of laws and regulations and drive leadership for necessary reforms that ensure future investment in digital transformation."[103] African policymakers must establish stronger alignment with relevant AU level laws and frameworks, including by leveraging existing efforts at the regional level, to bolster cross-jurisdictional efforts in securing cyberspace. This is a precondition for the success of continental initiatives such as the African Continental Free Trade Area and the Pan-African Payment and Settlement System (PAPSS), whose e-commerce ambitions will require secure and resilient digital financial rails across all participating jurisdictions.[104]

The mandate for individual AU member states to align their cybersecurity laws to the AU Convention on Cyber Security and Personal Data Protection provides an entry point to address regulatory fragmentation across the continent. The convention, initially drafted in 2011 and later adopted in 2014, finally gained the requisite number of ratifications and entered into force in 2023. It is a unique legal instrument combining the areas of cybersecurity, cyber crime, digital transactions, and data protection, with input from both cybersecurity and financial sector experts. The convention's salient features call for robust cross-border collaboration in combating cyber threats. The convention affords a regulatory confluence of cybersecurity and the financial sector, providing an opportunity to improve information sharing and knowledge exchange through public-private partnership. These convention features—many of which will need updating—provide opportunities for the main ecosystem players, including the donor community, to facilitate collaboration at the regional level, while also amplifying local ecosystem conditions. Challenges will, of course, arise at the intersection of local contexts and decisionmaking; the convention affords selective opt-out mechanisms that can encourage countries to ensure alignment with the continental instrument while still protecting local sovereignty.

Conclusion

Digitalization can drive innovation and socioeconomic development. But it also generates risks of fraud, exploitation, and other vulnerabilities. These risks threaten the stability of both national and global financial systems. The CyberFI project's efforts reveal that policymakers and funders largely know what needs to be done but continue to face obstacles in putting in place the necessary components to secure digital financial inclusion.

The issues outlined in this paper will only grow in importance, as DFS is a central starting point for many countries going through digital transformation. With common services like mobile money and mobile lending frequently serving as a gateway to broader digital transformation, the cybersecurity and resilience approaches that countries establish for DFS will have outsized impacts on their longer-term digital trajectories. Donors, multilateral organizations, and national policymakers all have a responsibility to ensure that amid this digital revolution, cyber risks—and the resulting harms borne by those participating in this digital revolution—are effectively minimized.

As the international community further shifts its focus toward DPI, the project's insights and recommendations will likely become increasingly relevant. Digital payments, digital IDs, and data exchanges will play ever more critical roles in a country's ability to participate in a global digital economy and serve its citizens in a digital age. And cloud-based services will become more integrated in financial service provisions worldwide. As such, a wider range of policy responses to the challenges will undoubtedly arise from the activities and priorities of largely U.S.-based cloud service providers as they seek to find footing across Africa.

Over the long term, practices, policies, and regulations must be flexible and resilient in responding to the steady evolution of DFS technologies and their inherent vulnerabilities. Many in Africa complain that overly broad or restrictive regulations risk stifling growth of an innovation-filled sector that supports financial inclusion and economic activity. As a result, policymakers sometimes remove or limit regulations to avoid the appearance of slowing local growth. But policymakers cannot afford to eschew protections for the sake of short-term growth. And donors cannot afford to push stock solutions to distinctive problems. Policies and approaches that better promote overall trust in the health of the digital economy—and that address the specific needs of those engaging in Africa's vibrant and ever-evolving digital financial ecosystem—are more likely to contribute to sustained economic growth.

About the Authors

Aubra Anthony is a senior fellow in the Technology and International Affairs Program at Carnegie, where she researches the human impacts of digital technology, specifically in emerging markets.

Nanjira Sambuli is a fellow in the Technology and International Affairs Program.

Lakshmee Sharma is a senior research analyst in the Carnegie Technology and International Affairs Program.

Notes

1 Stella Dawson, "Why Does M-PESA Lift Kenyans Out of Poverty?," CGAP (blog), January 18, 2017, https://www.cgap.org/blog/why-does-m-pesa-lift-kenyans-out-of-poverty.

2 "Igniting SDG Progress through Digital Financial Inclusion | Department of Economic and Social Affairs." United Nations. Accessed February 6, 2024. https://sdgs.un.org/publications/igniting-sdg-progress-through-digital-financial-inclusion-30370.

3 "Financial Inclusion in Sub-Saharan Africa," FinDev Gateway, accessed January 19, 2024, https://www.findevgateway.org/region/financial-inclusion-sub-saharan-africa.

4 "Fintech in Africa: The End of the Beginning," McKinsey & Company, August 30, 2022, https://www.mckinsey.com/industries/financial-services/our-insights/fintech-in-africa-the-end-of-the-beginning.

5 "The Mobile Economy: Sub-Saharan Africa 2023," *The Mobile Economy* (blog), GSMA, accessed January 19, 2024, https://www.gsma.com/mobileeconomy/sub-saharan-africa/.

6 "Cybersecurity Threatscape of African Countries 2022–2023," Positive Technologies, July 28, 2023, https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

7 Daniel F. Runde and Thomas Bryja, "The Role of AGOA in Accelerating Africa's Digital Transformation," Center for Strategic and International Studies, November 7, 2023, https://www.csis.org/analysis/role-agoa-accelerating-africas-digital-transformation.

8 Timi Odueso, "CAF Is Tackling Africa's $4bn Cybersecurity Threat," *TechCabal* (blog), May 6, 2022, https://techcabal.com/2022/05/06/africa-cybercrime-cyber-africa-forum.

9 "This Type of Fraud Has Spiked in South Africa—and People Are Losing Thousands of Rands,"BusisnessTech, October 23, 2022, https://businesstech.co.za/news/mobile/634947/this-type-of-fraud-has-spiked-in-south-africa-and-people-are-losing-thousands-of-rands/.

10 "SABRIC Annual Crime Stats 2022," SABRIC, accessed January 19, 2024, https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2022/.

11 "FinCyber Strategy Project: Cybersecurity and Financial Inclusion," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/specialprojects/fincyber/financialinclusion/.

12 Nanjira Sambuli and Taylor Grossman, "Introducing CyberFI: Perspectives on Cybersecurity, Capacity Development, and Financial Inclusion in Africa," Carnegie Endowment for International Peace, May 2, 2022, https://carnegieendowment.org/2022/05/02/introducing-cyberfi-perspectives-on-cybersecurity-capacity-development-and-financial-inclusion-in-africa-pub-87001.

13 Silvia Baur-Yazbek, "Cyber Attacks That Threaten Financial Inclusion," CGAP (blog), September 18, 2018, https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion.

14 "What Is Social Engineering?," Kaspersky, November 1, 2023, https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

15 Dan Rafter, "SIM Swap Fraud Explained and How to Help Protect Yourself," Norton, June 13, 2023, https://us.norton.com/blog/mobile/sim-swap-fraud; and "What Is a Sim Swap? Definition and Related FAQs," *Yubico* (blog), accessed January 19, 2024, https://www.yubico.com/resources/glossary/sim-swap/.

16 "What Is a Distributed Denial-of-Service (DDoS) Attack?," Cloudflare, accessed January 19, 2024, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

17 Nnenna Ifeanyi-Ajufo, "Digital Financial Inclusion and Security: The Regulation of Mobile Money in Ghana," Carnegie Endowment for International Peace, September 19, 2022, https://carnegieendowment.org/2022/09/19/digital-financial-inclusion-and-security-regulation-of-mobile-money-in-ghana-pub-87949.

18 "Ransomware—Definition," Trend Micro, accessed January 19, 2024, https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

19 Ifeanyi-Ajufo, "Digital Financial Inclusion and Security."

20 Ibid.

21 Ibid.

22 Kyle Chin, "What Is a Third-Party Breach? Definition & Tips for Reducing Risk," UpGuard, June 26, 2023, https://www.upguard.com/blog/third-party-breach.

23 Njuguna Ndung'u, "M-PESA, a Success Story of Digital Financial Inclusion," July 1, 2017, https://www.bsg.ox.ac.uk/research/publications/m-pesa-success-story-digital-financial-inclusion.

24 Omoleye Omoruyi, "Mobile Money Account Ownership in Nigeria Grows by 6% Despite Various Concerns," Technext, May 18, 2023, https://technext24.com/2023/05/18/mobile-money-grows-from-16-to-22/.

25 Jookyung Ree, "Nigeria's eNaira, One Year After," International Monetary Fund, May 16, 2023, https://www.imf.org/en/Publications/WP/Issues/2023/05/16/Nigerias-eNaira-One-Year-After-533487.

26 Tomslin Samme-Nlar, "Securing Digital Finance in Post-Conflict Central African Republic," Carnegie Endowment for International Peace, May 22, 2023, https://carnegieendowment.org/2023/05/22/securing-digital-finance-in-post-conflict-central-african-republic-pub-89799.

27 Mapuranga, Douglas. *Sandbox or Quicksand? An Analysis of Zimbabwe's Fintech Regulatory ...* Carnegie Endowment for International Peace, February 7, 2024. https://carnegieendowment.org/publications/91533.

28 Noëlle Van der Waag-Cowling, "Dividend or Liability? Financial Inclusion, Digital Deprivation, and Cyber Risk Proliferation in South Africa," Carnegie Endowment for International Peace, May 2, 2022, https://carnegieendowment.org/2022/05/02/dividend-or-liability-financial-inclusion-digital-deprivation-and-cyber-risk-proliferation-in-south-africa-pub-87017.

29 Elmarie Biermann, "A Digital Odyssey: The Convergence of Rapid Digitization, Population Dynamics, and Financial Risk in Namibia," Carnegie Endowment for International Peace, April 2, 2024, https://carnegieendowment.org/2024/04/02/digital-odyssey-convergence-of-rapid-digitization-population-dynamics-and-financial-risk-in-namibia-pub-92080.

30 Tomslin Samme-Nlar, "Cameroon's Fintech Start-Ups' Attitudes Toward and Culture of Cybersecurity," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/05/19/cameroon-s-fintech-start-ups-attitudes-toward-and-culture-of-cybersecurity-pub-87137.

31 Tomslin Samme-Nlar, "Securing Digital Finance in Post-Conflict Central African Republic," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.

org/2023/05/22/securing-digital-finance-in-post-conflict-central-african-republic-pub-89799.

32 Emmanuel Mwanambali Mungongo, "Benefits and Risks of Bank and Savings Group Partnerships in Tanzania," Carnegie Endowment for International Peace, January 8, 2024, https://carnegieendowment.org/2024/01/08/benefits-and-risks-of-bank-and-savings-group-partnerships-in-tanzania-pub-91327.

33 Elizabeth Kolade, "Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security," Carnegie Endowment for International Peace, May 13, 2022, https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123.

34 Olatunji Olaigbe, "The Deep Roots of Nigeria's Cybersecurity Problem," WIRED, September 19, 2022, https://www.wired.com/story/nigeria-cybersecurity-issues/.

35 Noëlle Van der Waag-Cowling, "Dividend or Liability? Financial Inclusion, Digital Deprivation, and Cyber Risk Proliferation in South Africa," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/05/02/dividend-or-liability-financial-inclusion-digital-deprivation-andcyber-risk-proliferation-in-south-africa-pub-87017.

36 Nnenna Ifeanyi-Ajufo, "Digital Financial Inclusion and Security: The Regulation of Mobile Money in Ghana," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/09/19/digital-financial-inclusion-and-security-regulation-of-mobilemoney-in-ghana-pub-87949.

37 Hanno Labuschagne, "Big Surge in Banking App Fraud in South Africa—Beware Sneaky SIM Swaps," MyBroadband, accessed January 19, 2024, https://mybroadband-co-za.cdn.ampproject.org/c/s/mybroadband.co.za/news/banking/464867-big-surge-in-banking-app-fraud-in-south-africa-beware-sneaky-sim-swaps.html/amp; and "Vodacom's Results Inflated by Fraudulent Subscriptions," MyBroadband, August 23, 2022, https://mybroadband.co.za/news/cellular/457587-vodacoms-results-inflated-by-fraudulent-subscriptions.html.

38 Tomslin Samme-Nlar, "Cameroon's Fintech Start-Ups' Attitudes Toward and Culture of Cybersecurity," Carnegie Endowment for International Peace, May 19, 2022, https://carnegieendowment.org/2022/05/19/cameroon-s-fintech-start-ups-attitudes-toward-and-culture-of-cybersecurity-pub-87137.

39 Nnenna Ifeanyi-Ajufo, "Digital Financial Inclusion and Security: The Regulation of Mobile Money in Ghana," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/09/19/digital-financial-inclusion-and-security-regulation-of-mobilemoney-in-ghana-pub-87949.

40 "Global Development Finance Coalition Commits Over $5.5 Billion for MSME Financing in Africa," African Development Bank Group, February 16, 2022, https://www.afdb.org/en/news-and-events/press-releases/global-development-finance-coalition-commits-over-55-billion-msme-financing-africa-49250.

41 "Rapport Préliminaire Des Principaux Résultats Du Deuxième Recensement Général Des Entreprises Du Cameroun (RGE-2)." Institut National de la Statistique du Cameroun. Accessed February 6, 2024. https://ins-cameroun.cm/document/rapport-preliminaire-des-principaux-resultats-du-deuxieme-recensement-general-des-entreprises-du-cameroun-rge-2-2/.

42 "Growing Resilient MSMEs in Africa for a Sustainable Future," United Nations Development Programme, June 27, 2022, https://www.undp.org/ghana/blog/growing-resilient-msmes-africa-sustainable-future.

43 "Digital Downsides: The Economic Impact of Misinformation and Other Digital Harms on MSMEs in Kenya, India, and Cambodia." Digital @ DAI. Accessed February 6, 2024. https://dai-global-digital.com/digital-downsides-the-economic-impact-of-misinformation-and-other-digital-harms-on-msmes-in-kenya-india-and-cambodia.html.

44 Madhvi Mavadiya, "Future of Fintech in Africa 2023: Cloud Will Open New Doors for the African Fintech Industry," Finextra Research, August 9, 2023, https://www.finextra.com/the-long-read/754/future-of-fintech-in-africa-2023-cloud-will-open-new-doors-for-the-african-fintech-industry.

45 Emmanuel Mwanambali Mungongo, "Benefits and Risks of Bank and Savings Group Partnerships in Tanzania," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2024/01/08/

benefits-and-risks-of-bank-and-savings-group-partnerships-in-tanzania-pub-91327.

46 (2023) Guidance note for digital credit providers - office of the Data Protection commissioner Kenya. In: OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA - ODPC Kenya. https://www.odpc.go.ke/download/guidance-note-for-digital-credit-providers/. Accessed 8 Feb 2024.

47 Licensing of digital credit providers – January 2023. In: CBK. https://www.centralbank.go.ke/2023/01/30/licensing-of-digital-credit-providers-january-2023/. Accessed 8 Feb 2024.

48 Catherine Agbo, "Bank Customers Get N89bn Refund on Failed Transactions in 9 Years – CBN," Twenty-First Century Chronicle, August 6, 2021, https://21stcenturychronicle.com/banks-customers-get-n89bn-refund-on-failed-transactions-in-9-years-cbn.

49 This X user was instrumental in making widely known via social media how to prevent remote SIM swaps: Bravin Yuri, Twitter post, May 30, 2022, 1:43 a.m., https://twitter.com/BravinYuri/status/1531194495588524032.

50 "SABRIC Urges South Africans to #TakeACloserLook This National Cyber Security Awareness Month," SABRIC, October 4, 2021, https://www.sabric.co.za/media-and-news/press-releases/sabric-urges-south-africans-to-takeacloserlook-this-national-cyber-security-awareness-month/.

51 "Social Engineering: What Is Social Engineering," *Learning Center* (blog), Imperva, accessed January 19, 2024, https://www.imperva.com/learn/application-security/social-engineering-attack/.

52 "Cybersecurity Threatscape of African Countries 2022–2023."

53 "INTERPOL Report Identifies Top Cyberthreats in Africa," October 21, 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.

54 Aubra Anthony, "Cyber Resilience Must Focus On Marginalized Individuals, Not Just Institutions," Carnegie Endowment for International Peace, March 13, 2023, https://carnegieendowment.org/2023/03/13/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions-pub-89254.

55 Tomslin Samme-Nlar, "Cameroon's Fintech Start-Ups' Attitudes Toward and Culture of Cybersecurity," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/05/19/cameroon-s-fintech-start-ups-attitudes-toward-and-culture-of-cybersecurity-pub-87137.

56 "Situational Analysis of Digital Security in Cameroon," Internews, September 24, 2021, https://internews.org/resource/situational-analysis-of-digital-security-in-cameroon/.

57 Nnenna Ifeanyi-Ajufo, "Digital Financial Inclusion and Security: The Regulation of Mobile Money in Ghana," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/09/19/digital-financial-inclusion-and-security-regulation-of-mobile-money-in-ghana-pub-87949.

58 Elizabeth Kolade, "Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security," Carnegie Endowment for International Peace, accessed January 19, 2024, https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123.

59 Marta Kuc-Czarnecka, "COVID-19 and Digital Deprivation in Poland," *Oeconomia Copernicana* 11, no. 3 (2020): 415–31, https://ideas.repec.org//a/pes/ieroec/v11y2020i3p415-431.html.

60 Waag-Cowling, "Dividend or Liability?"

61 Robert Dartnall, Kit Palmer, and Wiebe Ruttenberg, "Cyber Threats to the Financial Sector in Africa: An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape," World Bank, March 1, 2022, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099830405172214598/P164770006015307 60af01093740e385fe8.

62 "Sub-Saharan Africa," Cybil Portal (page 2), accessed January 19, 2024, https://cybilportal.org/projects-by/?page=region&_sft_region=sub-saharan-africa&_sft_themes=cyber-security-culture-skills&sf_paged=2.

63 Abraham Augustine, "The Limits of Accelerating Digital-Only Financial Inclusion," Carnegie Endowment for International Peace, July 13, 2023, https://carnegieendowment.org/2023/07/13/

limits-of-accelerating-digital-only-financial-inclusion-pub-90175.

64 Majorie-Chalwe Mulenga, Eric Duflos, and Gerhard Coetzee, "The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence," February 2022, https://www.cgap.org/research/reading-deck/evolution-of-nature-and-scale-of-dfs-consumer-risks-review-of-evidence; and Kate McKee, Michelle Kaffenberger, and Jamie Zimmerman, "Doing Digital Finance Right," June 2015, https://www.cgap.org/research/publication/doing-digital-finance-right.

65 McKee, Kaffenberger, and Zimmerman, "Doing Digital Finance Right."

66 Sarah Corley, "Is Cloud Computing the Answer to Creating a Diverse Digital Finance Ecosystem and Increasing Financial Inclusion?," *Alliance* (blog), August 22, 2023, https://alliancedfa.org/2023/08/22/is-cloud-computing-the-answer/.

67 "Rise of African Cloud Report—2023 Edition," *Xalam Analytics* (blog), accessed January 19, 2024, https://xalamanalytics.com/rise-of-african-cloud-report-2023/.

68 Alexis Akwagyiram, "New Data Centers Are Supercharging Cloud Computing in Smaller African Countries," *SEMAFOR*, June 22, 2023, https://www.semafor.com/article/06/22/2023/data-centers-fuel-cloud-computing-in-smaller-african-countries.

69 Abraham Augustine, "Africa's Cloud Market Is Small but Growing Fast, and Everyone Wants a Slice," *TechCabal* (blog), October 26, 2023, https://techcabal.com/2023/10/26/a-slice-of-africas-appetite-for-cloud/; and "Huawei Mobile Money," Huawei, accessed January 19, 2024, https://carrier.huawei.com/minisite/software/mobile-money/monney.html.

70 Leo Komminoth, "Can Africa Achieve 'Digital Sovereignty' in an Era of Big Tech?," *African Business*, July 21, 2023, https://african.business/2023/07/technology-information/can-africa-achieve-digital-sovereignty-in-an-era-of-big-tech; and Iginio Gagliardone, "A Postcolonial Perspective on Digital Sovereignty," in *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, ed. Steven Feldstein (Washington, DC: Carnegie Endowment for International Peace, 2023), https://carnegieendowment.org/2023/11/29/postcolonial-perspective-on-digital-sovereignty-pub-91079.

71 Shana Warren, "Consumer Protection in Digital Finance Users Survey in Nigeria," IPA, accessed February 6, 2024, https://poverty-action.org/recovr-study/consumer-protection-digital-finance-users-survey-nigeria.

72 Elmarie Biermann, "A Digital Odyssey: The Convergence of Rapid Digitization, Population Dynamics, and Financial Risk in Namibia," Carnegie Endowment for International Peace, April 2, 2024, https://carnegieendowment.org/2024/04/02/digital-odyssey-convergence-of-rapid-digitization-population-dynamics-and-financial-risk-in-namibia-pub-92080.

73 "Regulation for Inclusive Digital Finance—Regulatory Sandboxes," CGAP, accessed January 19, 2024, https://www.cgap.org/topics/collections/regulatory-sandboxes.

74 Regulatory Sandbox by the Intergovernmental Fintech Working Group (IFWG), https://www.ifwg.co.za/Pages/Regulatory-Sandbox.aspx

75 Zimbabwe Fintech Regulatory Sandbox, https://frs.rbz.co.zw/

76 "Social Engineering: What Is Social Engineering"; and Tochukwu Ironsi, "The Evolution of Agency Banking in Africa," *Paystack* (blog), October 5, 2023, https://paystack.com/blog/operations/agency-banking-africa.

77 Ifeanyi-Ajufo, "Digital Financial Inclusion and Security."

78 Peris Mburu, "Agency Banking Transforming Markets and Financial Access: The Case of Fidelity Bank," *FSD Africa* (blog), August 27, 2020, https://fsdafrica.org/blog/agency-banking-transforming-markets-and-financial-access-a-case-of-fidelity-bank/.

79 Arpit Sharma, "How Agency Banking Is a Driving Catalyst in Fostering Financial Inclusion," Panamax, Inc. (blog), June 12, 2023, https://www.panamaxil.com/blog/the-current-scenario-of-agency-banking-in-developing-nations.

80 Josephat Lotto, "The Role of Agency Banking in Promoting Financial Inclusion: Descriptive Analytical Evidence from Tanzania," *European Journal of Business and Management*, 2016, https://www.semanticscholar.org/paper/The-Role-of-Agency-Banking-in-Promoting-Financial-Lotto/

ff6c2ff8c730173c2c1621bca71e79f145e97eb4.

81 David Indeje, "Policy Brief: Kenya's Cybersecurity Capacity Building Needs Outlined," KICTANet, August 2, 2023, https://www.kictanet.or.ke/policy-brief-kenyas-cybersecurity-capacity-building-needs-outlined/.

82 "E-Levy: Telecom Chamber Warns Public against Fraudsters." Adomonline.com, May 9, 2022. https://www.adomonline.com/e-levy-telecom-chamber-warns-public-against-fraudsters/.

83 "Security Challenges of Financial Mobile Apps in Africa." CyLab Report. Accessed February 5, 2024. https://approov.io/info/security-challenges-of-financial-mobile-apps-in-africa.

84 "Anonymous Sudan Launches Cyberattacks on Nigeria's Vital Information Systems," *CyberPlural* (blog), August 3, 2023, https://blog.cyberplural.com/anonymous-sudan-launches-cyberattacks-on-nigerias-vital-information-systems/.

85 "MAUSHIELD – Mauritius Cyber Threat Information Sharing Platform," accessed January 19, 2024, https://maushield.govmu.org/misp/.

86 Nanjira Sambuli, "When the Rubber Meets the Road: Cybersecurity and Kenya's Digital Superhighway," Carnegie Endowment for International Peace, October 12, 2023, https://carnegieendowment.org/2023/10/12/when-rubber-meets-road-cybersecurity-and-kenya-s-digital-superhighway-pub-90766.

87 "Ghana Launches a Platform to Promote Cybersecurity," The Paypers, May 29, 2023, https://thepaypers.com/digital-identity-security-online-fraud/ghana-launches-a-platform-to-promote-cybersecurity--1262813.

88 Cameroon ANTIC, https://www.antic.cm/index.php/en/mssions/computer-security-audit.html#:~:text=CIRT%20centralises%20and%20processes%20requests,incident%20related%20to%20computer%20security.

89 Tomslin Samme-Nlar, "Securing Digital Finance in Post-Conflict Central African Republic," Carnegie Endowment for International Peace, May 22, 2023, https://carnegieendowment.org/2023/05/22/securing-digital-finance-in-post-conflict-central-african-republic-pub-89799.

90 Ghana CERT, https://www.csa.gov.gh/cert-gh.

91 Kenya CIRT, https://www.ca.go.ke/cyber-security#:~:text=The%20National%20KE%2DCIRT%2FCC%20detects%2C%20prevents%20and%20responds,the%2Dclock%20operations%20in%202017

92 Sambuli, "When the Rubber Meets the Road."

93 Nzilani Mweu, "Kenya: Cybersecurity," DataGuidance, March 15, 2022, https://www.dataguidance.com/opinion/kenya-cybersecurity.

94 Namibia CERT, https://www.cran.na/national-security-and-cyber-incidence-response-team/

95 Nigeria CERT, https://nitda.gov.ng/computer-emergency-readiness-and-response-team-unit/

96 "Nigeria: CBN Issues Risk-Based Cybersecurity Framework and Guidelines," DataGuidance, July 18, 2022, https://www.dataguidance.com/news/nigeria-cbn-issues-risk-based-cybersecurity-frameworkon; and Kolade, "Cybersecurity in Nigeria's Financial Industry."

97 South Africa CERT, https://www.cybersecurityhub.gov.za/

98 Tanzania CERT, https://www.tzcert.go.tz/services/

99 *REGULATIONS (Made under Section 165)*. Electronic and Postal Communications (Computer Emergency Response Team) , 2018. https://www.mawasiliano.go.tz/uploads/documents/sw-1687497567-The Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018.pdf.

100 The Postal and Telecommunications Regulatory Authority of Zimbabwe, https://www.potraz.gov.zw/wp-content/uploads/2022/02/2017_POTRAZ_ANNUAL_REPORT.pdf

101 https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9ZIM17008

102 Vusumuzi Maphosa, "An Overview of Cybersecurity in Zimbabwe's Financial Services Sector," *F1000Research* 12 (2023): 1251, https://doi.org/10.12688/f1000research.132823.1.

103 Central Bank of Brazil: https://www.bcb.gov.br/en/financialstability/pix_en

104 National Payments Corporation of India: https://www.npci.org.in/

105 Luca Belli, "Building Good Digital Sovereignty Through Digital Public Infrastructures and Digital Commons in India and Brazil," CyberBRICS (blog), September 11, 2023, https://cyberbrics.info/building-good-digital-sovereignty-through-digital-public-infrastructures-and-digital-commons-in-india-and-brazil/.

106 Kenn Abuya, "Kenya Picks Microsoft As Its Cloud Partner for E-Govt Services, Beating Google and Amazon" TechCabal (blog), November 23, 2023, https://techcabal.com/2023/11/23/kenya-microsoft-cloud-partner/; and "Vodafone and Microsoft Sign 10-Year Strategic Partnership to Bring Generative AI, Digital Services and the Cloud to More Than 300 Million Businesses and Consumers," Vodafone, January 15, 2024, https://www.vodafone.com/news/corporate-and-financial/vodafone-microsoft-sign-10-year-strategic-partnership-generative-ai-digital-services-cloud.

107 "The Digital Transformation Strategy for Africa (2020–2030)," African Union, May 18, 2020, 8, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

108 Alberto Lemma, Maximiliano Mendez-Parra, and Laura Naliaka, "AfCFTA: Unlocking the Potential of the Digital Economy in Africa," ODI, July 13, 2022, https://odi.org/en/publications/afcfta-unlocking-the-potential-of-the-digital-economy-in-africa/.; and Pan- African Payment and stem, https://papss.com/

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org