Access Partnership

Centre for Human Rights, University of Pretoria

July 2024

Elevating Africa's Cyber Resilience:

Unveiling Regional Challenges and Charting AI Solutions

Authors: Access Partnership and the Centre for Human Rights, University of Pretoria

accesspartnership.com

Contents

Elevating Africa's Cyber Resilience

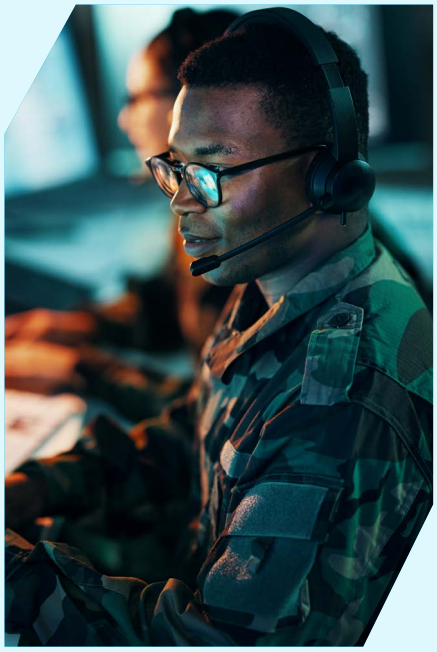
1 Introduction

Look again at the African continent: over two transformative decades, the combined Gross Domestic Product (GDP) has increased more than fivefold. Much of this is driven by increasing internet use to support digital services and enabled by the ubiquity of mobile banking, social networks, and AI-driven processes – from predicting climate changes to improving maternal health outcomes. This drives further optimism, with combined GDP expectations of more than USD 4 trillion by 2027. That qualifies Africa's potential as an economic powerhouse.[1]

And this is true, as Cisco's Executive Vice President Fran Katsoudas cautions, **while 60% of Africans remain unconnected** and so shut out from the global economy and its innovations.[2] For GDP projections to materialize, therefore, African governments and their partners must introduce initiatives that will connect those **700 million unconnected**, and do so at speed. Simultaneously, they must address the most significant threat to effective digital transformation and meaningful accessibility: cybersecurity.

That risk is spread equitably among growth sectors across the continent, but its mitigation turns on the intellectual dexterity, continuous learning, and adaptability of Africa's human resources. The very same qualities that drive entrepreneurialism, from Cairo to the Cape, will also provide effective cybersecurity across these diverse and innovative economies.

This study demonstrates clearly that people and skills remain central to mitigating Africa's cybersecurity threat and to scaling her cybersecurity defenses over the long term. While trusted technology is an indispensable component of this continuous campaign, other key support will come from policymakers. By relying heavily on representatives from an open, collaborative, multistakeholder process—including trusted industry participants, academia, and civil society partners who have adopted a considered, ethical, and fair approach to digitalization—policymakers will be instrumental in both innovating and continuously reinventing solutions to address the continent's enduring challenges.



1.1 Global Context: Cybersecurity as a Shared Threat

The evolving threat landscape, resource challenges, and complexity of networks and applications are a significant burden on today's organizations even in the most advanced economies. Globally, 2023 alone saw over 2,800 publicly disclosed data breaches, involving the theft of over 8.2 billion records.[3] And this represents just the tip of the iceberg, as countless more data breaches occur in lesser-known organizations. When assessing

the overall cybersecurity readiness of over 8,000 businesses across 30 global markets, Cisco's Index found that **only 3% of respondent organizations fall into the "Mature" (ready) category.**[4]

The International Information System Security Certification Consortium (ISC2) Cybersecurity Workforce 2023 Report clarifies pressing challenges in the cybersecurity sector, which include economic uncertainty, technological advancement (or not), regulatory fragmentation, and widening skills gaps. It counts a global cybersecurity workforce of 5.5 million in 2023, a 9% increase from 2022, and the highest recorded to date.[5] According to the World Economic Forum's Strategic Cybersecurity Talent Framework the global talent shortage is projected to reach 85 million workers by 2030, causing an estimated $8.5 trillion in unrealized annual revenue. In the cybersecurity sector alone, there is an **urgent need for nearly 4 million professionals to bridge the talent gap**.[6] What is evident from both studies, is that there is a rising demand for cloud computing security and AI/machine learning skills, indicating an anticipated shift in cybersecurity skill requirements as technology evolves.

1.2 Africa's Cybersecurity Landscape

If cybersecurity is a global challenge, Africa is confronted with the most significant impact from cyber threats of any continent,[7] and the consequences are measurable. Cybercrime slashed Africa's GDP by over 10% in 2021, amounting to approximately USD 4.12 billion in losses.[8] The frequency and complexity of cyberattacks have surged, presenting a significant obstacle to continental socio-economic development: in the second quarter of 2023, Africa witnessed its highest average number of cyberattacks per week per organization (fully 2164 attacks), a 23% increase compared to the same period in 2022.[9] Compounding the complexity is the proliferation of cyberattacks which outpaces response mechanisms such as the development of robust regulatory frameworks and the cultivation of proficient human resources, to counter such threats.

Critical information infrastructure therefore remains vulnerable to exploitation, posing threats to not only national security but also economic prosperity. According to a 2023 study by Positive Technologies, the most targeted organizations were in the financial sector (18% of attacks), followed by telecommunications companies (13%), government agencies (12%), and organizations in the trade (12%) and industrial (10%) sectors.[10] This reality is not not lost by international investors or national leadership. Rwanda's long-serving president and longtime champion of digitalization presents a simple trade-off, having made clear that Africa cannot take full advantage of the digital revolution "until data is stored in safe and trusted

systems that protect privacy and are difficult for criminals to breach."[11] Failure to counter these cyber threats can have serious consequences for individuals, businesses, and the socio-economic development of the continent."

So recognition grows of cybersecurity's importance among African nations, which drives some collaboration and establishment of dedicated units to address cybercrime and breaches. However, long-term solutions demand a workforce with advanced expertise in cyberspace that is able to analyze cybercriminal motivations, apprehend offenders, and devise the preventive strategies essential to leveraging the digital revolution.

Africa's unique cyber-related skills deficit (people) highlights technological transformations impacting infrastructure and systems (technology) and shows how current policies, rules, and laws (policy) offer necessary but as yet insufficient recourse to Africa's cybersecurity challenges. For each challenge identified, however, there are actionable solutions.

2 People: Strategies for Overcoming Africa's Cybersecurity Skill Gap

2.1 The Challenge: Confronting Digital Literacy, Cyber Talent Gaps, and AI Education

Scholars, including Assane Gueye, co-director of CyLab-Africa, highlight five cybersecurity challenges specific to Africa. Digital illiteracy, especially prevalent in rural areas, hampers personal data protection amid rapid digital technology growth like mobile money. The severe shortage of cybersecurity professionals is exacerbated by limited training programs.[12] Even with a combined population of 280 million people, as of 2023, Nigeria stood at 8,352 cybersecurity professionals, while South Africa recorded 57,269.[13] Compared to the US, with a cybersecurity workforce of 482,985 cybersecurity, and Brazil, with 231,921, it becomes clear how far the continent lags behind even by this simple metric. [14]

Figure 1:
4 Cybersecurity challenges unique to Africa

Lack of tested security measures
Black-hat hackers are taking advantage of vulnerabilities

Digital illiteracy
Many users, especially in rural areas, do not know how to keep their data secure or recognize phishing threats

Hidden costs of aging infrastructure
Critical infrastructure is increasingly dependent on technology that is too outdated to patch or secure effectively

Lack of security professionals
There are not enough cybersecurity training programs to build a trusted digital future

Note: Learn how Carnegie Mellon University experts are working to address these challenges to ensure trusted financial technology on the continent: africa.engineering.cmu/cylab-africa

But this digital literacy gap is especially pronounced among African women in Africa: not least because they generally have limited access to internet-based technologies compared to men.[15] This suggests that women are also missing out on employment opportunities in an economy that is becoming increasingly digital. Predictably, their representation in cybersecurity-related professions is highly limited: **only 9% of cybersecurity professionals in Africa were women as of 2021,**[16] - significantly lower than the global average of 25%.[17]

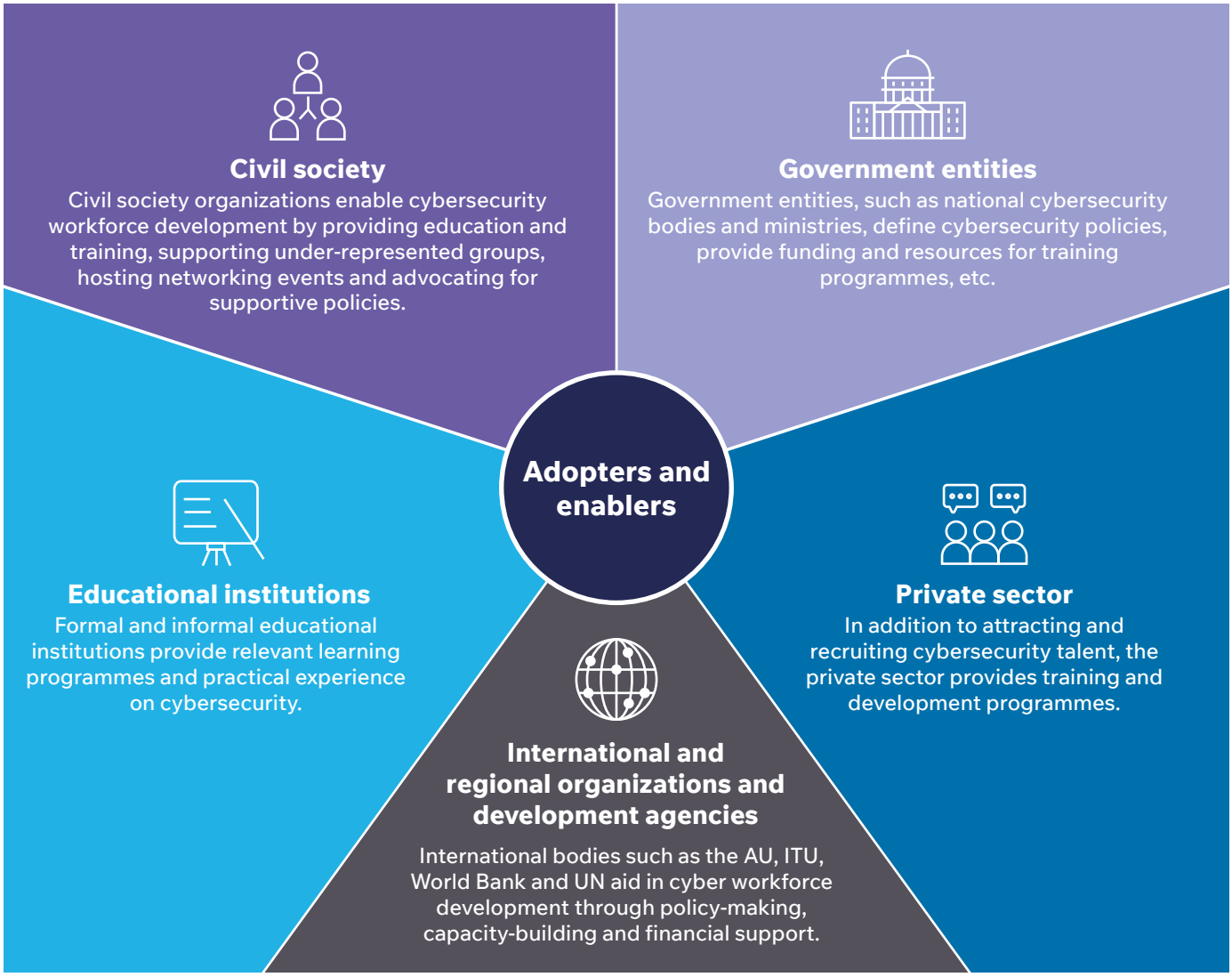
By 2030, AI applications in sub-Saharan Africa, including Ghana, Kenya, Nigeria, and South Africa, are projected to generate an economic value of USD 136 billion, surpassing Kenya's current GDP.[18] This growth presents an unprecedented opportunity to lower barriers to entry and expand opportunities for under-utilized populations, addressing skills gaps and unfilled cyber roles. However, challenges such as social and digital disparities, limited access to education, and inadequate digital infrastructure impede equitable AI adoption. To unlock the full potential of AI, targeted improvements are essential. Mudongo's research highlights these existing obstacles, emphasizing the urgency

of addressing infrastructure gaps and fostering a skilled workforce.[19] Through strategic initiatives and policies, AI has the potential to empower under-represented groups, providing them with the skills and opportunities needed to participate in the digital economy. This can lead to a more inclusive and diverse workforce, capable of driving innovation and addressing the region's most pressing challenges.

2.2 The Solution: Building Skills Bridges Through Public and Private Sector Collaboration

Education underpins Africa's digital progression, a fact related to its youthful population. Moreover, private sector partnerships have an essential role to play in tackling Africa's cybersecurity skills deficit, deploying their resources, expertise, and ability to scale initiatives effectively. Collaboration between private sector organizations such as Liquid Intelligence Technologies (providing innovative technology solutions), Oracle (who offer expertise in cloud computing and infrastructure solutions), and Cisco (with its Networking Academy providing IT and cybersecurity courses), along with institutions of higher learning, are necessary to equip professionals with relevant skills.

For instance, The Networking Academy, offered by Cisco, provides a diverse range of IT and



The World Economic Forum's Enablers of Cybersecurity Talent Framework 2024

cybersecurity courses, including 11 free, online, self-paced courses such as "Introduction to Cybersecurity" and "Programming Essentials in Python."[20] Nearly 3 million students attribute their job success to the program's courses, underscoring its profound impact on career opportunities. In Nigeria, Cisco's Networking Academy has provided training to more than 400,000 individuals in digital and cybersecurity skills. This dedication to education extends beyond Nigeria's borders, with Cisco committing to training 3 million people across Africa in digital and cybersecurity skills. Fran Katsoudas underscores the significant impact of the Networking Academy, which has empowered over 1.5 million learners across Africa, including 466,000 women.[21]

Collaborations with the private sector further support professionals in attaining certifications,

There are ongoing initiatives to tackle the digital gender gap in the African continent. These include specialized STEM education programs tailored specifically to empower women, crucial for their involvement in cyber and digital professions.[27]

One notable initiative that could serve as a model for other African countries is South Africa's KnowBe4, which is one of the world's largest security awareness training and simulated phishing platforms, and which recently launched the "KnowBe4 Women in Cybersecurity Scholarship."[28] This scholarship targets women of color and is being conducted in collaboration with the Centre for Cyber Safety and Education. Siemens has partnered with UN Women Germany to launch the African Girls Can Code Initiative (AGCCI). AGCCI upskills and empowers young African women with digital literacy, programming, and work-readiness skills. The program targets girls and young women aged 17 to 25 in South Africa, Kenya, Senegal, Rwanda, and Uganda.[29]

There are also inspiring examples of women breaking barriers and making significant contributions to cybersecurity in Africa. Dr. Dorcas Muthoni, founder, and CEO of OPENWORLD Ltd, is a prominent figure in Kenya's cybersecurity landscape, advocating for gender diversity in the industry.[30] Fatoumata Ba, founder, and CEO of Janngo Capital, is spearheading initiatives to empower women in technology across Africa, including cybersecurity.[31] Gender inclusion is not just a matter of advancement but also serves the overall security and resilience of digital ecosystems in Africa.

facilitating skill enhancement, and bridging the cybersecurity workforce gap.[22] Certifications are essential for cybersecurity professionals, showcasing their dedication to skill enhancement despite economic challenges. Even amid corporate cutbacks, over half of professionals receive employer support for certification exams, aiding in addressing the skills gap.[23]

These partnerships not only benefit students but also enhance universities' reputations for producing job-ready graduates. Private organizations, in turn, influence cybersecurity curricula, shaping the skills of future professionals and streamlining the hiring process. By fostering a skilled cybersecurity workforce, these partnerships contribute to meeting the growing demands of the industry and driving sustainable economic growth across Africa.

2.3 Opportunity: How Cybersecurity Skills Transfer Secures Africa's Key Sectors

Carnegie Mellon University Africa shows in simple terms how financial inclusion and cybersecurity resilience in Africa intersect: over 50% of organizations express uncertainty in the effectiveness of their cyber incident response teams (despite experience with cybercrime incidents[24]). Even where there are relatively higher percentages of proficient cyber skills, financial services, and public administration face acute demand.[25] Recognizing the severity of the cybersecurity skills deficit, 55% of African organizations intend to recruit skills next year. Meanwhile, small-and-medium enterprises (SMEs), crucial to the African economy and which contribute about 50% to the total sub-Saharan GDP, could be significantly affected if they integrate AI into SME operations. This could significantly impact overall economic growth, but not integrating AI would dampen growth more, which highlights the need for an enabling environment to support their digital transformation.[26]

Case Study Box: Kenya - Partnership between Strathmore University and Fortinet Security Academy

Context: Strathmore University partnered with Fortinet, a global cybersecurity solutions provider, to offer cybersecurity training to students. The collaboration aimed to address the increasing demand for cybersecurity professionals in Kenya's job market.

Approach: Strathmore University integrated Fortinet's cybersecurity curriculum into its academic programs, equipping students with industry-relevant skills. By leveraging Fortinet's expertise and resources, the university sought to enhance its cybersecurity education offerings and maintain its position as a leader in the field.

Impact: The partnership likely empowered students with practical cybersecurity knowledge and skills, making them more competitive in the job market. By being the first university in Kenya to join Fortinet's Security Program, Strathmore University potentially gained a competitive advantage in attracting students interested in cybersecurity education.

3 Technology: Understanding the Vulnerabilities and Opportunities

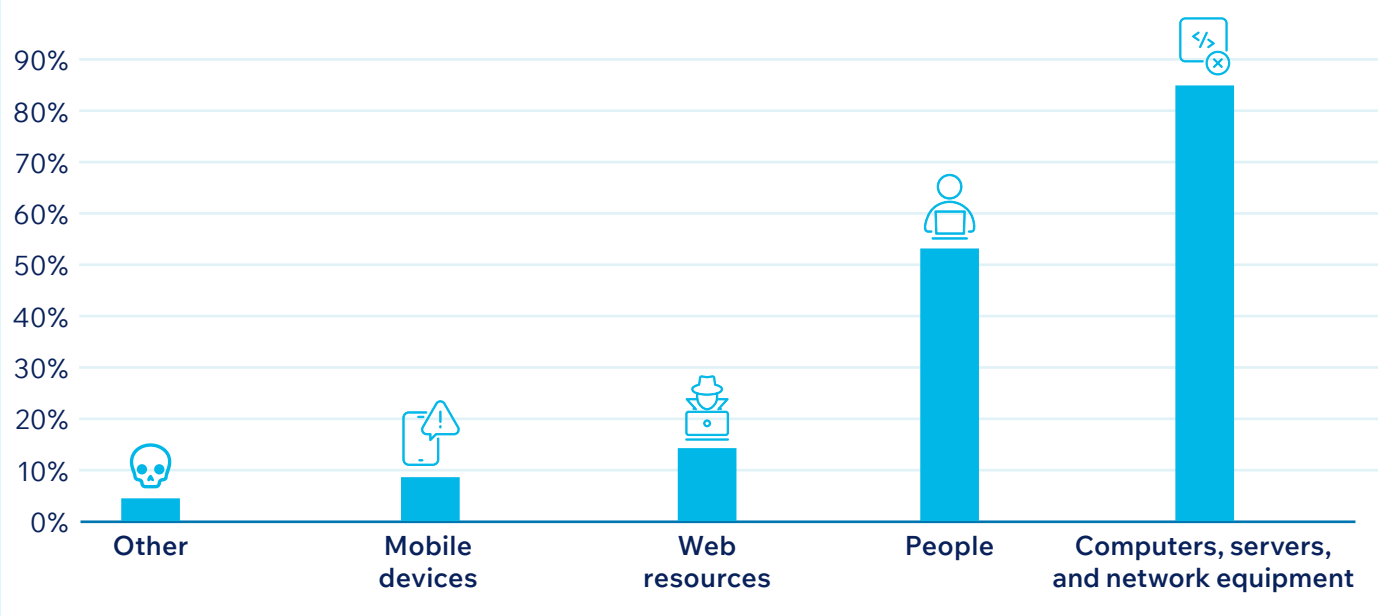
If new technologies create enormous potential in Africa, cyber attackers are intensifying their focus on critical infrastructure and harnessing artificial intelligence (AI) to fuel their malicious activities. Maher Yamout, lead security researcher at Kaspersky, highlights how threat actors are exploiting AI large language models (LLMs) to orchestrate sophisticated social engineering attacks across multiple languages. This trend underscores a concerning rise in attacks, fueled by the accessibility of AI technologies, which enable cybercriminals to craft convincing phishing emails, synthetic identities, and deepfakes, exacerbating existing inequalities. Rachel Adams, a principal researcher at Research ICT Africa, warns of the real and potential threats posed by AI technologies to societies, underscoring the urgent need for vigilance and proactive measures to safeguard against cyber threats in Africa.[32]

The rapid development of technologies such as 5G, robotic process automation, and generative AI opens up new prospects for cyberattacks and data breaches. However, equally so, technologies to combat the observed growth in cybercrime are available for the continent to utilize.

3.1 Cybersecurity Vulnerabilities

The financial sector in Africa has been the heaviest hit by cyberattacks, with **cybercriminals targeting 85% of their attacks on computers, servers, and network infrastructure.** Web resources become the target in 15% of attacks, often resulting in successful DDoS attacks.[33] Below is a full breakdown of the most prevalent targets:

Figure 2:
Targets of attacks (percentage of successful attacks)



In 2023, attackers of these targets used malware in four out of every five successful attacks on organisations. Every second incident involved social engineering and in each tenth case, attackers were able to gain access to the organization's resources by compromising credentials. For example, in South Africa, 94% of organizations were targeted by phishing attacks.[34] Interpol also identifies social engineering as one of the region's major risks. Attackers use a variety of social engineering techniques, automated tools, and spam bots to improve their chances of success. With inadequate cybersecurity knowledge among users, the risks associated with phishing attacks in Africa remain extremely high. According to assessments by KnowBe4 researchers of employee knowledge in African organizations, one out of every three employees clicks on a phishing link or follows an attacker's request.[35]

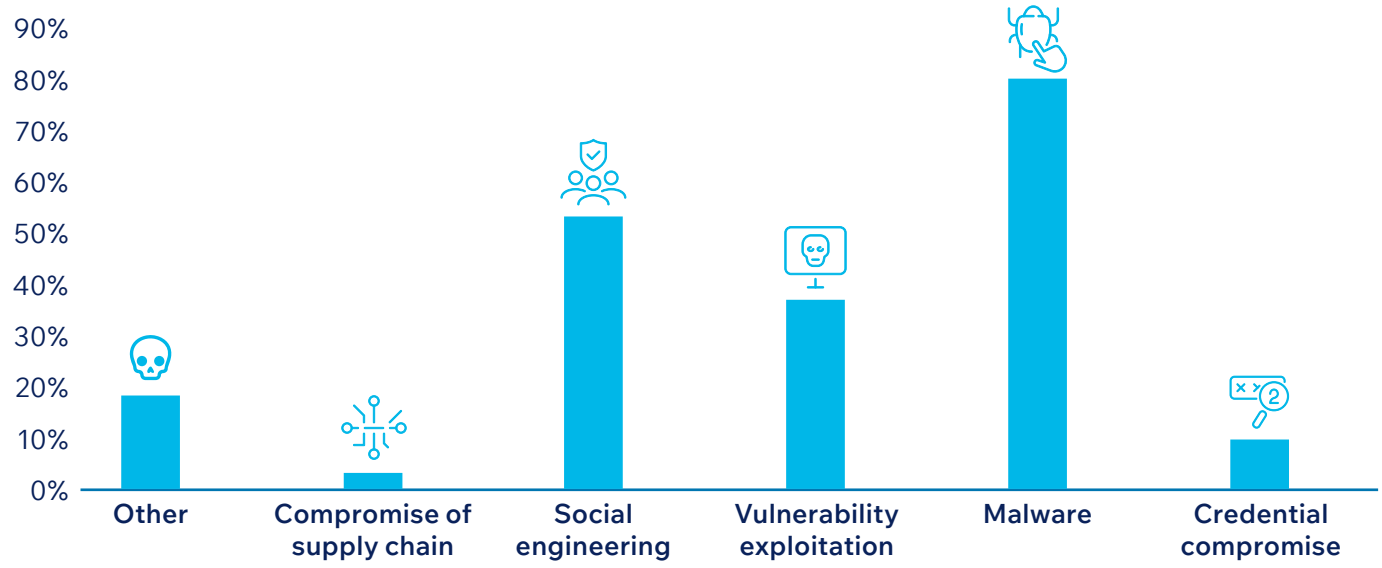
In April of 2023, the BlackCat group launched an attack on the internal network of the African Union headquarters, infecting approximately 200 PCs, just ten days after the organization's annual heads-of-state summit. It took experts from Interpol, Afripol, and the African Bank intervened to restore the systems.[36]

3.2 Innovative Solutions: Technology's Role in Preventing Cybersecurity Breaches

Cyberattacks take various forms, each with its own scale of consequences, so it is necessary to understand the technology used in these attacks to determine what technology is needed to counter them. The most crucial counter technologies are outlined below.

- **Encryption and Cryptography:** Encryption and cryptography serve as vital defences against unauthorized access and data breaches. Encryption encodes data to ensure confidentiality, typically using encryption keys, safeguarding data during transit over networks like the Internet or mobile devices. Cryptography verifies data integrity through hash functions, enabling secure authentication mechanisms like SSL/TLS for web browsing and bolstering trust between parties. In Africa, where data privacy concerns are heightened due to limited frameworks, encryption plays a crucial role in protecting sensitive information across sectors like finance, healthcare, and government, ensuring data security amid increasing digitization and cyber threats.

Figure 3:
Attack methods (percentage of successful attacks)



- **Security Information and Event Management (SIEM) Systems:** SIEM systems provide comprehensive monitoring solutions, detecting, and responding to security incidents by aggregating and analyzing data from various sources. These systems offer essential visibility into cyber threats, facilitating timely incident response, particularly for organizations with limited cybersecurity resources. Leveraging advanced analytics, SIEM enables real-time threat detection, minimizing the impact of cyberattacks. Additionally, SIEM supports forensic investigation and root cause analysis by providing detailed logs and historical data. In the African context, SIEM systems are invaluable for organizations seeking to enhance their cybersecurity posture and comply with regulatory requirements, despite the need for infrastructure investment and skilled personnel. Their ability to provide comprehensive threat detection and incident response capabilities makes them a top choice for bolstering cybersecurity resilience.

- **Cloud computing:** Cloud computing technology offers significant advantages in cybersecurity, including scalability and flexibility to adapt resources according to demand, effectively addressing dynamic security requirements. It facilitates centralized security management, consolidating controls across applications and network environments, overcoming on-premises infrastructure limitations. Additionally, cloud-based security tools leverage advanced threat detection technologies like machine learning for real-time identification and response to emerging threats. Moreover, built-in resilience and disaster recovery capabilities minimize downtime, enhancing organizational resilience against cyberattacks. In Africa, where infrastructure challenges persist, cloud computing technologies enable the consolidation of controls across applications and networks, mitigating limitations of on-premises infrastructure.

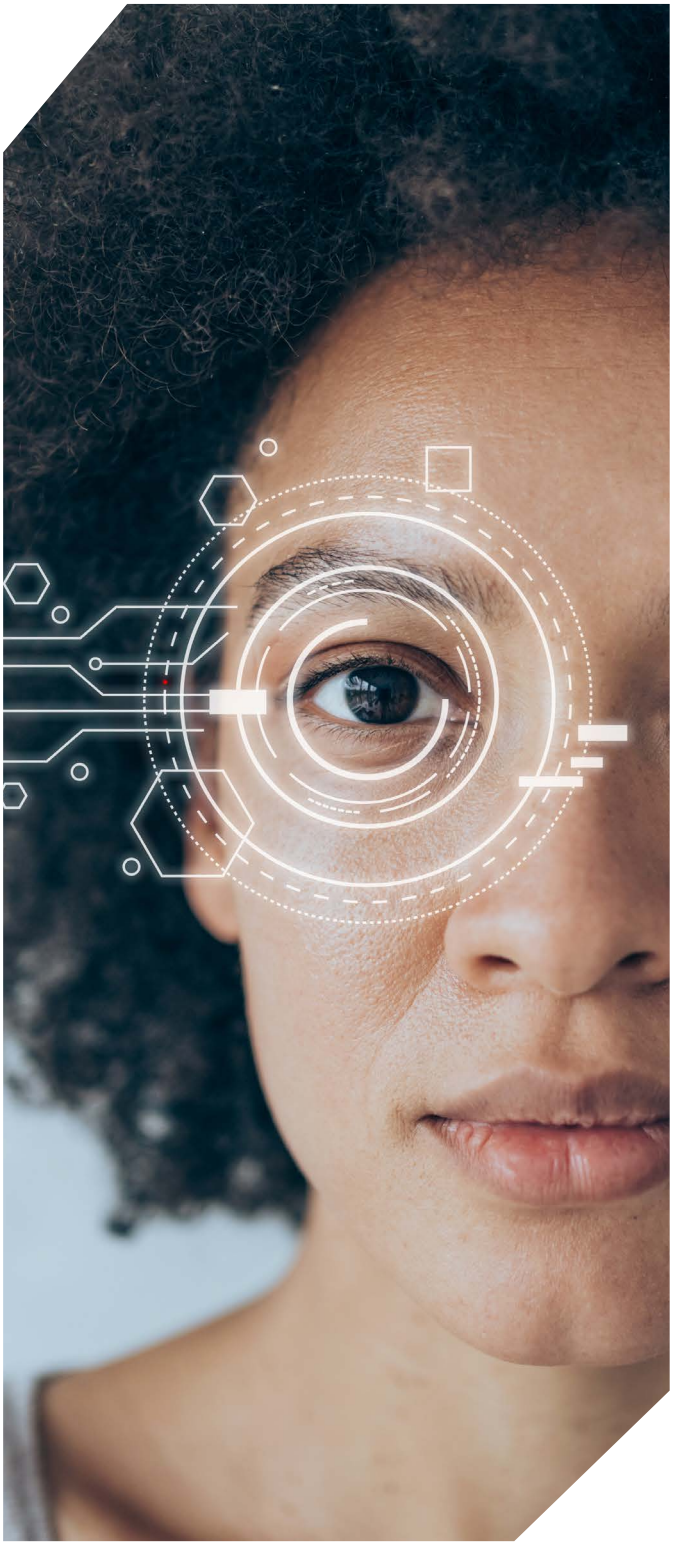
- **Artificial Intelligence (AI) and Machine Learning (ML):** This empowers organizations by leveraging algorithms to analyze extensive datasets, identifying patterns that signal potential security breaches or malicious activities. Through machine learning and deep learning techniques, AI systems enable real-time detection, prevention, and response to cyber threats, significantly enhancing human capabilities in threat detection and incident response. This technology also plays a crucial role in simplifying cybersecurity operations by automating routine tasks such as malware detection and vulnerability assessment. In Africa, where resource constraints are common, AI offers scalable solutions that align with operational needs and budget limitations, overcoming the shortage of skilled cybersecurity professionals. By reducing complexity and automating processes, AI not only strengthens defenses against evolving cyber threats but also democratizes access to sophisticated cybersecurity technologies, fostering a more secure digital environment across the continent.

- **Biometrics and Multifactor Authentication:** Biometrics and MFA (Multi-Factor Authentication) technologies authenticate users based on unique physiological or behavioural characteristics, such as fingerprints, enhancing access control and identity management. In Africa, where traditional authentication methods may be vulnerable to impersonation or theft, biometrics and MFA strengthen authentication processes, safeguarding sensitive systems and data. Biometric authentication improves user experience by eliminating complex passwords, while MFA adds an extra layer of security by requiring multiple forms of identification. This mitigates risks of credential theft and phishing attacks, reducing successful access attempts and enhancing cybersecurity resilience. In regions with low digital literacy or high rates of identity fraud, such as Africa, biometric technologies like fingerprint and facial recognition provide secure and convenient authentication methods. Kenya's recent national digital identity project is a notable example of addressing identity fraud issues through biometric authentication.

- **Zero Trust:** In countries where data privacy concerns are heightened due to limited frameworks, Zero Trust architecture presents a

critical strategy for enhancing cybersecurity. Zero Trust operates on the principle of not trusting any entity by default, whether inside or outside the network perimeter. Instead, it verifies every request and access attempt regardless of location, requiring strict identity verification and continuous authentication. This approach is particularly relevant in sectors such as finance, healthcare, and government, where sensitive information must be safeguarded against cyber threats. By implementing Zero Trust, organizations can mitigate the risk of unauthorized access and data breaches, ensuring robust protection of valuable data assets amidst increasing digitization. This proactive security model not only strengthens defenses against evolving cyber threats but also fosters trust and reliability in digital interactions across the continent.

Each of these technologies addresses specific cybersecurity challenges in Africa by providing innovative solutions tailored to the region's needs, infrastructure limitations, and socio-economic factors. By effectively leveraging these technologies, Nigeria, Kenya, Ghana, and South Africa can bolster their cyber resilience and defend against evolving cyber threats. Crucially, careful consideration must be given to determining the most suitable technology for specific regions or scenarios for it to be effective, and citizens capacitated to use them.



4 Policy: Effectively Regulating Cybersecurity Challenges

4.1 Existing Cybersecurity Policies and Frameworks

Continental and Regional Initiatives

While cybersecurity legislation has been enacted by a majority of African countries, the absence of a harmonized approach creates its own risk, particularly in the face of growing inter-African trade and travel spurred by the progress of the African Continental Free Trade Area (AfCFTA) agreement. There are some initiatives towards alignment:

- **The Malabo Convention:** The Malabo Convention is the African Union (AU)'s cybersecurity protocol. Only 15 countries have adopted the framework.[37] The AU's Peace and Security Council of the African Union is hard at work, forging the Continental

Overview of Cybersecurity Policies in Africa. Source: Access Partnership 2024

Cybersecurity Strategy.[38] This strategy provides cybersecurity protocols against cyber threats.

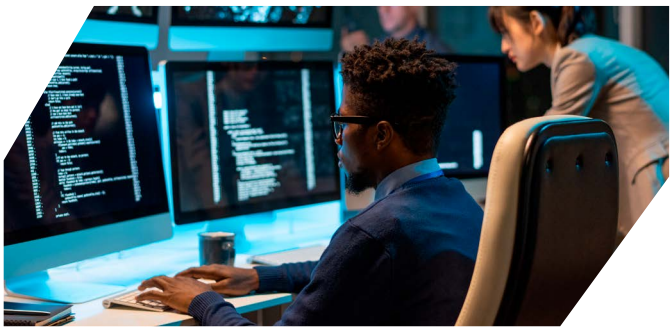
- **Global Alliances:** The Budapest Convention's Role: In tandem with the Malabo Convention, Africa has aligned with the Budapest Convention,[39] the global gold standard in the fight against cybercrime. 12 African countries have become parties that have adopted, signed, or been invited to partake in the convention.

- **Regional Frameworks:** African regional economic communities (RECs) are making progress in promoting cybersecurity-related policies and programs. For instance, ECOWAS,[40] ECCAS,[41] EACO, COMESA, and SADC have implemented policies to promote cooperation, information-sharing, and harmonizing protection measures.[42]

Although, at a foundational level, Africa finally has a regional cybersecurity framework, the concerns outweigh the promise it provides: only 28% of the continent have ratified the Malabo Convention, and even then, because it took almost a decade to reach the minimum number of signatures for the convention to enter into force, the extent of its implementation is questionable. An immediate challenge for the convention will be the varying rates of adoption, further complicated by how it lines up with individual countries' laws on cybersecurity and data protection.

In examining the cybersecurity provisions of the African Continental Free Trade Area (AfCFTA), it is evident that the current framework is insufficient. The digital protocols lack references to "risk-based" approaches to cybersecurity and fail to include commitments from the Member States to adopt these approaches, focusing solely on the private sector. This oversight limits the effectiveness of the cybersecurity measures within the AfCFTA. To address these shortcomings, it is crucial to align national and regional frameworks with risk-based standards developed through open, collaborative, multi-stakeholder processes.

The United States-Mexico-Canada Agreement (USMCA) makes explicit reference to the need for interoperable risk-based approaches for managing



cyber threats. This agreement emphasizes regulatory consistency, capacity building, and fostering public-private partnerships, all while ensuring robust data protection and privacy. Such a holistic and integrated approach can serve as a blueprint for cybersecurity policy within the AfCFTA.

By emulating the USMCA, the AfCFTA can aspire to adopt comprehensive risk-based strategies and commitments from all parties involved. This would include:

1. **Regulatory Consistency:** Establishing uniform cybersecurity regulations across member states to ensure a cohesive defense strategy.

2. **Capacity Building:** Investing in the development of cybersecurity skills and infrastructure across the continent to enhance resilience.

3. **Public-Private Partnerships:** Encouraging collaboration between government bodies and the private sector to share threat intelligence and resources.

4. **Robust Data Protection and Privacy:** Ensuring that data protection laws are up-to-date and effectively enforced to protect against cyber threats.

Such an approach would significantly improve the effectiveness of cybersecurity measures within the AfCFTA, ensuring that both public and private sectors are adequately prepared to address and mitigate cyber threats. But, this also suggests an urgent need for enhanced commitment, participation, and regional collaboration to aid in national alignment and implementation of regionally enforceable frameworks.

National Policies

Thirty-nine of fifty-four African nations have implemented cybersecurity legislation, a mark of the continent's progress and a demonstration of a regionalized desire to safeguard citizens and businesses. Nonetheless, seven African countries - Mauritius, Egypt, Tanzania, Ghana, Tunisia, Nigeria, and Morocco - rank among the top 50 countries with the highest cybersecurity indices, according to the ITU Global Cybersecurity Index.[43] Even in these advanced economies, there is a lack of technical capacity among law enforcement, inadequate regulation enforcement, a need for alignment with global cybersecurity strategies, and socioeconomic factors that actively foster cybercrime. Addressing these challenges requires increased cybersecurity awareness, regulatory compliance, resource allocation, and international cooperation to enhance cybersecurity resilience across Africa.[44]

The table below outlines the frameworks from a selection of countries in the various sub-regions that enjoy different levels of digitalization.

Kenya

Recognizing the urgent need to combat the burgeoning cyberthreat, Kenya's approach to tackling cybercrime has incorporated legislative and policy interventions. The revised Information, Communications, and Technology (ICT) Policy of 2019 explicitly acknowledges cybercrime and cybersecurity vulnerabilities as formidable obstacles hindering the nation's progress.[45] Kenya also unveiled its National Cybersecurity Strategy for the period 2022-2027, underscoring cybersecurity as a paramount national priority.[46]

Despite commendable legislative and policy efforts, the journey toward effectively tackling cybersecurity challenges in Kenya remains arduous. Mitigating cyber threats in Kenya's context requires multifaceted strategies, particularly the nurturing of skilled cybersecurity skills and heightened public awareness of cybersecurity as a risk to public safety.

	Identity	Devices	Network	Application	Data
Kenya	National Cybersecurity Strategy,2022	Computer misuse and cybercrime (Critical Information Infrastructure and Cybercrime Management Regulations 2024	Computer Misuse and Cybercrimes Act 2018 ('Cybercrime Act')	National Digital Masterplan 2022-2032	The Data Protection Act, 2019
Nigeria	National Cybersecurity Policy 2021	Cybercrimes Act 2015			Data Protection Act 2023
South Africa	National Cybersecurity Policy Framework 2015	Electronic Communications and Transactions Act 25 of 2002 Cybercrimes Act, 2020			Protection of Personal Information (POPI) Act of 2013
Cote d'Ivoire	Cybercrime and Cybersecurity Bill 2017	National Cybersecurity Strategy 2021-2025			Law no. 2013-450 on the protection of personal data
Morocco	Cybercrime Law 07-03 Law 05-20 Cybersecurity		Cybersecurity strategy 2021		Data Protection Law 2009
Ghana	Cybersecurity Act, 2020		National Cyber Security Policy & Strategy 2014		Data Protection Act, 2012

Table of Cybersecurity Policies and Frameworks. Source: Access Partnership 2024

Nigeria

Nigeria's emergence and growth as a technology hub has come hand in hand with an uptick in cybercrimes that encompasses a growing cohort of victims and perpetrators.[47] In 2023, the Nigerian senate (the upper chamber of Nigeria's bicameral legislature) confirmed an annual loss of USD 500 million attributed to cybercrimes within its borders.[48]

Despite the foundational role played by Nigeria's Cybersecurity Act, it will need updating and enhancing to include the establishment of clearer penalties and stronger cybersecurity architecture. Moreover, while the Act has served as a deterrent, it has fallen short in forestalling vulnerabilities within vital institutions such as banks.[49] Complications in real-time coordination have complicated early detection and prevention, while instances of rogue elements of law enforcement agencies exploiting the law to target young individuals or colluding with perpetrators are also a matter of record.[50]

South Africa

South Africa lacks a cybersecurity framework that is either comprehensive or specialized. Cybersecurity is addressed through various adjacent frameworks, but there remains an urgent need for further action to tackle cybercrime, particularly in light of its alarming surge and the consequential impact on the economy. According to the South African Council for Scientific and Industrial Research's 2023 briefing, cybercrime inflicts an estimated ZAR 2.2 billion (USD 120 million) worth of damage annually on the economic landscape.[51]

Ghana

Ghana has been progressing in addressing cybersecurity vulnerabilities with various initiatives and campaigns such as the CISAB Vigilance First Campaign. The Ghanaian Cyber Security Authority (CSA) is advocating for robust cybersecurity measures, including multi-factor authentication (MFA), to enhance defense efforts, especially in financial security.[52] However, despite these efforts, the reported cybercrime cases have significantly increased, resulting in over USD 200 million in losses annually. More than half of these cases are related to online fraud.[53] These statistics highlight the need for continued vigilance and efforts to improve cybersecurity measures to combat the rising threat of cybercrime.

Cote d'Ivoire

In December 2021, the government implemented a National Cybersecurity Strategy to enhance cyberspace security and support digital transformation efforts – which it is still currently implementing. The CSRIT team has been instrumental in these efforts, apprehending a number of cyber criminals and even assisting neighboring countries in capturing them.[54] However, cybercrime in the country is still rampant, especially in financial services.[55]

Morocco

Weak institutional frameworks, including insufficient judicial capability and fragmented legislation, contribute to ineffective enforcement and operational inefficiency in Morocco. As a result, cyber incidents are on the rise, with a reported increase of 8% between 2022 and 2023,[56] highlighting the urgent need for robust and proactive cybersecurity measures.

4.2 Developing a Harmonized Digital Ecosystem

The hurdles in adopting unified AI, data protection, and cybersecurity frameworks across Africa are significantly shaped by varied regulatory landscapes, infrastructural deficits, economic variances, pronounced skill gaps, and the sporadic enforcement of privacy legislation among its nations. These are further intensified by differing stages of development, impacting the ability to invest in cutting-edge technologies. While initiatives like the African Union's Malabo Convention aim for norm harmonization, the realization of continent-wide standardization demands massive investment in infrastructure, educational programs, and legal systems, all requiring heightened regional and continental cooperation to meet Africa's distinct necessities. Moreover, the lack of political willpower and the slow ratification of essential conventions underline

a critical need for bolstered coordination against the backdrop of evolving cyber threats. Addressing these issues is crucial for a secure and cohesive technological landscape in Africa.

For Africa to establish a robust and resilient digital ecosystem, it is essential to boost political resolve to enact cybersecurity measures, hasten the adoption of vital agreements, enforce cybersecurity laws, invest in necessary infrastructures, tools, and skills enhancement and elevate awareness and education on the matter. With cyber threats rising, fostering collaboration across legislative, judicial, and civil bodies, regulators, and industry stakeholders is paramount in bolstering cybersecurity resilience and effectively confronting emerging challenges. This is vital for protecting the continent's digital domains and attracting international investments by ensuring a secure operational environment.

4.3 Contextualizing International Best Practice for the African Ecosystem

Developing more tailored cyber risk management solutions in Africa is crucial for addressing national cybersecurity challenges and incorporating global technological best practices should be a part of this. Given the rapid evolution of technology and cyber threats, a dynamic regulatory framework is essential, though African nations would be well-served by collaborating to establish a comprehensive regional approach to cybersecurity that aligns with international standards.

There are sources of inspiration: alignment with international guidelines will naturally lead to a risk-based approach to policymaking. By implementing established models such as the EU's Network and Information Security Directive (NIS 2), NIST's AI Risk Management Framework (AI RMF), and ISO/IEC 27001, entities are compelled to proactively identify, assess, prioritize, and mitigate AI-related cybersecurity threats.[57] Such alignment ensures that resources are allocated efficiently, addressing the most critical threats first and enhancing the overall security posture of local organizations. For example, the NIST framework's guidelines on risk assessment

can be used to identify potential vulnerabilities in AI models, such as adversarial attacks and data poisoning, and implement appropriate mitigation measures - guidance which, as we have identified, is lacking in most local legislation.

Even well-established principles can provide valuable guidance in safeguarding information systems and data, particularly in addressing cyber incidents of international concern. By adopting non-sector-specific best practice from leading global frameworks, African policymakers can ensure that their legislation remains relevant despite evolving cyber risks.

There is additional cybersecurity value in policymaking that fosters international cooperation, exemplified by mechanisms like the World Trade Organization (WTO)'s Information Technology Agreement (ITA). The ITA abolishes customs duties on over 97 percent of ICT products traded globally, benefiting the 82 signatory countries.[58] Among these signatories, only Egypt and Morocco represent African nations. However, numerous African countries could enhance their cybersecurity infrastructure by gaining access to more affordable equipment, including quality computers, semiconductors, data storage media, software, and telecommunication apparatus, through participation in such agreements.

As a global challenge, Africa can tap into international resources to address its needs, such as the African Growth and Opportunity Act (AGOA) and

the Millennium Challenge Act (MCA) Modernization Act, which aim to enhance economic development, trade, and investment. Of MCC's 41 signed compact grant agreements, 22 have been with sub-Saharan African countries, totaling over $8 billion. While these initiatives create opportunities, policymakers have yet to fully utilize the potential for knowledge-sharing and technical assistance in cyber defense. Modernizing AGOA, rather than simply renewing it, could address this gap by expanding coverage to both goods and services, fostering broader economic engagement. Qualifying countries should enjoy benefits without review for at least three years, with out-of-cycle reviews for significant changes like coups or human rights abuses. This modernization would necessitate stronger cybersecurity measures and infrastructure, encouraging African countries to develop robust frameworks.

Integrating these improvements with support from and within AfCFTA structures can significantly bolster Africa's cyber defense capabilities, protect digital assets, and ensure a secure environment for economic growth. Embracing worldwide best practices enables African countries to choose the most effective standards for regulating cyber issues, fostering a more harmonized and comprehensive cyber regulatory framework. Such an approach would support the region's cyber stability, prosperity, and international cooperation.

4.4 Public-Private Collaboration to Address Policy Gaps

The most immediate success is obtainable through collaboration between industry stakeholders and policymakers to develop people-centric cybersecurity strategies. Where industry players drive innovation and know how to apply it to best advantage, policymakers frame and set the terms for implementation and enforcement. The first are funded, the second less so. But in collaboration, they can translate regulatory goals into effective cybersecurity strategies and implement them. Regulatory sandboxes and nurturing collaborations such as technical working groups and harmonization forums such as the AU Cybersecurity Expert Group (AUCSEG) and the AU Cyber Security Experts (ACE) help to facilitate advancements in cybersecurity awareness, capacity building, and regulations.

Case Study Box: Effective Public-Private Collaboration – Kenya and Cisco

In collaboration with the University of Nairobi and the ICT Authority, Cisco launched the first Cyber Security Experience Center on the African Continent in April 2024. The center aims to:

- Build strategic, in-country cybersecurity capabilities and expertise.
- Showcase the latest cybersecurity threat intelligence solutions.
- Support the Kenyan government with cybersecurity architecture and validated designs.
- Utilize AI/VR to deliver cybersecurity awareness experiences to Kenyan officials.

The lack of a standardized approach to cybersecurity education leads to inconsistent learning outcomes, misaligned accreditation criteria, and industry misalignment, hindering the development of a cohesive workforce capable of tackling evolving cyberthreats. The debate continues on whether standardization or customization better serves cybersecurity education, with arguments on both sides. Through a consultative effort with private sector, policymakers should mandate cybersecurity education that integrates with various disciplines, incorporate industry-recognized certifications, and be included in primary and secondary school curricula. Programs need to be adaptable, incorporate AI, and offer continuous education for professionals. Centralized, freely accessible training resources, gamified and immersive learning tools, specialized advanced training, and adaptive learning platforms are essential for effective cybersecurity education and training.[59]

In addition to traditional policy measures, African economies can benefit from proven strategies to further enhance cybersecurity capabilities. These include establishing cybersecurity centers of excellence, fostering public-private partnerships for cybersecurity research and development, incentivizing industry collaboration through cybersecurity grants or subsidies, and promoting cyber hygiene campaigns to raise public awareness and engagement. Implementing these measures can significantly bolster cyber resilience across the continent.

Leveraging emerging technologies like AI and ML for threat detection and response, instituting cybersecurity testing and certification programs, and encouraging information sharing and collaboration platforms for cybersecurity professionals are additional avenues for strengthening cyber defenses in Africa.

4.5 Prioritizing Vulnerable and Marginalized Groups

Policymaking will need to factor in vulnerable and marginalized groups in Africa, including women, children, the elderly, and people with disabilities. Persons with disabilities (PWDs) encounter barriers such as the high cost of assistive technologies and a lack of awareness about digital risks, leaving them vulnerable to cyber threats such as phishing and identity theft. Similarly, the elderly struggle with limited access to technology, low digital literacy levels, and inadequate support systems, making them targets for online scams and exploitation. Children, while benefiting from technology's educational opportunities, are exposed to cyberbullying and inappropriate content, particularly in low-income and rural communities where internet access is limited.

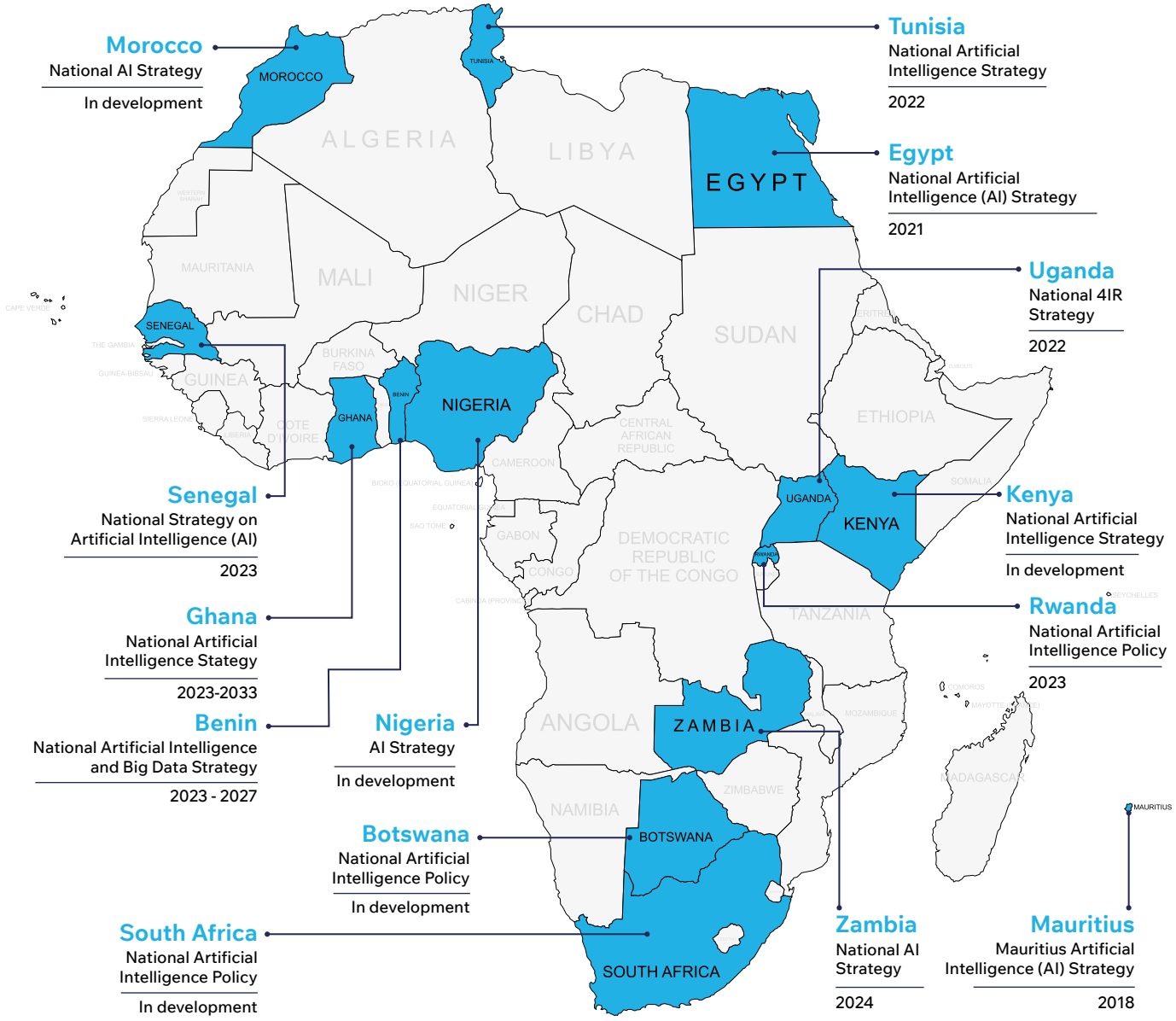
These elements demand that accessibility features be integrated into cybersecurity frameworks along with tailored digital literacy initiatives for vulnerable groups. To address the cybersecurity skills shortage in Europe, the European Commission's Cyber Skills Academy has developed a targeted strategy to achieve gender convergence in cybersecurity positions by 2030 through initiatives such as Women4Cyber. It also demonstrates its commitment to diversity and inclusion by creating a scoreboard that assesses Member States' performance in internet use, internet user skills, specialist skills, and employment based on 12 indicators.[60]

This sort of focus, such as affordable assistive technologies and educational programs, can empower marginalized communities to navigate the digital world securely and foster collaboration between governments, civil society, and private sectors, which remains crucial to implementing effective cybersecurity measures and safeguarding the online well-being of vulnerable populations across Africa.

4.6 Aligning AI and Cybersecurity Frameworks

Integration of AI into Africa's cybersecurity landscape demands a shift towards bolstering the continent's digital defenses. Demand for this is clear from the emergence of innovative startups pioneering AI-driven security solutions, collaborative public-private initiatives that leverage AI for threat mitigation, and coalitions such as the AI-Enabled ICT Workforce Consortium that assess AI's impact on technology jobs and identify skills development pathways for the roles most likely to be affected by AI.

But no African country has implemented formal AI regulation yet, though at least several have developed national AI Policy Strategies, and a few others (e.g., Botswana) are in the process of drafting their own. Given the rising cybersecurity risks, AI applications must be tailored to Africa's unique cybersecurity environment. This includes addressing the lack of explicit data privacy legislation and under-resourced enforcement authorities, which leave citizens vulnerable. Outdated privacy and data protection laws are often inefficient in addressing AI-specific issues, largely due to a lack of political will to update them. Finally, there is a preference for strict regulations that are intended to be enduring, rather than flexible, principle-based rules. This predisposition ultimately delays adaptation to



Africa's AI Policies and Frameworks. Source: Access Partnership 2024

technological changes and potentially increases cybersecurity vulnerabilities.

Overcoming these barriers requires cross-sectoral regulatory clarity, tech-neutral policymaking, and enhanced collaboration to unlock AI's full potential to fortify Africa's cyber resilience and contribute to the global cybersecurity landscape.
To aid in this, the African Union has made significant progress on its Continental AI Strategy, which aims to harness the power of artificial intelligence to support the continent's development goals. This strategy was endorsed during the AU's 2nd Extraordinary session of the Specialized Technical Committee on Communication and ICT in June 2024. The strategy emphasizes the importance of creating AI systems that reflect African diversity, languages, cultures, and geographical contexts. The AU's efforts represent a proactive step towards integrating AI into Africa's development agenda.

5 Recommendations

Clear and actionable recommendations derive from an examination of the cybersecurity circumstances this paper has considered. Each is an effective way to reduce cybersecurity threats across Africa and, by extension, to realize the growth it can enable for the digital economy.

5.1 Public-Private Partnership: Enabling Knowledge Transfer and Addressing Policy Lacunas

Private Public Partnerships play a pivotal role in addressing Africa's cybersecurity challenges: they help alleviate the insufficiency of skilled professionals by facilitating capacity building and mentorship initiatives tailored to the cybersecurity skills gap. By collaborating with effective, non-governmental entities that possess expertise in cybersecurity, African economies can amplify the intent of policymakers, and leverage funding from partners who are keen to contribute to the upskilling of the market they seek to open and hold.

Such partnerships also contribute to enhancing Africa's cybersecurity legislation by providing valuable insights, resources, and technical assistance. Through engagement with industry leaders and technical and legal experts – many of whom are keen to share their experience and knowledge of best practice from elsewhere in the world – African governments can refine and enact legislation that is robust, comprehensive, and adaptable to evolving cyber threats.

For example Cisco's Network Academies and Experience Centres could provide a platform for thought leadership by publishing insightful content such as whitepapers, and case studies, and hosting webinars, expert panels, and virtual events. These platforms can facilitate community engagement through forums and social media, showcase customer success stories, and offer interactive technology demonstrations. By collaborating on research initiatives and providing educational resources, the private sector can provide forward-thinking leadership.

5. 2 Focus on AI, Cloud Computing, and Encryption Technologies

Encryption and cryptography are essential for safeguarding sensitive data in Africa amid concerns about data privacy given the limited data frameworks in place. As digitalization extends to other growth sectors such as finance and healthcare, encryption becomes vital against cyber threats. Cloud computing resolves infrastructure challenges by consolidating controls across applications, overcoming on-premises limitations, and does so at scale. And AI's scalability solves resource constraints while aligning with operational needs and budget limitations while mitigating the shortage of skilled cybersecurity professionals through task automation and training platforms that enable robust defense mechanisms against evolving cyber threats in Africa.

5. 3 Broadening the Scope of Existing Cyber Frameworks

To strengthen cybersecurity efforts comprehensively, it is recommended to expand beyond the current heavy reliance on cybercrime and data protection laws. Priority should be given to developing robust frameworks for institution building, such as creating dedicated cyber agencies, national CERTs, and Security Operations Centers. Policy efforts should prioritize enhancing skills

and capacity building, and promoting incident and threat intelligence sharing to preemptively mitigate threats and enable rapid response capabilities.Policy efforts should prioritize enhancing skills and capacity building, promoting incident and threat intelligence sharing to preemptively mitigate threat and enable rapid response capabilities.

Furthermore, it is imperative to implement baseline security requirements for critical infrastructure organizations. This can be incentivized by introducing funding opportunities and tax incentives for businesses and public entities to invest in advanced security technologies and practices.

5.4 Multistakeholder Call to Action:

People-Centered Recommendations

African talent will do the most to mitigate cybersecurity risk across economies, by knowing what infrastructure to trust and actively working to protect citizens. To support the predisposition of the mighty continental talent pool in these endeavors, governments should:

- Develop and support initiatives to enhance digital literacy, including in cybersecurity professions.
- Collaborate with relevant stakeholders such as civil society organizations and academic institutions to promote digital literacy through events, workshops, and educational initiatives.

Governments, in collaboration with media channels, should:

- Conduct regular awareness campaigns across various media platforms to educate the public about cybersecurity.
- Work with relevant stakeholders to initiate digital literacy and digital security programs.

Technology Centered Recommendations

Without using and building on the tools developed worldwide, the race to balance cybersecurity with cyber threats will be long. To that end, governments should:

- Prioritize technology investments in underserved communities by allocating adequate budgetary resources for implementing inclusive ICT policies and programs.

The private sector, with respect to the technology to which it has such ready access, should:

- Make ICTs more affordable and accessible, especially for Persons with Disabilities (PWDs), and integrate inclusive design principles into technology products.
- Conduct continuous technology impact assessments and adopt approaches that promote positive outcomes for the public in accordance with international norms and standards.

Process Centered Recommendations

The building blocks of people and technology together are indomitable but cannot be put to the highest and best use without effective processes. To which end governments should:

- Establish protections, reporting mechanisms, and accountability measures for cyberattacks.
- Develop, review, and update comprehensive legislation to address new and emerging cybersecurity issues, including the protection of vulnerable and marginalized groups.
- Publish regular, detailed reports on the cybersecurity status in their countries.

Media should:

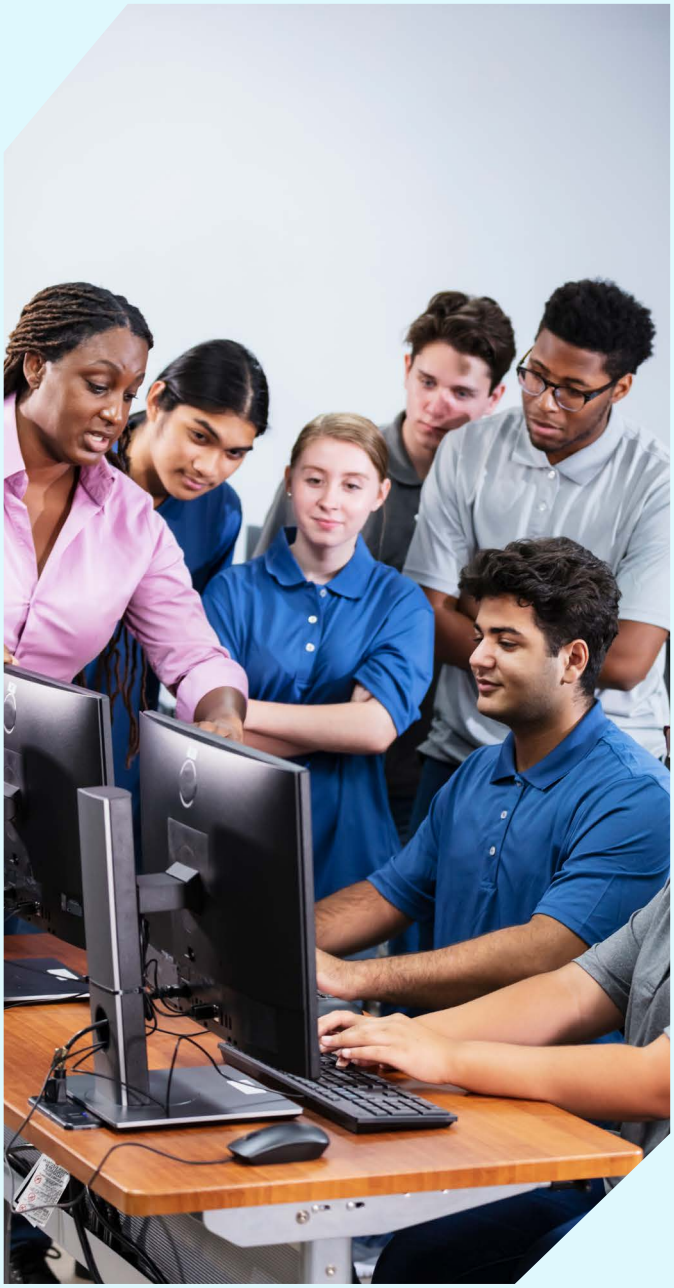
- Facilitate open dialogues and provide platforms for discussing laws and policies on cybersecurity in collaboration with policymakers, legislators, civil society, and regulatory bodies.

Civil Society should:

- Advocate for the adoption and implementation of frameworks related to the intersection of emerging cybersecurity technologies and society.
- Monitor the implementation of cybersecurity frameworks and expose malpractices, calling for accountability and transparency from governments and the private sector.

6 Conclusion

No African economy, no matter its level of development, can delay its work to expand its cybersecurity capabilities. With traditional sectors facing the same level of risk as the most innovative ones, no government can take the liberty of waiting for others to pave the way, establish best practice, or adopt the best bouquet of services: the exposure that is measured and recorded today demands immediate action, and this will only increase. With this certainty, the urgent work of Cisco and its partners will need to continue to scale at speed and be supported by the governments whose technology solutions Cisco proudly underpins for the long term.



Endnotes

1 Statista, 'Gross Domestic Product (GDP) in Africa from 2010 to 2027 (in billion U.S. dollars)'. Available at: https://www.statista.com/statistics/1300858/total-gdp-value-in-africa/

2 Cisco, 'Empowering Africa with 3 million more tech workers'. Available at: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m12/empowering-africa-with-3-million-more-tech-workers.html

3 Cisco, '2024 Cisco Cybersecurity Readiness Index'. Available at: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html

4 Ibid. These are organizations that have achieved advanced stages of deployment and are most ready to address contemporary risks across the full spectrum of cybersecurity solutions.

5 ISC2, 'ISC2 Cyber Security Workforce Study, How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023', pp3. Available at: ISC2_Cybersecurity_Workforce_Study_2023.pdf

6 World Economic Forum "Strategic Cybersecurity Talent Framework 2024," Available: https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf pp4

7 Password Managers, 'Cybersecurity Exposure Index (CEI) 2020'.

8 Mphatheni, M.R., & Maluleke, W. 'Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions'. Research in Business & Social Science, 11(4). (2022). Available at: https://www.ssbfnet.com/ojs/index.php/ijrbs.

9 Check Point Research, 'Average weekly global cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year'. Available at: https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

10 Positive Technologies, 'Cybersecurity threatscape of African countries 2022–2023'. Available at: https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

11 Tony Blair Institute for Global Change, 'Cybersecurity in Africa: What Should African Leaders Do to Strengthen the Digital Economy?' Available at: https://institute.global/policy/cybersecurity-africa-what-should-african-leaders-do-strengthen-digital-economy

12 Mphatheni, M.R., & Maluleke, W. 'Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions'. Research in Business & Social Science, 11(4). (2022), pp394. Available at: https://www.ssbfnet.com/ojs/index.php/ijrbs

13 Tony Blair Institute for Global Change, 'Cybersecurity in Africa: What Should African Leaders Do to Strengthen the Digital Economy?'. Available at: https://institute.global/policy/cybersecurity-africa-what-should-african-leaders-do-strengthen-digital-economy

14 ISC2, 'ISC2 Cyber Security Workforce Study, How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023', pp12. Available at: ISC2_Cybersecurity_Workforce_Study_2023.pdf

15 Santiago, J.E. 'Cyber heroines: African women in cyber defense'. Available at: https://www.sans.org/blog/cyber-heroines-african-women-in-cyber-defense/

16 United Nations Office on Drugs and Crime, 'Women in Cyber: A newsletter by the UNODC Global Programme on Cybercrime', pp3. Available at: https://www.unodc.org/westandcentralafrica/uploads/documents/Women_in_Cyber_-_Newsletter_-June_2022.pdf

17 KnowBe4, 'Women in cybersecurity 2022 report'. Available at: https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf. Several factors contribute to this gender gap, including gender norms steering women away from pursuing careers in science, technology, engineering, and maths (STEM), "a lack of cybersecurity awareness among women and girls, a lack of visibility for women within the cybersecurity field, and work cultures that are not conducive —and sometimes actively hostile —to their participation."

18 Access Partnership, 'AI in Africa: Unlocking Potential, Igniting Progress', pp6. Available at: https://cdn.accesspartnership.com/wp-content/uploads/2023/09/Access-Partnership-AI-in-Africa-A-working-paper-Single.pdf

19 Sey, A., & Mudongo, O. 'Case Studies on AI Skills Capacity-building and AI in Workforce Development in Africa'. Available at: AI-Capacity-Case-Studies-Final.pdf (researchictafrica.net)

20 Hurd, S. '5 things you didn't know about Cisco Networking Academy'. Available at: https://blogs.cisco.com/csr/5-things-you-didnt-know-about-cisco-networking-academy

21 Zeus, K. 'Cisco Looks to Help Close the Skills Gap in Africa by Investing in EDGE'. Available at: https://www.nojitter.com/digital-transformation/cisco-looks-help-close-skills-gap-africa-investing-edge

22 ISC2, 'ISC2 Cyber Security Workforce Study, How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023', pp60. Available at: ISC2_Cybersecurity_Workforce_Study_2023.pdf

23 Ibid.

24 Diorio-Toth, H. 'Five unique cybersecurity challenges in Africa'. *Africa Engineering*. Available at: https://www.africa.engineering.cmu.edu/news/2023/08/23-cybersecurity.htm

25 KPMG, 'KPMG's Africa Cyber Security Outlook 2022 Survey: Addressing Cybersecurity – Africa's economic opportunity!'. Available at: kpmg-africa-cyber-security-outlook-survey.pdf

26 Mphatheni, M.R., & Maluleke, W. 'Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions'. Research in Business & Social Science, 11(4). (2022), pp394. Available at: https://www.ssbfnet.com/ojs/index.php/ijrbs

27 Ibid.

28 All Bursaries South Africa, 'KnowBe4 Cybersecurity Scholarship 2024'. Available at: https://allbursaries.co.za/computer-science-it/knowbe4-cybersecurity-scholarship/#:~:text=KnowBe4%20partners%20with%20the%20Center,field%20of%20cybersecurity%20amongst%20women.

29 https://www.siemens.com/global/en/company/stories/research-technologies/cybersecurity/african-girls-can-code-empowering-women-in-cybersecurity.html

30 https://openworldsolutions.co.ke

31 https://www.janngo.com

32 Lemos, R. 'Infrastructure Cyberattacks, AI-Powered Threats Pummel Africa'. Available at: https://www.darkreading.com/vulnerabilities-threats/ai-powered-threats-cyberattacks-on-infrastructure-pummel-africa

33 Positive Technologies, 'Cybersecurity threatscape of African countries 2022–2023'. Available at: https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

34 ZAWYA, 'With phishing on the rise, it's worth being prepared: South Africa'. Available at: https://www.zawya.com/en/economy/africa/with-phishing-on-the-rise-its-worth-being-prepared-south-africa-tn9y0jnt

35 KnowBe4, 'Report: 2023 Phishing Benchmarking For Africa'. Available at: https://info.knowbe4.com/phishing-benchmarking-africa

36 Hochet-Bodin, N. 'Vent de panique à l'Union africaine après une nouvelle cyberattaque'. Available at: https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvelle-cyberattaque_6170976_3212.html

37 Malabo Convention 2024. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

38 African Union, 'The 2024 Statuary meeting at the Technical and Political level on AGA – APSA Platform concludes ahead of the AU summit in Addis Ababa'. Available at: "Development of the Common African Position on Cyber-Security in Africa"

39 EU treaty No 185,2000. Available at: Convention on Cybercrime (Budapest convection)

40 ECOWAS, 'ECOWAS Regional Cybersecurity and Cybercrime Strategy'. Available at: https://ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf. ECOWAS, 'ECOWAS Regional Critical Infrastructure Protection Policy'. Available at: https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf. ITU, 'Cybercrime directive: Explanatory notice Economic Community of West African States (ECOWAS)'. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL DOCUMENTS/FINAL DOCS ENGLISH/cybercrime_directive-explanatory_notice.pdf

41 UNECA, 'Cyber security: Central African States adopt model cross-border laws' Available at: https://archive.uneca.org/stories/cyber-security-central-african-states-adopt-model-cross-border-laws

42 ATU, 'Enhancing Cybersecurity in Africa: New challenges for Regional Organizations?'. Available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S3P2_Meriem_Slimani.pdf

43 ITU, 'Global Cybersecurity Index 2020'. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. The index assesses countries' cybersecurity commitments across five pillars, including legal measures, technical measures, organizational measures, capacity development measures, and cooperation measures.

44 Etti J and Edu. 'In a nutshell: data protection, privacy and cybersecurity in Nigeria'. Available at: https://www.lexology.com/library/detail.aspx?g=f44586b1-0048-4d93-a461-4d8c0aada232. Adisa, O.T. 'The impact of cybercrime and cybersecurity on Nigeria's national security'. Available at: https://dspace.cuni.cz/bitstream/handle/20.500.11956/187353/120460718.pdf?sequence=1. State Security Agency, 'The National Cybersecurity Policy Framework (NCPF)'. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

45 Kenyan Ministry of Information, Communications, and Technology, 'National Information, Communications, and Technology (ICT) Policy'.

46 Kenyan National Cybersecurity Strategy (2022-2027), p2. Available at: https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf.

47 Igwe, U. 'Nigeria's growing cybercrime threat needs urgent government action'. Available at: https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy.

48 Olomu, S. 'Nigeria tightens laws to tackle yearly cyber-crime losses of $500m'. Available at: https://itweb.africa/content/mYZRXM9gxVNvOgA8

49 Igwe, U. 'Nigeria's growing cybercrime threat needs urgent government action'. Available at: https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/.

50 Ibid.

51 Mzekandaba, S. 'Cyber crime's annual impact on SA estimated at R2.2bn'. Available at: https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m.

52 Global Cyber Alliance, 'Safeguarding Ghanaian Cyberspace'. Available at: https://globalcyberalliance.org/safeguarding-ghanaian-cyberspace-mfa-passwords/

53 CITI Newsroom, 'Momo fraud: Don't let others use your Ghana card – Telcos Chamber warns Ghanaians\'. Available at: https://citinewsroom.com/2023/09/momo-fraud-dont-let-others-use-your-ghana-card-telcos-chamber-warns-ghanaians/

54 SecurityWeek, 'Interpol: Key Member of Major Cybercrime Group Arrested in Africa'. Available at: https://www.securityweek.com/interpol-alleged-member-of-major-cybercrime-group-arrested-in-africa/

55 Africa Intelligence, 'Cybersecurity: Foxtrot International hit by $200,000 fraud'. Available at: https://www.africaintelligence.com/west-africa/2023/09/19/cybersecurity-foxtrot-international-hit-by-dollars200000-fraud,110054664-art

56 MEA Tech Watch, 'Moroccan Internet Users Rank 15th Globally for Cyber Infections in 2023: Kaspersky Report. Available at: https://meatechwatch.com/2024/01/04/moroccan-internet-users-rank-15th-globally-for-cyber-infections-in-2023-kaspersky-report/#:~:text=In%20a%20concerning%20trend%2C%20an,instances%20traced%20back%20to%20Morocco.

57 EU, 'NIS2 Directive'. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive; 'NIST AI Risk Management Framework'. Available at: https://doi.org/10.6028/NIST.AI.100-1

58 WTO, 'Information Technology Agreement'. Available at: https://www.wto.org/english/tratop_e/dtt_e/dtt-ita_e.htm#:~:text=Over%2080%20WTO%20members%20are,software%3B%20and%20parts%20and%20accessories.

59 World Economic Forum "Strategic Cybersecurity Talent Framework 2024," Available: https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf pp12-14

60 EU Commission 'Cybersecurity Skills Academy'. Available at: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy-diversity-inclusion

Access Partnership

accesspartnership.com

Follow us

Our offices

North America

Washington DC
Suite 512
1730 Rhode Island Ave N.W.
Washington DC 20036
USA

+1 202 503 1570
washingtondc@accesspartnership.com

Europe

London
The Tower, Buckingham Green,
Buckingham Gate,
London, SW1E 6AS
United Kingdom

+44 20 3143 4900
london@accesspartnership.com

Brussels
8th Floor, Silversquare Europe
Square de Meeûs 35
1000 Bruxelles
Belgium

+32 (0)2 791 79 50
brussels@accesspartnership.com

Middle East

Abu Dhabi
Al Wahda City Tower, 20th Floor
Hazaa Bin Zayed The First Street
PO Box 127432
Abu Dhabi, UAE

+971 2 815 7811
abudhabi@accesspartnership.com

Africa

Johannesburg
119 Witch-Hazel Avenue
Highveld Technopark
Johannesburg
Gauteng, South Africa

+27 72 324 8821

Asia-Pacific

Singapore
Asia Square, Tower 2
#11-01
12 Marina View
Singapore 018961

+65 8323 7855
singapore@accesspartnership.com