CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

APRIL 2024

A Digital Odyssey: The Convergence of Rapid Digitization, Population Dynamics, and Financial Risk in Namibia

Elmarie Biermann

A Digital Odyssey: The Convergence of Rapid Digitization, Population Dynamics, and Financial Risk in Namibia

Elmarie Biermann

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

Digital adoption and expansion across economic sectors enables growth in digital financial inclusion for a country's entire population. Namibia's experience in this offers valuable lessons for addressing the security and governance challenges in accelerating the adoption of digital financial systems. It shows how the country emulated key aspects of South Africa's approach to securing digital financial systems and the unintended consequences of this approach, which has not been sufficiently adapted to respond to particular elements of Namibia's cybersecurity landscape. Addressing issues specific to Namibia surrounding digital transformation and security requires an integrated and multitiered approach that includes private participation, sharing of infrastructure, and importing of digital policies.

This paper assesses the level of digital financial inclusion in Namibia and identifies its unique challenges in terms of the regulatory environment, digital literacy and associated security awareness, the technological environment, and the digital risk profile. It also makes suggestions for building a secure national cyber posture that will enhance secure digital financial inclusion.

Background

Namibia is home to a population of 2.6 million that is thinly spread across 824,292 square kilometers. The majority (55 percent) of the population lives in the northern and northeastern regions, with the capital, Windhoek, as the main hub. The conquest of then German

South West Africa by South African forces during the First World War resulted in its subsequent administration by South Africa until Namibia's independence in 1990.

The country's economy is still closely linked to and largely dependent on that of South Africa because of the Namibian dollar being pegged one-to-one to the South African rand, continued corporate footprints, intertwined critical infrastructure systems, and long-standing trade relationships. Namibia's economic performance and low rates of crime are driving increased foreign direct investment and progress.

Most of Namibia's major commercial banks, insurance companies, and wholesale businesses are controlled by South African interests. The country receives 30–40 percent of its revenues from the Southern African Customs Union, with financial services in Namibia attracting more foreign direct investment from South Africa than any other sector, at a capital expenditures value of R2.73 billion ZAR over the period from 2011 to 2023.[1]

Like many African countries, Namibia is experiencing increasing urbanization and digitization.[2] At the same time, according to the World Bank, it lags behind peer countries in the adoption of digital technologies despite having a mature telecommunications market.[3] The activation in the coastal city of Swakopmund in June 2023 of Google's Equiano subsea cable, which connects South Africa and Europe, has heightened digital connectivity between Namibia, the rest of southern Africa, and the wider world.[4] Terrestrial fiber networks are expanding, enabling more widespread access to cyberspace. The Communications Regulatory Authority of Namibia (CRAN) has announced it will hold an auction in 2024 for spectrum in the 3500-megahertz band to be used for the rollout of fifth-generation (5G) wireless technology.[5] 5G in turn will pave the way for smart cities as it allows the efficient deployment of Internet of Things devices.

All of this will lead to higher bandwidth capacity, better latency, and faster speeds at a much lower cost, setting Namibia on course for more rapid digitization and an inclusive digital economy. These advances in communication technology also inevitably mean greater exposure to new digitally enabled threats and a significantly expanding threat surface, especially in a consumer market with low levels of security awareness. Namibia is a very safe country with low crime rates and good law enforcement. Unlike South Africans, Namibians generally do not have a heightened perception of threat, including in the digital realm. This has enabled a wide range of cyber threats, with social engineering and phishing attacks topping the list.

Cybersecurity strength and resilience relies on the ability and preparation to defend against and respond to cyber threats. Without leadership and guidance from the state, the establishment of regulatory bodies, and the implementation of regulations, there will be little public trust in the safety of cyberspace. At the same time, Namibia's close entanglement with South Africa has produced an institutional legacy that does not suit the needs of an independent country. This inhibits Namibia's ability to foster secure digital financial inclusion. The country has emulated South Africa's approach, which does not adequately incorporate key

domestic factors: Namibian user and cultural profiles, a unique threat profile, and particular digital and financial inclusion challenges. This results in a high exposure to cyber risks, particularly at the population level.

Regulatory Environment

The Cybersecurity Capacity Maturity Model for Nations, developed by the Global Cybersecurity Capacity Centre at the University of Oxford, measures maturity across five dimensions, the first of which evaluates whether a company has an effective strategy based on national risks, especially for critical infrastructure.[6] Namibia does not have a national cybersecurity strategy. Meanwhile, its critical infrastructure, economic growth, digital inclusion, and governance are under attack from a wide range of cyber actors. In 2013, the World Bank noted that Namibia, as a small country, should in principle have agile public policies and be able to respond rapidly to new challenges and opportunities.[7] This has not yet been realized and the capacity of the public sector is limited, resulting in policy implementation shortfalls.

Namibia does not have any official national or sector-specific cybersecurity framework for supporting and implementing international cybersecurity best practices. However, it is improving its legislation with the development of the Electronic Transactions and Cybercrime Bill.[8] The main objectives of the bill in combating cyber crime are to protect critical data, address data privacy, and enable the Minister of Information and Communication Technology to appoint a computer security inspector and establish a team with clearly defined powers and responsibilities to investigate offenses. The bill also includes a section on accrediting providers of security services and products, such as encryption of data and creating keys for encryption algorithms. The bill refers to CRAN as the accreditation authority, which may lead to practical difficulties in implementation of the bill, as CRAN's mandate is to regulate licenses for telecommunications in Namibia.

This bill was intended to be presented to Parliament in 2020 but has not been presented as of January 2024, though the Electronic Transactions Act was rectified in 2019. The bill is reportedly being refined as part of a comprehensive strategy to overhaul the legislative and policy frameworks governing the information and communication technology (ICT) sector.[9]

In parallel, efforts by the Ministry of Information and Communication Technology to improve the draft Data Protection Bill of 2013 and to rectify the Communications Act of 2009 led to the draft Data Protection Bill of 2022, which includes ten principles of data protection and the creation of a data protection authority.[10] It is very similar to South Africa's Protection of Personal Information Act.[11]

In March 2023, the Ministry of Information and Communication Technology launched the National Cybersecurity Strategy and Awareness Creation Plan with the theme "A Step to Cyber Resilience & Digital Security."[12]

The plan aims to protect the national critical information infrastructure, to educate and create awareness, and to foster collaboration between players to continuously improve the safety of internet users in cyberspace.

Namibia has not so far adopted policies and laws on cyber crime, data protection, or protection of personal identifiable information. It is one of the few countries in the Southern African Development Community (the others are Angola, Mauritius, Mozambique and Zambia), that have ratified the African Union Convention on Cybersecurity and Personal Data Protection (the Malabo Convention),[13] which entered into force in June 2023. As a signatory, Namibia is required to establish a national data protection authority in charge of protecting personal data and to have domestic laws in place to guard personal data. This may place pressure on Namibia to pass those bills and establish the necessary authorities.

A lack of cybersecurity-related interventions and leadership by the state forces sectors to introduce sector-specific measures and partnerships to combat cyber crime, similar to the situation in South Africa.[14]

The South African Banking Risk Information Centre (SABRIC),[15] established in 2001, is an organization that aims to protect the banking industry and its customers from various risks, including cyber crime. Most of the banks in South Africa are members, including those with satellite offices in Namibia. Namibia's financial sector appears to be dragging its feet with regard to establishing a similar entity. The Financial Industry Cybersecurity Council was launched only in 2022 by the Bank of Namibia.[16] It is focused on combating cyber fraud by providing a forum for the banking and nonbanking financial sectors to foster conversations and develop strategies. However, no information on its activities has been made public, and none of the sources interviewed for this paper was able to shed light on its progress.

National intelligence on cyber risks and cyber crime, coordination on reporting of incidents, and assistance in recovery following an attack are normally consolidated in a national computer security incident response team (CSIRT) or computer emergency response team. In 2020, CRAN established a three-member National Security and Cyber Incidence Response Team (NSCIRT-Namibia).[17] The responsibilities of such national teams are to establish sector-specific response structures and to provide guidance on immediate risks and possible mitigations. Informing the public and organizations on methods of attack is an essential component in building and fostering a cybersecurity awareness culture. However, the guidance published by NSCIRT-Namibia does not include current cybersecurity-related risks.

To sum up, advances in and the adoption of digital and communication technology lead to economic opportunities and growth in an increasingly connected cyberspace. The related cyber risks and extended threats to government, companies, and people require the rollout of a national security strategy and connected regulations and standards to protect and enable a digital economy.

Digital Connectivity

The past decade saw significant global advances in artificial intelligence (AI), robotics, and the Internet of Things that have helped bring solutions to socioeconomic problems. Namibia, like other African countries, still faces challenges, though, in terms of access to the internet, technology infrastructure, and education. The government is under pressure to address inequalities, especially in the northern part of the country, regarding poor access to transportation, sanitation, and energy. Access to electricity is limited for a significant portion of the population; the World Bank reported in 2021 that only 55.2 percent of the population had access.[18] Some controls are in place to guard against extended power outages.

According to Paratus Namibia—a private company providing extensive connection services throughout Africa and a major actor in the provision of connectivity in Namibia— more than 40,000 households were equipped with fiber access in 2023. Internet penetration was at 53 percent at the start of 2023 and the number of mobile connections was equivalent to 108 percent of the country's population.[19]

Only a limited number of government schools are connected to the internet, hindering the participation of younger generations in cyberspace. The Harambee Prosperity Plan (2016–2020)[20] and the Fifth National Development Plan (2017–2022) include the target of 80 percent broadband connection to all public schools by 2020 to allow for e-learning—but it has not been reached. As of 2022, 78 percent of schools were still without the necessary infrastructure, including a connectivity rate of less than 18 percent for those in the less-connected far north.[21] The reasons for this slow adoption include the impact of coronavirus and the slowing down of the South African economy. During the pandemic, the Ministry of Universities and Technology announced the provision of free laptops and 10 gigabytes of data monthly to 32,000 higher education students in need. Though this was a positive move, the project experienced major drawbacks, such as access to limited energy sources and internet connectivity in some places. The Sixth National Development Plan,[22] the Second Harambee Prosperity Plan (2021–2025), and Vision 2030 have been drafted. All these documents identify infrastructural development as a core objective and confirm the need to expand ICT coverage.

The government and private sector recognize the need to overcome these obstacles by implementing necessary measures to improve connectivity, infrastructure, energy security, and education. Different task forces, such as the Task Force on the Fourth Industrial Revolution that operated in 2021–2022, will contribute to shaping policies and strategies to enable Namibia to embrace the opportunities offered by digital inclusion.[23]

For a country to effectively address the issue of financial exclusion, the private and public sectors must work together to promote inclusion. In terms of digital development, this applies to the cyber infrastructure layer and the software layer. The Fiber to the Village project, which aims to bring fiber connectivity to underserved villages, exemplifies this. It is driven and implemented by Paratus Namibia.[24] Since 2016, fiber connections have been established in the Golden Corridor, including the Trans-Cunene corridor (which links Walvis Bay to southern Angola) and parts of the route from Grootfontein to Oshakati, as well as that from Windhoek to Tsumeb, spinning off access to rural villages in the northern part of the country. This new cable infrastructure has significantly reduced Namibia's dependence on South African infrastructure.

Financial Inclusion Ecosystem

The Namibia Statistics Agency defines financial inclusion as a process to ensure equal access to financial services for all citizens, including vulnerable groups such as women, youth, and low-income earners, at an affordable cost.[25] Financial inclusion requires access to quality financial services for everyone to help people reach their full potential.

Digital financial services are crucial for enhancing financial inclusion by including previously underserved and marginalized people in the formal financial system. At the same time, in a country with a low-density population like Namibia's, the difficulties in servicing rural areas prevent a large part of the population from using the formal banking sector, leading to a push to adopt digital payment solutions. The coronavirus pandemic also drove this, with e-commerce and mobile applications being added to the financial payment landscape.[26] The total transaction value in the digital payments market in Namibia was projected to reach $1,414 million USD in 2024.[27]

The central bank, the Bank of Namibia, has identified digital transformation as a key enabler of financial inclusion objectives, which has led to investments in systems and platforms supporting digitization, and to exploring digital currencies. The Bank of Namibia lists thirteen authorized payment instrument issuers, including three authorized electronic-money issuers.

The growth of the digital payment market is also fueled by the increasing digitization of businesses and the quest for solutions to streamline transactions and promote cost efficiencies. Likewise, the growth of online marketplaces has increased the need for secure and efficient payment systems that are nontraditional.

Limited banking facilities for African populations has contributed to the creation of new financial services such as mobile banking (like M-PESA, a Kenya-based mobile money service).[28] Especially with the rollout of 5G, the use of mobile money is on the rise in Namibia. As elsewhere on the continent, mobile money solutions and agent banking have brought affordable, instant, and reliable transactions, savings, credit, and even insurance opportunities to rural villages and urban neighborhoods where no bank had ever established a branch.[29]

The adoption of new technology such as blockchain and AI in the market is also expected to play a role in increasing financial inclusion by enhancing security and efficiency of applications and authentication mechanisms. Reflecting the growing relevance of new technologies, the Virtual Assets Act was adopted in 2023.[30] It provides for the licensing and regulation of virtual asset service providers to ensure consumer protection and to mitigate the risk of money laundering and financing of terrorism.

As digital financial services expand and fuel greater financial inclusion, it is essential to identify and address potential barriers surrounding security and awareness. Financial illiteracy and lack of consumer protection are major impediments to accessing financial services and thus to financial inclusion. Protecting customers from fraud and abuse is crucial for digital financial inclusion in developing countries.[31] This must include not only technological safeguards, but also national policies and regulations for securing people's data and financial information.

The lack of such policies and regulations in Namibia has resulted in the development of cyber resilience and cyber maturity programs within organizations, including major banks, that are mostly driven by head offices in South Africa. This means that branches and satellite offices in Namibia operate on the South African model when it comes to cyber risk frameworks and information-security management systems.

In the case of financial literacy, there has been some progress in assisting consumers in making informed decisions suitable to their needs and capacity. Stakeholders, such as the Namibia Financial Institutions Supervisory Authority, have designed and rolled out financial educational programs.[32]

Overall, although the scene is set for rapid progress toward digitization and financial inclusion in Namibia, especially in terms of infrastructure and financial systems, this could be derailed by gaps in addressing cybersecurity risks.

Cybersecurity Risks

The cybersecurity landscape in Namibia is immature and fragmented in terms of the adoption of suitable controls, especially in the financial space. The regulatory environment for financial institutions is mainly based on that of their South African counterparts, with no domestic regulations or legislations to ensure privacy and combat security vulnerabilities. The following sections summarize and categorize risks unique to Namibia that hamper improvements in the country's security posture.

Threat Profile and Evolving Cyber Crime Ecosystem

Interpol has highlighted that the move toward a digital society—particularly in Africa—has created new ways for criminals to hide their identity and target new victims in sextortion and ransomware attacks, among others.[33] The transformation fueled by increased digital accessibility and connectivity to underserved communities has facilitated the emergence of new attack vectors and opportunities for cyber criminals. For example, South Africa saw a 100 percent increase in mobile banking application fraud in 2020.[34] The emerging mobile financial market in Namibia seems to be experiencing the same trend. Faced with the risk of fraud, identity theft, and cyber attacks, the population may lose trust in digital payments, potentially hindering their further adoption of digital banking and thus their financial inclusion.

The increase in mobile banking applications, the low level of cybersecurity awareness, and the lack of regulations have coincided with a surge in new scams linked to these new technologies.[35] Phishing and other forms of social engineering attacks targeting companies and bad actors take advantage of victims' fears, insecurities, and vulnerabilities.

Namibia is being targeted by advanced persistent threat (APT) groups and, increasingly, by cyber crime networks. In the financial space, for example, Namibia has the highest number of infections with the Emotet Trojan horse virus globally, leading to millions of dollars lost. This malware, spread by the APT group Mealybug from Ukraine, infects computers in the banking sector and steals sensitive information.[36] Emotet relies on sophisticated phishing campaigns for Windows-based users and was initially launched to target banks in Germany. A national CSIRT with the capability to stay abreast of APTs and their targets would play a pivotal role in combating such attacks.

Namibia is significantly impacted by the evolution and transnational nature of cyber crime, and it is trying to establish suitable defensive mechanisms and controls. The increase in internet access and adoption of mobile technologies is partly made possible by the influx of cheaper feature phones from China. But not only do feature phones lack the advanced capabilities of smartphones, such as adding-on of applications, they may also introduce security risks that are often unknown to the user. The cybersecurity and antivirus firm Kaspersky

Lab tested a number of feature phones to determine possible security threats and revealed that, in addition to leaking user data, some were also programmed to steal money by, for example, sending hidden text messages to paid numbers.[37]

To enhance the growth and adoption of digital financial services, unstructured supplementary service data (USSD) codes are used for accessing such services, especially on feature phones. The GSM Association, a nonprofit industry organization representing the interests of mobile network operators worldwide, has estimated that 90 percent of mobile money transactions in Africa are still driven by USSD.[38] According to the Financial Inclusion Global Initiative and the International Telecommunication Union, security testing for USSD revealed threats and vulnerabilities, including remote unauthorized access to and tampering with mobile devices.[39]

National and Sector-Specific Threat Intelligence and Communication Centers

Protection of the digital landscape relies on actionable threat intelligence and a realistic view of the current threat profile at the country, sector, and organization level. In Namibia, there is a relative lack of intelligence flow and mechanisms for sharing information on unique threats and vulnerabilities, as well as of assistance in the event of a cyber incident. This enables a cyber crime ecosystem to thrive undetected and hinders digital expansion and growth. Cyber incident response plans at all levels help to identify unique risks and are also a way to promote visibility and awareness of cyber crime.

The lack of a national center for identifying vulnerabilities and threats, communication to stakeholders, and continuous monitoring of threats, attacks, and vulnerabilities is somewhat alleviated by the private sector providing some threat analysis and monitoring services. This is done, for example, through secure operation centers (SOCs) that continuously monitor the security status of clients. Incident response following identification of, for example, access anomalies is monitored and communicated mainly via private SOCs or security information and event management platforms. These services, however, are still limited and not included by default in most organizations.

There is a need for detailed and reliable cyber crime threat information that is specific to Namibia, incorporating—among other things—its technology infrastructure, private-sector actors, security sensors (for use in the monitoring of national data flow), and population profile. The absence of such detailed threat information as a core part of a national strategy leads to misunderstanding of cyber risks, vulnerabilities, and the cyber actors involved. This in turn leads to ineffective initiatives and policies to address the impact and stem the rising tide of cyber crime.

Low Cybersecurity Awareness in Rural and Limited-Access Populations

In a country with unequal access to technology and digitization solutions, information regarding security and threat awareness does not spread evenly, leading to a low level of awareness, especially in underserved communities. Information dissemination in places such as informal settlements is erratic and dependent on individuals rather than organizations.[40]

As the Fiber to the Village project increases the number of people with access to cyberspace, cyber risks increase too. Prior internet exposure in rural communities is low, making inhabitants extremely vulnerable when they come online, especially in the absence of a national cyber awareness and resilience program. Metrics to assess the success of national awareness programs are prescribed via models such as the Cybersecurity Capacity Maturity Model for Nations, a comprehensive framework that assesses cybersecurity maturity across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory frameworks; and standards, organizations, and technologies.[41]

Namibia's overall security maturity in terms of awareness is extremely low and organizations, especially micro- to medium enterprises, are inadequately prepared to guard against a growing cyber crime ecosystem, as is evident from the number and intensity of attacks and breaches experienced by organizations. This has led to Namibia being considered one of the most exposed countries in Africa.[42] In a country where poverty and unemployment are high, slackness in implementing cybersecurity laws and regulations enables cyber crime because of the lack of any credible deterrence.[43]

Cyber awareness in organizations, especially among the most senior management, is insufficient and boards appear to underrate cybersecurity risk, as there is a lack of knowledge about the intricacies of this issue.[44] A lack of awareness and/or education about risks and red flags reduces organizations' ability to protect their services from attacks.

Toward a Stronger National Cybersecurity Strategy

While regulations are vital in combating cyber crime, educating citizens about the risks associated with it and the significance of cybersecurity is also important. The National Cybersecurity Strategy and Awareness Creation Plan, launched in 2023 by the Ministry of Information and Communication Technology, aims to protect critical information infrastructure, educate the public, and collaborate with public and private entities on cybersecurity to enhance the safety of internet users.[45] It targets government employees, ministries,

agencies, regional councils, local authorities, school learners, teaching staff, and the public. The plan aims to build awareness around mobile technologies and the safe use of applications, which will improve financial inclusion in the digital space.

The implementation of the plan began with the signing of a memorandum of understanding between the government and the Namibian company SALT Essential IT for an initial five-year period to develop and deliver cybersecurity training to the government sphere.[46] The memorandum of understanding is indicative of the government's commitment to increasing the security awareness of the general population.

The Ministry of Information and Communication Technology recognizes the increasing threat of cyber crime as Namibians rely more on technology. It aims to protect technology platforms and to educate vulnerable individuals about online risks. The ministry emphasizes the importance of a multi-stakeholder approach and urges all internet users to practice safe habits to protect their privacy.

Raising awareness is one building block for an improved security posture. A meshed approach is required that also includes partnerships with the private sector for the development of secure applications and infrastructure for the protection of data and assets. Targeted solutions to build up security nationally are needed, especially because Namibia has low levels of digital inclusion and literacy. For example, in the absence of a national Computer Emergency Response Team to disseminate cyber-threat warnings and coordinate response assistance, the country could establish a network of private and public entities for information-sharing and initiating actionable response.

The only organizations in Namibia that are focused on developing in-house security skills and awareness are a few satellite offices of South African entities, including companies in the security (especially financial security) space. But building and fostering security awareness is context- and culture-specific. Programs built for South Africa are not ideal for Namibia because of cultural and language differences. Namibia's policy structure aligns with that of South Africa, but the client-side technology that underlies it is completely different. For example, the penetration of feature phones is extremely low in South Africa but high in Namibia, which means differences in threat profiles and how awareness training should be approached.

The Payment Association of Namibia, the self-regulatory body for the payment industry, lists a number of short fraud-awareness tips, including for avoiding mobile banking fraud, phishing scams, and fraudulent proof-of-payment scams.[47] The mandatory registration of SIM cards, which should have been completed by the end of 2023, ought to facilitate the investigation of crimes committed with the aid of mobile devices.[48] This plan follows in the footsteps of South Africa, which in 2023 adopted the Regulation of Interception of Communications and Provision of Communication-Related Information Act. This act requires SIM cards to be a registered as a means to regulate the interception of communication.

Conclusion

The rise of cyber crime globally—fueled by increased connectivity, remote work, reliance on technology, and automation—is a reality for Namibia as well. As Namibians increasingly rely on information and communication technologies, there has been a corresponding rise in criminal activities in cyberspace, posing threats to digital connectivity and the integrity of critical infrastructure. As access to the internet and digital services increases, there is no matching growth in security expertise to combat cyber threats in organizations and law enforcement. Namibia's law enforcement bodies face challenges in combating cybercrime, including skills shortages, inadequate training, and a lack of specialized resources. The country must develop and foster specialized law enforcement units, focusing on technical skills such as digital forensics, and develop legislative frameworks to ensure successful prosecutions.

It is vital to manage cyber risks at the national level with a strategy adapted to Namibia's unique and increasingly complex threat profile, to be implemented through national policies and framed by laws and regulations. Forgoing a risk-based approach to identifying threats, probabilities, and impacts that is based on Namibia's specific macro and micro threat profile will lead to misallocation of resources and implementation of ineffective controls. Establishing and implementing such a national strategy requires, among other things, commitment, specialized skills, advanced knowledge, and digital and human capital. Information security is continuous, and the array of potential crimes in the digital space requires a mesh of solutions. Strategically, smaller-scale approaches may yield early benefits to ensure digital inclusion and growth as well as a safe environment for users, business, and the government. Such approaches could include capacity- and knowledge-building in defined pockets of excellence, partnerships with vendors and global organizations, intensified security awareness drives, and incident-response channels.

Namibia is a late responder to cyber threats, and its national governance environment does not facilitate cybersecurity intelligence filtering down to the population. With the bulk of the population spread out in rural communities, and digital adoption being driven by cheap, imported, insecure feature phones, threats are widely present. Communication channels should be utilized to spread incident response plans and threat intelligence, adding to the development and fostering of a cybersecurity awareness culture.

Namibia faces increasing cybersecurity challenges as it embraces digitization and technology. Sophisticated threats like phishing, ransomware, and data breaches pose risks to individuals, businesses, and government institutions. Lack of awareness of and education on cybersecurity practices is a major obstacle, leaving many vulnerable to attacks. Additionally, there is no comprehensive, country-specific legal and regulatory framework for cybersecurity. However, there are opportunities to strengthen cybersecurity through government proactivity, such as

partnerships with AI and machine learning companies to aid in the design and implementation of mitigating controls. A collaborative approach involving government, businesses, and individuals is crucial to promoting awareness, education, and best practices.[49]

Awareness training programs, such as those provided by SALT Essential IT, may strengthen information flow structures and help them develop resilience. The Seventh National ICT Summit, held in October 2023, also saw the launch of the iSecureBot, a WhatsApp information bot that provides cybersecurity awareness and education to the public.

Cybersecurity is an emerging topic within the Namibian business environment, which is still in its infancy of awareness and management on these issues. Building a cybersecurity awareness culture at the national level is vital, as is the provision of secure infrastructure and actionable threat intelligence to adequately control cyber risks.

Cyber risks should be managed as an extended enterprise, incorporating different levels of controls to ensure a security-mature population. At the center must be policies, regulations, and laws to help cybersecurity professionals curb adversaries and threats. Namibia's lack of high-level policies greatly hinders the country's move toward greater digital inclusion. The protection of personal information and digital assets is currently left to individuals, who mostly lack the necessary knowledge, skill, and authority to adequately protect their digital assets. Balancing risk with digital growth requires standards, awareness, knowledge, and skills to address the security susceptibilities in Namibia's cyber landscape.

A national cybersecurity strategy, implemented in partnership with current and upcoming stakeholders in industry, is required. Expanding the cybersecurity incident response capability—in terms of technology, monitoring capabilities and expertise—must be part of that strategy. International vendors already present in Namibia have the ability to provide targeted threat intelligence and solution guidance. International standards and frameworks to guide cyber risk management processes, especially around the protection of critical infrastructure, are essential, as are increased international cooperation between agencies to share information and capabilities.

With its extensive growth in digital infrastructure and applications driving greater financial inclusion, Namibia requires a unique cybersecurity strategy based on its current posture, cultural and language profile, vast geography, population size and spread, and level of literacy. And by not merely adopting processes and models from South Africa, Namibia could set an example for the continent.

About the Author

Elmarie Biermann is director of the Cyber Security Institute in South Africa, which specializes in guiding organizations in identifying and managing cyber risks, as well as partnering with universities and institutes to provide specialized cybersecurity training to a global audience

Notes

1 "Namibia Factsheet," Wesgro, April 2023, https://www.wesgro.co.za/resources/namibia-factsheet-april-2023.

2 "Namibia," Wesgro, May 2021, https://www.wesgro.co.za/uploads/files/Research/Wesgro-IQ_Namibia_2021.05.pdf.

3 "Creating Markets in Namibia," World Bank Group, July 2022, https://documents1.worldbank.org/curated/en/099850311112236455/pdf/IDU0ff2db1400403c046b2099a300571336f9a6d.pdf.

4 Grace Goodrich, "Namibia's Equiano Cable Boosts Connectivity," Submarine Telecoms Forum, June 13, 2023, https://subtelforum.com/namibias-equiano-cable-boosts-connectivity/#:~:text=Namibia%3A%20Equiano%20Connectivity%20Cable%20Comes%20Online&text=Representing%20a%20one%2Dbillion%2Ddollar,from%20Portugal%20to%20South%20Africa.

5 Matshepo Sehloho, "Namibia to Auction 5G Spectrum," Connecting Africa, May 29, 2023, https://www.connectingafrica.com/author.asp?section_id=816&doc_id=785095.

6 "Cybersecurity Capacity Maturity Model for Nations," Global Cyber Security Capacity Centre, 2021, https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

7 "International Bank for Reconstruction and Development International Finance Corporation and Multilateral Investment Guarantee Agency Country Partnership Strategy for the Republic of Namibia for the Period FY2014–FY2017," World Bank, June 16, 2013, https://documents1.worldbank.org/curated/en/247341468323960034/pdf/777480CAS0NA0R00Box0377356B00OUO090.pdf.

8 "Electronic Transactions and Cybercrime Bill," ICT Policy Africa, last updated October 28, 2019, 1, https://ictpolicyafrica.org/fr/document/ggel4vdlal?page=1.

9 Hertta-Maria Amutenja, "Namibia's Cybercrime Bill Undergoes Redrafting," *Windhoek Observer*, September 2026, https://www.observer24.com.na/namibias-cybercrime-bill-undergoes-redrafting.

10 "Draft Data Protection Bill 2021," *Government Gazette of the Republic of Namibia*, 2022, https://action-namibia.org/.

11 "Protection of Personal Information Act," POPIA.co.za, accessed February 26, 2024, https://popia.co.za/.

12 "Namibia's Ministry of ICT to Launch New Cybersecurity Policy Document,"

Namibia Daily News, April 1, 2023, https://namibiadailynews.info/namibias-ministry-of-ict-to-launch-new-cybersecurity-policy-document.

13 "Southern African Development Community Cybersecurity Maturity Report 2021," C3SA, 2022, https://open.uct.ac.za/server/api/core/bitstreams/308c9128-87a8-4a84-83cf-f811f2e7c39e/content.

14 Noëlle Van der Waag-Cowling, "Dividend of Liability? Financial Inclusion, Digital Deprivation, and Cyber Risk Proliferation in South Africa," 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.

15 "SABRIC," South African Banking Risk Information Centre, accessed February 26, 2024, https://www.sabric.co.za/.

16 Kazembire Zemburuka, "Bank of Namibia Launches Financial Industry Cybersecurity Council," Bank of Namibia, November 22, 2022, https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/95/95b55ccf-5a68-485b-adb2-5a1883f5b06b.pdf.

17 "Namibia Cyber Security and Cyber Incidence Response Team," Communications Regulatory Authority of Namibia, accessed February 26, 2024, https://www.cran.na/national-security-and-cyber-incidence-response-team.

18 "Access to Electricity (% of Population) – Namibia," World Bank, last updated 2021, https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=NA.

19 Simon Kemp, "Digital 2023: Namibia," Datareportal, February 14, 2023, https://datareportal.com/reports/digital-2023-namibia.

20 "Harambee Prosperity Plan," Republic of Namibia, April 2016, https://op.gov.na/documents/84084/572904/HPP.pdf/3c5b6d5f-3394-4302-aeec-bd10ca58a119%20.

21 "78% of Namibian Schools Lack ICT Infrastructure," Brief, July 18, 2022, https://archive.thebrief.com.na/index.php/component/k2/item/1434-78-of-namibian-schools-lack-ict-infrastructures.

22 Elao Aipanda, "Launch of the Sixth National Development Plan (6NDP) Formulation Process," Republic of Namibia National Planning Commission, June 9, 2023, https://www.npc.gov.na/tag/ndp5.

23 Roswitha Ndumbu, "The 4IR in Namibia Faces Fundamental Issues," *IPPR Blog*, November 29, 2021, https://ippr.org.na/blog/4ir-faces-fundamental-issues-in-namibia.

24 "Africa's Quality Network," Paratus, accessed February 26, 2024, https://paratus.africa.

25 "Namibia Financial Inclusion Survey (NFIS) 2017, Namibia Statistics Agency, 2017, https://finmark.org.za/system/documents/files/000/000/205/original/NFIS-2017-Report.pdf?1601977875.

26 "Digital Payments – Namibia," Statista, last updated January 2024, https://www.statista.com/outlook/dmo/fintech/digital-payments/namibia.

27 "Digital Payments – Namibia," Statista.

28 "African Cyberthreat Assessment Report: Interpol's Key Insight Into Cybercrime in Africa," Interpol, October 2021, https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf.

29 "Digital Access: The Future of Financial Inclusion in Africa," International Finance Corporation and MasterCard Foundation, May 2018, https://www.ifc.org/content/dam/ifc/doc/mgrt/201805-digital-access-the-future-of-financial-inclusion-in-africa-v1.pdf.

30 "Government Notice: Promulgation of Virtual Assets Act, 2023," Government Gazette of the Republic of Namibia, July 21, 2023, https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/90/90d8c518-f9a2-4e6d-98a4-b192c1a93253.pdf.

31 Lee-Ying Tay, Hen-Toong Tai, Gek-Siang Tan, "Digital Financial Inclusion: A Gateway to Sustainable Development," *Heliyon* 6, vol. 8 (June 2022), https://doi.org/10.1016/j.heliyon.2022.e09766.

32 Ipumbu Shiimi, "Financial Inclusion – An Imperative Towards Vision 2030" (speech), October 28, 2010,

33 Interpol, "African Cyberthreat Assessment Report."

34 "Hackers on the Dark Web Love South Africa – Here's Why We Suffer 577 Attacks per Hour," News24, June 3, 2020, https://www.news24.com/news24/bi-archive/sa-third-highest-number-of-cybercrime-victims-2020-6.

35 Interpol, "African Cyberthreat Assessment Report."

36 "Emotet Malware Over the Years: The History of an Infamous Cyber-Threat," Heimdal Security, 2022, https://heimdalsecurity.com/blog/emotet-malware-history.

37 Enoch Root, "Dangerous Feature Phone," Kaspersky, October 15, 2021, https://www.kaspersky.com/blog/dangerous-feature-phones/42466.

38 Francesco Pasti, "State of the Industry Report on Mobile Money," GSMA, 2019, https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf.

39 Kevin Butler, Vijay Mauree, and Arnold Kibuuka, "Security Testing for USSD and STK Based Digital Financial Services Applications," Financial Inclusion Global Initiative, 2021, https://figi.itu.int/wp-content/uploads/2021/04/Security-testing-for-USSD-and-STK-based-Digital-Financial-Services-applications-1.pdf.

40 Marly Samuel et al., "Improving the Flow of Livelihood Information Among Unemployed Youth in an Informal Settlement of Windhoek, Namibia," *C&T '17: Proceedings of the 8th International Conference on Communities and Technologies* (June 2017), 256–265, https://dl.acm.org/doi/10.1145/3083671.3083687.

41 "Cybersecurity Capacity Maturity Model for Nations: Structure and Deployment Methodology," Global Cyber Security Capacity Centre, C3SA, Oceania Cyber Security Centre, and Oxford Martin School, April 28, 2021, https://cybilportal.org/wp-content/uploads/2020/04/GFCE-V-Meeting-Assessments-GCSCC.pdf.

42 Victor Oluwole, "List: African Countries Most Vulnerable to Cyber Threats in 2023," Business Insider, July 18, 2023, https://africa.businessinsider.com/local/markets/list-african-countries-most-vulnerable-to-cyber-threats-in-2023/zmghfbx?op=1; and Maihapa Ndjavera, "Namibia Susceptible to Cyberattacks . . . Country Experienced 40% Increase in 2022," October 11, 2023, https://neweralive.na/posts/namibia-susceptible-to-cyberattacks-country-experienced-40-increase-in-2022.

43 C3SA, "Cybersecurity Maturity Report 2021."

44 See for example "CFO Survey 2018: A Detailed Overview," Deloitte, June 2018, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-finance-CFO-survey-report-2018-noexp.pdf.

45 "Namibia National Cybersecurity Strategy and Awareness Raising Plan 2022 – 2027," Ministry of Information and Communication Technology, accessed March 8, 2024, https://mict.gov.na/documents/32978/267050/Namibia+Cybersecurity+Strategy+%26+Awareness+Raising+Plan+2022+-+2027+.pdf/07a6bc76-970a-497a-9dd5-3a54a4450ee1?version=1.1.

46 "Salt and MICT: Public Cybersecurity Awareness Partnership," SALT Essential IT, July 29, 2022, https://www.salt.na/salt-and-mict-public-cybersecurity-awareness/.

47 "Mobile Banking Fraud," Payments Association of Namibia, accessed February 26, 2024, https://www.pan.org.na/mobile-banking-fraud.

48 Matshepo Sehloho, "Connecting Africa, Namibia Starts Mandatory SIM Registration Process," Connecting Africa, January 20, 2023, https://www.connectingafrica.com/author.asp?section_id=816&doc_id=782804.

49 Sakeus Nangolo, "Cybersecurity in Namibia: Challenges and Opportunities," *Namibian*, April 11, 2023, https://www.namibian.com.na/cybersecurity-in-namibia-challenges-and-opportunities; Herman Nghidipaa, "Cybersecurity Awareness Strategies for a Happy Digital Namibia," *Namibian*, May 10, 2023, https://www.namibian.com.na/cybersecurity-awareness-strategies-for-a-happy-digital-namibia; and Daoud Vries, "Cybercrime Remains One of the Main Challenges in Namibia," NBC, 2023, https://nbcnews.na/node/99441.

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.

TIA's work informs and is informed by direct dialogues among thought-leaders, senior officials, and executives in key countries. We share the data, insights, and policy recommendations that result in reports, commentaries, and web tools. Carnegie's regional centers and networks in the United States, China, Europe, India, and Russia provide a widely respected international platform for promoting our policy proposals.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org