Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

‘Leapfrogging’ or ‘lagging’?: highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria

Nate Allen, Sherif Hashem & Elizabeth Kolade

To cite this article: Nate Allen, Sherif Hashem & Elizabeth Kolade (22 Jan 2024): ‘Leapfrogging’ or ‘lagging’?: highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria, Journal of Cyber Policy, DOI: 10.1080/23738871.2024.2304560

To link to this article: https://doi.org/10.1080/23738871.2024.2304560

Published online: 22 Jan 2024.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2024.2304560

Routledge
Taylor & Francis Group

'Leapfrogging' or 'lagging'?: highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria[1]

Nate Allen [a], Sherif Hashem[b] and Elizabeth Kolade[c]

[a]Africa Center for Strategic Studies, National Defense University, Washington, DC, USA; [b]Information Sciences and Technology, George Mason University, Fairfax, VA, USA; [c]University of Bristol, Bristol, UK

ABSTRACT

Emerging economies are experiencing dramatic rises in internet penetration, along with an expansion of cyber-dependent critical infrastructure. Nevertheless, in many countries and regions, critical information infrastructure protection (CIIP) efforts remain at a relatively nascent stage. Early and widespread approaches to critical information infrastructure protection are informed by higher income, early digitising nations, which may not reflect the priorities, needs, or challenges faced by late-digitising emerging economies. This paper analyses CIIP efforts and processes in Nigeria and Egypt, considering the degree to which the standards and approaches to CIIP adopted by early digitising countries apply to each county's experience. Evidence from both countries suggests that emerging economies will not follow the same trajectory or benefit from the same lessons learned in CIIP as early digitising regions of the world. Both countries face a different mix of CII and CII-vulnerabilities, a greater emphasis on internal cyberthreats, and significant resource and capacity constraints in comparison to early digitising nations. This suggests that 'leap-frogging' may not always be possible, and innovative, context-specific CIIP policies and strategies are needed.

ARTICLE HISTORY
Received 25 September 2023
Accepted 11 December 2023

KEYWORDS
Cyber; Cybersecurity; Egypt; Nigeria; critical infrastructure

Introduction

Emerging economies across the world are undergoing a rapid digital transformation. Over the past decade, the number of internet users has more than doubled to nearly 5 billion, and may reach 6.5 billion, 90 per cent of the world's population, by 2030 (Kemp 2022; Morgan 2019). Due to a growing population and low comparative rates of digitisation, the growth in global internet users is being driven not by high income countries, but by emerging economies in Asia, Latin America and Africa. As observed by former Google executive Caesar Sengupta (2020), these new users 'experience the internet differently from those who came before them … more and more, it's their needs and ideas that are shaping the future of technology.'

This accelerated digitisation has led to growing innovation in many emerging economies across the world. Low- and middle-income countries such as Kenya, India and El

CONTACT Nate Allen nate.df.allen@gmail.com Africa Center for Strategic Studies, National Defense University, Washington, DC, 20319, USA

Salvador are establishing themselves as global leaders in the adoption of mobile money and cryptocurrency (Onyago 2022; Chainalysis 2022; Lopez and Livni 2021). 'Smart' city technologies, from AI-powered surveillance systems to robots who direct traffic, can be seen on the streets of cities such as Tunis, Kinshasa, Astana and Medellin (Allen 2021). The COVID-19 pandemic has further accelerated this transition, with businesses moving their operations into the cloud to expand their reach and enable remote work.

While the global digital transformation has been recognised as being a source of prosperity and power, it is also a source of risk. As they have digitised, the critical infrastructure that is essential to the future growth and prosperity in emerging economies is becoming increasingly cyber-dependent – and vulnerable to cyber-enabled threats. Computer systems in India's electricity network and the Brazilian state-owned gas giant Petrobras were among those affected by the Wannacry ransomware attack, which has been widely attributed to North Korea (Gosh and Ashok 2017). In what has probably been the most significant act of cyber sabotage in Africa to date, shipping in much of Southern Africa was brought to a halt because of a ransomware attack against Transnet, the South African port operator (Reva 2021). Cybercriminal groups based in Egypt have repeatedly attempted to sabotage public services, government institutions, and ICT infrastructure in Ethiopia over the filling of the Grand Ethiopian Renaissance Dam, a major source of tension between the two countries (Al-Monitor 2022). In late 2022, Ghana's state-operated electricity company was hit with a ransomware attack, disrupting the entire country's supply of electricity (Segal 2022). And in July 2023, the hacking group Anonymous Sudan launched a debilitating cyberattack against Kenya's mobile payment and e-government services systems (Mwai and Nkonge 2023).

Despite these growing vulnerabilities, there has been little progress in protecting critical information infrastructure in many emerging economies, which we define for the purposes of our argument as late-digitising, low and middle-income countries that are predominantly located in the Global South. Many, if not most, emerging economies lack basic critical information infrastructure protection policies, strategies and legal frameworks; in some, what constitutes 'critical information infrastructure' is neither defined nor identified. To date, the most widely implemented approaches to critical information infrastructure protection have been designed by high-income, technology dependent countries. This may make them ill-suited to a more resource-constrained context confronted in emerging economies, who may need to prioritise sectors, resources and approaches.

In this paper, we argue that emerging economies need to take an approach to the protection of critical information infrastructure that is informed by, but also distinct from, the approaches, standards and policies set up by early digitising countries. Drawing on the case studies of ongoing critical information infrastructure protection efforts in Nigeria and Egypt, two large, rapidly digitising emerging economies with ongoing CII protection efforts, we argue that each country faces CII vulnerabilities, opportunities and risks that are different from early digitising countries. These differences include rapidly growing vulnerabilities in key sectors such as finance and telecommunications; nodes of critical infrastructure that serve as 'single points of failure' whose compromise has the potential to effect large swathes of their populations; significant constraints in physical and human resources; and a strategic prioritisation of cyberthreats from internal sources such as criminals and insurgent groups rather than external, state-sponsored actors. Due to these differences, we argue that 'leap-frogging' wealthier, early digitising nations is not always possible.

A key conclusion of our analysis is that emerging economies cannot and should not rely strictly on frameworks developed by wealthy, early digitising economies to protect their critical information infrastructure. These frameworks can serve as a starting point, but changes in technology, a different mix of sectoral-level vulnerabilities, and resource constraints means that leaders in emerging economies will need to adopt-context specific, adaptive and economical approaches to identifying and protecting critical information infrastructure in their countries. Experience from both Nigeria and Egypt indicate that context-specific investments in people and processes, as opposed to more expensive or advanced technologies, can go some way to mitigating deficits in physical and human resources that many emerging economies face in comparison to higher-income, more technology dependent nations.

The remainder of this article is structured as follows. In the second section, we briefly summarise and trace the evolution of existing global efforts to protect critical information infrastructure. In the third section, we discuss existing efforts to protect critical infrastructure in emerging economies, arguing that existing efforts to protect critical information infrastructure in emerging economies have been driven mostly by standards devised in wealthier, technology-dependent, high-income regions of the world. We lay out our argument for why different sectoral-level mixes of vulnerabilities, advances in technology, and resource constraints merit a different approach for understanding and redressing critical information infrastructure vulnerabilities in emerging economies. In the fourth and fifth sections, we illustrate our argument using examples from Nigeria and Egypt. A final section offers some brief concluding thoughts and recommendations to inform broader global critical information infrastructure protection debates based on the experiences of Egypt and Nigeria.

Existing approaches to critical information infrastructure protection

Critical information infrastructure (CII) is commonly defined by leading organisations as information systems whose disruption would have a debilitating impact on society. For example, the Internet Engineering Task Force (2007) defines CII as 'systems so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety' (86). This definition closely mirrors those adopted by leading countries and international organisations (ITU 2008; OECD 2008; African Union 2014; United States 2013; GFCE (Global Forum on Cyber Expertise) and Meridian 2017). Physically, critical information infrastructure includes interconnected systems, such as telecommunications and satellite networks, whose operation is necessary for the function of critical infrastructure across multiple sectors (Maglaras et al. 2018). It also includes systems within specific sectors, such as energy, manufacturing or transportation sectors, whose interruption would have significant impacts on national security or societal well-being. These systems may be connected to the internet, but also include industrial control systems (ICS) that automate industrial processes such as energy transmission or water treatment.[2]

Emerging economies have not entirely been absent from, and, to a degree, have been instrumental in helping to shape current global norms surrounding the protection of critical infrastructure. To date, the world's two major efforts include the UN-sponsored Group of Government Experts (GGE), which was largely led by the United States and its allies, and

the Open-Ended Working Group (OEWG), which grew out of a Russia-sponsored resolution. Despite these two groups working in opposition, both agree on the importance of CII protection. The GGE, which consisted of 25 experts roughly evenly divided between countries from the Global North and South, developed and endorsed a list of 11 voluntary norms of state behaviour, including norms that call on states to 'take appropriate measures to protect their critical infrastructure from ICT threats' and 'respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT-attacks' (United Nations 2021b, 13). The final report of the OEWG (United Nations 2021a), which also included the participation of many emerging economies, likewise recommends that states should not conduct or support ICT activity that 'intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public', and further calls on states to 'strengthen measures to protect all critical infrastructure from ICT threats' (5). Beyond the leadership of major global cyber powers such as the United States, China and Russia, it should be noted that several emerging economies from the Global South, including Brazil, India, Indonesia, Kenya, Egypt and South Africa, were active participants in both processes.

While there exists global consensus on the importance of CII protection, it should be noted that the guidelines recommended by the GGE and OEWG remain voluntary, and there is no universally accepted body of policies, laws, legislative and legal practices that address the protection of critical information infrastructure. More problematically, the current most widely adopted standards and approaches to CII protection have been developed in large part based on the experiences of high income, technology dependent countries predominantly located in the Global North. In part, this is because they were the first nations to digitise. For example, preventing cyberattacks to critical infrastructure was the first of three objectives outlined in the world's first national cybersecurity strategy, released in 2003 by the newly created United States Department of Homeland Security (2003). The European Network and Information Security Agency (ENISA) was founded in 2004 as an independent agency to improve the resilience of critical information infrastructure and systems across Europe (Hashem 2017).

Though many nations across the world have implemented or are in the process of implementing critical information infrastructure protection policies (de-Jong-Chen and O'Brien 2017), the earliest and the most widely used frameworks, such as the OECD's Council's Recommendation on the Protection of Critical Infrastructures, as well as the National Institute for Standard and Technology's (NIST) Cybersecurity Framework, were developed in Europe and the United States, respectively. Based on existing standards and guidelines, the NIST framework offers organisations a tiered approach to developing and assessing their cyber institutions along five core critical infrastructure protection functions: identification, protection, detection, response and recovery. The framework itself is meant to be flexible and can readily be applied to any of the 16 sectors identified by the US as containing critical infrastructure: chemical, commercial facilities, communications, manufacturing, dams, defence industry, emergency services, energy, finance, food and agriculture, government facilities, health care, information technology, nuclear materials, transportation and water.

These standards were developed to reflect the domestic priorities of Europe and the United States and, despite their widespread adoption, weren't necessarily intended to be global standards. A few organisations, such as the Global Forum on Cyber Expertise, offer general guides for emerging economies, largely based on leading international standards

(GFCE and Meridian 2017; Internet Society and AU 2017). More recently, regional bodies such as the African Union (AU 2014; Internet Society and AU 2017) and ECOWAS (2021) have begun to develop CII policies and standards of their own. The more comprehensive of these are clearly informed by, but also distinct, from the standards first put forth by early digitisers.

Nevertheless, in part because many emerging economies are still in the process of digitising, there have been few efforts to analyse how, whether, and to what extent their experiences with CII protection might differ from those in richer, and often more technology dependent regions of the world. Few, if any, in-depth case studies documenting the experience of emerging economies in designing and implementing CII protection policies exist.[3] This represents a major gap in our ability to effectively understand and approach CII protection in emerging economies across the world.

There are good reasons to suspect that some CII-related threats will manifest differently in emerging economies, and therefore require different mixtures of policies and standards to address than those developed by earlier digitising economies that are in widespread global use. For example, the African Union and Internet Society Guidelines on Internet Infrastructure Protection suggest that key differences between Africa's threat landscape from much of the rest of the world includes 'intermittent connectivity' resulting from insufficient resources, high costs, and lack of trained workers, as well as out-of-date and unpatched software embedded in many commercial systems. Some scholars have suggested that existing protection guidelines and standards, such as Computer Security Incident Response Teams (CSIRTS), are too costly for many stakeholders in emerging economies, in particular, small, medium and informal enterprises. They propose the creation of cost-effective, community-oriented cybersecurity protection entities such as Security, Advisory and Warning Teams (C-SAWs) or Warning, Advice and Reporting Points (WARPs) (Ellefsen and von Solms 2010; Mouton and Ellefsen 2013). Others have observed that the growth in mobile broadband in Africa is leading to new kinds of vulnerabilities that 'must be realised and taken into account within Critical Information Infrastructure' (von Solms and Kritzinger 2012, 120; Musarurwa and Jazri 2015).

The rapidly expanding pace of digitisation has meant that there now exists a significant number of emerging economies with growing rates of internet penetration. Many such countries have yet to begin, or have only just begun, to develop legal, policy, institutional architecture to address cyber-related threats to their critical infrastructure. In Europe, for example, nearly 90 per cent (40/46) countries address critical information infrastructure protection as a component of national cybersecurity strategy and policy, compared to just over 50 per cent (78/148) across the rest of the world (ITU 2021, 10).

In-depth case studies documenting CII protection efforts in late-digitising, lower income countries could significantly further our understanding of the degree to which the oldest and most widely adopted CII standards, such as the NIST, offer useful frameworks for CII protection in emerging country contexts. Fortunately, while much of the rest of the world continues to lag significantly wealthy, technology dependent nations in Europe, North America and parts of Asia, there now exist quite a few emerging economies with experience in developing, adopting and implementing their own CII protection policies. For example, between 2018 and 2020, the African region added six new National Computer Emergency Responses Teams, increasing the total number of countries from 13 to 19 (out of a total of 44) (ITU 2021, 7).

Critical information infrastructure in emerging economies

While global critical information infrastructure protection approaches can inform the experience of late-digitising emerging countries, such countries face different sets of opportunities and challenges. We draw on the experiences of two emerging economies with significant ongoing critical information infrastructure protection efforts, Nigeria and Egypt, to advance three series of interrelated arguments.

First, emerging, late digitising regions tend to face a mix of sectoral-level risks to their critical information infrastructure that is different from early digitising regions. High income, technology-dependent countries possess a significant cyber-dependent critical infrastructure, and have long feared broad, debilitating attacks by geopolitical rivals. Former US Defense Secretary Leon Panetta (2012) famously warned of a 'cyber-Pearl Harbor' targeting 'computer control systems that operate chemical, electricity and water plants' that could cause 'physical destruction and the loss of life'. For this reason, it is state-sponsored attacks, such as those against Iran's nuclear programme, Russia's attacks on Ukraine's energy grid and the US industrial supply chain, and China's hack of the attacks on the US Office of Personnel Management, that have tended to draw attention from policymakers because of their perceived geopolitical, economic and national security implications.

For emerging economies, state-sponsored threats to critical infrastructure are not insignificant. The Chinese sponsored hack of the African Union (Fidler 2018), the use of Pegasus malware for interstate espionage by countries such as Rwanda and Morocco (Allen and La Lime 2021), and threats against Ethiopia from the Egypt-based Cyber Horus group (Al-Monitor 2022) each attest in various ways to the rising significance of state-sponsored cyberthreats. Nevertheless, for many emerging economies, an 'almost total dependence on imported hardware and software' (van der Waag-Cowling 2020), combined with a relative lack of technology dependent critical infrastructure, may make the threat of a major, devastating state-sponsored cyberattack more remote (Allen and van der Waag-Cowling 2021).

Furthermore, many emerging economies across the world are equally, if not more sensitive, to internal cyberthreats from organised criminal networks, armed groups, or disgruntled insiders within businesses or government organisations who use their privileged access to extort resources. As Mailyn Fidler (2023) argues in her analysis of cyber stability in Africa, 'for many African states, negotiations on the international stage also serve a second goal of increasing government control and regime stability at home' much of which 'comes from African state experiences with conflict and governance by proxy' (284).

Sectorally, perhaps the biggest risks to critical information infrastructure in emerging economies lie in rapidly digitising areas of the economy such as finance, or in the threats to specific single points of failure. Whereas in Europe and the United States, banking companies such as Deutsche Bank, JP Morgan Chase, or Bank of America have enabled the financial sector to remain relatively secure by investing billions of dollars in cybersecurity, the banking sector in much of the emerging world is highly vulnerable (Bursztynsky 2021). In part, this is because local banks in emerging economies do not have the same degree of resources as their counterparts based in higher income countries. But it is also because the financial sector landscape in these countries is more diverse, with the

explosion of growth in the mobile payment sector. The African region, for example, has become a global leader in digital finance in part because companies like Kenya's MPESA offer convenient, affordable means for underserved individuals to store and transfer money. As these mobile payment networks have grown, however, they have also become increasingly insecure and subject to an array of novel kinds of cyberattacks (INTERPOL 2020; Augustine 2022).

In addition, whereas higher income regions of the world face the problem of needing to protect an abundance of CII, the scarcity that exists in many emerging economies poses its own series of challenges: the existence of 'single' points of failure that, if attacked, have significant economic implications. The Global North, for example, has the luxury of being served by dozens of undersea internet cables, such that the cut of one or two cables does not much affect internet speeds in places such as Tokyo or Madrid. In places such as Mauritania and South Africa, however, undersea cable cuts have meant days, weeks or even months of limited or significantly degraded internet access (Baynes 2018; Browdie 2020; Fidler 2023). There is perhaps no better illustration of the risks posed by cyberattacks on single points of failure than the 2021 attack against South Africa's state-owned port operator, Transnet, which briefly brought shipping – and thus a significant chunk of economic activity – across the entire South African region to a halt (Reva 2021).

Second, and relatedly, critical information infrastructure protection efforts in emerging economies are hampered by deficits in physical and human resources. When it comes to physical capital and resources, much of the extant critical infrastructure that exists in emerging economies across the world does not have or cannot afford state of the art systems or software. Instead, enterprises who manage and protect CII tend to rely more on outdated platforms and older machines, and often critical infrastructure that is a hybrid mix of both existing legacy infrastructure and newer systems (Allen and van der Waag-Cowling 2021).

Similar challenges exist with respect to human resources. Across the world, there exists a well-documented gap in the number of qualified cybersecurity professionals and open positions. However, whereas in high income countries, this gap is driven in part by a tendency on the supply-side to seek certified, and at times, overqualified applicants for entry level jobs (ISC2 2022), in emerging economies, the issue is as much to do with a lack of qualified entry-level applicants. Leading publications and practitioners often opine how easy it is to learn basic cybersecurity skills through online courses offered by platforms such as Coursera or Udemy (Brown and Tomaschek 2022; Gupta 2022). However, even basic cybersecurity training requires literacy, programming knowledge, access to a personal computer, and internet connectivity, luxuries which remain out of reach for much of the world's population. For nations who face what they perceive to be choices between investing in critical infrastructure cybersecurity and more basic needs surrounding the need for access to education and digital connectivity, the latter is often, and with some justification, prioritised over the former.

In part as a result of these resource constraints, our analysis calls into question simplistic narratives about whether digitisation offers, in part through the development of critical information infrastructure, the opportunity for emerging economies to 'leapfrog' wealthier, more digitised nations. To be sure, late digitising countries do receive significant benefits in being able to learn from the experiences and adapt from state-of-the-art policies, strategies and infrastructures from wealthier, highly digitised regions of the world (Soete 1985; Fong

2009). There has been much innovation, and a significant amount to learn from how policymakers and practitioners in emerging countries have adapted CII protection standards to their local contexts. And insofar as emerging economies seek to build out and prioritise their existing energy, telecom, transportation, financial and public service infrastructure, opportunities to leapfrog wealthier regions of the world do exist.

Nevertheless, our analysis also suggests that leapfrogging efforts face serious obstacles. So long as emerging economies cannot afford state of the art systems, software, or investments in human resources, their critical infrastructure is likely to remain more vulnerable than in higher income countries. And insofar as their critical infrastructure in sectors such as finance and telecommunications is structured differently, with a different mix of technologies and vulnerabilities, than in early digitising countries, emerging economies need to adopt their own, localised, context-specific approaches to identifying and protecting critical information infrastructure. Successful leapfrogging requires 'much more than the mere installation and application of systematized knowledge', but also 'the application of implied knowledge regarding the organisation and management of the technology and its application to the contextual environment in which it is to be used' (Davison et al. 2000). Deficits in resources and different sectoral-level risks suggest that there is no 'one-size-fits-all' approach to CII protection, and that emerging economies would do well to prioritise adopting context-specific policies, processes and legal frameworks to mitigate what are likely to be persistent deficits in their ability to adopt state of the art systems and updated software (Fidler 2023).

We advance these arguments through case studies of ongoing efforts to protect critical information infrastructure in Nigeria and Egypt. Both emerging economies have internet penetration rates that have rapidly risen and are higher than those in their region, and partially as a result have undertaken CII protection efforts that go back approximately a decade or more. This puts them ahead of many other emerging economies, some of which do not have any type of critical information infrastructure protection policy, so to speak. In this sense, they represent 'typical' cases (Seawright and Gerring 2008) for the kinds of challenges and opportunities many emerging economies are likely to face as internet penetration rates rise, they become more cyber mature, and as they seek to implement CII protection policies and standards of their own. We find that each country has adopted different CII protection policies, which are to some extent a function of differences in factors such as regional politics, geography and regime type. We also find each country has faced shared challenges when it comes to issues such as resource constraints and the spread of mobile money. Taken together, these two findings strongly suggest that emerging economies will not necessarily follow the same trajectory or benefit from the same lessons learned in CII protection as early digitising regions of the world.

Critical information infrastructure protection in Nigeria

Nigeria, home to over 200 million people, is Africa's most populous country and largest economy. Over the past two decades, the country has undergone rapid, if uneven digitisation. As of 2020, approximately 36 per cent of Nigeria's population had internet access, according to the UN International Telecommunications Union. Most of the country accesses the internet via a mobile device, due to the rapid digitisation of the telecommunications sector, where mobile penetration rates have reached over 90 per cent. The

adoption of mobile money is also driving the digitisation of Nigeria's financial sector, though the country remains behind regional leaders such as Ghana, Mauritius and Kenya (Bailey 2022). Nigeria ranks 47th out of 183 countries on the International Telecommunications Union Global Cybersecurity Commitment Index, or 4th in Sub-Saharan Africa.

Nigeria's relatively high ranking is due, in part, to an established national cybersecurity infrastructure, including critical information infrastructure protection policies. CII protection efforts in Nigeria date back to 2014, when the Nigerian government released a strategy on critical information infrastructures protection as part of its initial National Cybersecurity Strategy (NCS) (Republic of Nigeria 2014). This strategy was updated with the release of a 2021 National Cybersecurity Policy and Strategy (NCPS) (Republic of Nigeria 2021). Efforts to implement the recommendations in both strategies are ongoing.

Closely mirroring accepted international standards, the NCPS defines CII as 'any system, network and infrastructure that underpins our national life and ensures our existence and survival as a country.' This broad definition means that any digital device, process, or infrastructure whose disruption could lead to undermining Nigeria's economic prosperity, social wellbeing and national security is considered critical information infrastructure. The latest NCPS also identifies 13 sectors of the Nigerian economy as essential for protection against physical, human and cyber related threats. These sectors include Power and Energy, Water, Information Communications, Science and Technology, Banking/ Finance and Insurance and Health, Public Administration, Education, Defence and Security, Transport, Food and Agriculture, Safety and Emergency Services, Industrial and Manufacturing and Mines and Steel. These sectors, virtually all of which are included in the NIST, illustrate that internationally accepted definitions and standards have played an important role in defining Nigeria's broader approach to critical infrastructure protection.

The infrastructure that is in the process of being set up to enable Nigeria to protect CII is more reflective of Nigeria's local context and bureaucratic imperatives. The overall responsibility for cybersecurity in Nigeria resides with the Office of the National Security Adviser. The 2021 NCPS has recommended the establishment of a National Cybersecurity Coordination Centre (NCCC) to coordinate and facilitate cybersecurity at strategic, operational and tactical levels across the government and private sector. The establishment of these institutions came from extensive consultations within government and with private sector, civil society and independent bodies like the Cyber Security Experts Association of Nigeria (Allen and Ajijola 2022). The NCCC is intended to balance the need for high-level leadership and the need for security sector actors to play a central role with an inclusive, multistakeholder approach to ensure that citizens and the private sector are actively involved in the design, implementation, and protection of CII. The NCCC has, however, yet to become fully operational, in part because the strategy did not contain dedicated funding allocated to setting it up (Allen and Ajijola 2022).

A significant fraction of Nigeria's critical information infrastructure is owned or operated by the private sector, which is primarily responsible for the security of these systems. Protection of these critical assets is a shared responsibility that cuts across both government and owners and operators. Owners and operators of these assets are therefore required to register them in a database created by the government. The NCPS calls for the establishment of a Trusted Information Sharing Network (TISN), overseen by the NCCC, to enable owners and operators to collaborate with one another to share information and mitigate cyber risk. Trusted Information Sharing Networks were

first established by the Australian government in 2003, and considered an international good practice (OECD n.d.). The NCCC provides an oversight function to coordinate activities of stakeholders and provide necessary information on threats and vulnerabilities that affect these assets as well as mitigation mechanisms to be shared via the TISN. Though TISNs do not appear to have begun to mitigate cyber risk (OECD n.d.), such information sharing mechanisms to enable the protection of CII are becoming increasingly common throughout the world.

While much of Nigeria's formal institutional architecture might not differ significantly from international standards and good practices, Nigeria faces its own unique mix of risks, challenges and vulnerabilities at the sectoral level. This becomes evident when examining the threat landscape and ongoing response efforts in the finance, energy and defence sectors, which, according to threat analysis from firms such as KPMG (2022), are among the region's most vulnerable. In high income countries, bank account ownership is nearly universal among adults (World Bank 2021, 15), and large, multinational banks who devote significant portions of their resources to prevent fraud and cyber theft dominate the market. Nigeria's financial landscape is far more diverse. As of 2021, only 45 per cent of Nigerian adults own a bank account, up from 30 per cent of the population in 2011 (Bailey 2022). Much of this increase has been driven by the adoption of mobile money, which stood at 9 per cent of the population in 2021, and, with a more than doubling of the number of financial transactions through mobile devices between 2021 and 2022, appears to be rapidly growing (World Bank 2021; Bailey 2022). The migration from physical to online banking, the need for digital service providers to keep up with the digital appetite of end users, and increase in technology dependent financial platforms have contributed to the expansion of the attack surface for this sector.

It has also led to a distinct set of challenges. With so much of the population remaining unbanked, financial access and inclusion, not cybersecurity, remain the Nigerian banking sector's biggest challenge. According to a report by the KuCoin (2022), the volatility of the naira and the lack of access to other forms of banking has led up to 35 per cent of Nigeria's adult population to trade in cryptocurrency, which given the recent collapse of major exchanges such as FTX, poses its own set of cyber risks. In the traditional banking sector, it is insider threats, rather than externally driven cyberattacks, that constitute the biggest threat (Vanguard Nigeria 2021). At the same time, Nigeria's commercial banking sector has faced a mass resignation of software engineers, who have secured better paying jobs in the Global North (Idowu and Ibeh 2022). Taken together, this strongly suggests that Nigeria's formal institutional architecture will not be sufficient without investments in human resources, mitigation measures that are tailored to reduce insider threats, and broader efforts to retain talent and offer a more diverse array of financial services to citizens.

Though the country has made some investments in the digital transformation of its electricity, oil and gas sectors, Nigeria's power sector has yet to record any significant disruption as a result of a cyberattack (Elemide 2021). In part this is due to a relatively small attack surface compared to other regions of the world. It is not, however, due in any meaningful sense to 'leap-frogging'. Despite a growing dependence on digital systems, Nigeria's power system, according to experts, is best characterised as a traditional and centralised grid system which has been upgraded to a hybrid configuration consisting of legacy equipment and automated systems. The digitised portions of Nigeria's power

grid are potentially quite vulnerable to cyberthreats, even as the power grid continues to rely substantially on legacy systems and infrastructure.

Digitisation also has exposed Nigeria's power grid to potential 'single points of failure' that, if attacked, could have significant consequences. In a security assessment of Nigeria's upgraded power system, researchers warn that a cyberattack on the electric power system, especially the centralised transmission system, would have a significant impact on electricity supply, most likely leading to blackouts across the country (Ogundari et al. 2021). This 'single point of failure' renders Nigeria vulnerable despite the small attack surface. Despite these concerns, the prospect of a cyberattack does not rank all that high on the list of concerns faced in Nigeria's power sector. Eighty-five million Nigerians, or 43 per cent of the country lack access to electricity, and even for those with access, the electricity grid is far from consistent or reliable (World Bank 2021). As with the finance sector, regulators face legitimate questions over whether they should be prioritising cybersecurity over expanding access to reliable power.

Finally, in the defence sector, Nigeria is one of the few African countries to have set up an Army Cyber Warfare Command, consisting of an offensive force of up to 2,000 people (O'Flaherty 2018). The main impetus for the Command appears to have been the rise of the Boko Haram insurgency, which has harnessed the spread of cellular technology and social media for purposes of recruitment, defaced the website of the Nigerian Defence headquarters, and was accused of hacking the website of the country's electoral commission on election day (O'Flaherty 2018). In addition to a mandate to protect critical infrastructure, the broad remit of the Command is to 'monitor the Nigerian Army's networks and advise field commanders on how to use the computer-based weapons systems' (ibid). While these activities are similar to the cyber units of other nation states, the focus on internal threats is unusual and potentially assumes responsibilities for CII protection that in most other contexts are left to domestic authorities. In countries widely considered to have a high degree of cyber maturity, such as the United States and China, the main mission of offensive cyber units is to conduct operations against nation-state rivals or foreign cybercriminal actors with sophisticated cyber capabilities and global reach.

Nigeria has clearly made significant strides to protect its critical information infrastructure over the past decade. And while the country's formal institutional architecture to protect CII has been clearly informed by international good practices from early digitising countries, the country faces a distinct set of challenges, from the prioritisation of service delivery and access over cybersecurity to cyberthreats from homegrown insurgencies, to which this institutional architecture must adapt.

Critical information infrastructure protection efforts in Egypt

Egypt, located in North Africa, is the most populous country in the Arab world, home to over 100 million people and possessing over $1 trillion real (PPP) GDP (CIA 2023). Since the mid-1980s, Egypt has heavily invested in its ICT infrastructure and info-structure as one of the key building blocks for development (Kamel 2021; El Sherif and El Sawy 1988). Currently, over 70 percent of the population use the internet and possess near-universal cell phone access (Egypt Ministry of Communications and Information Technology 2023). These high rates of internet penetration, which have nearly quadrupled over the course of the previous decade, coupled with the country's strategic location, and concerted education and

awareness-raising efforts by government officials have each contributed to the emergence of Egypt as a regional, and even global, leader in cybersecurity. It ranks 23rd in the ITU's cybersecurity index (ITU 2021). Egypt's CII protection institutions date back to 2009, when the National Telecom Regulatory Authority (NTRA) established Egypt's Computer Emergency Readiness Team (EG-CERT). It was among the first countries in its region to create a CERT, which was first created at Carnegie Mellon University under a US government contract and has since become globally accepted good practice recommended and measured by organisations such as the United Nations' ITU (2014; 2021). Egypt's Computer Emergency Readiness Team is the country's focal point for CII protection and was founded to support the ICT, then the financial and government sectors, and anticipate and recover from cybersecurity threats through incident handling, cyber forensics, malware analysis, vulnerability assessment, and penetration testing (Hashem 2017; 2019). The establishment of EG-CERT predates the founding of the country's main cybersecurity institutions, whose development its technical expertise helped inform.

Between 2009-2010, a $1.2M national cybersecurity training programme was funded, organised and sponsored by the National Telecom Regulatory Authority (NTRA), for training 220 professionals in 38 organisations within the governmental/public sector, banking sector, education sector, and ICT sector (Hashem 2019). The programme resulted in close to 200 cybersecurity professionals receiving international accreditation on technical cybersecurity skills including incident handling, perimeter security, and penetration testing. The nation programme had a 'positive impact in creating awareness, enhancing readiness, and establishing a network of trust and enhanced cooperation spirit among participating entities as well as among professionals' (Hashem 2019, 90). The success of that pilot training programme, along with other capacity building initiatives, resulted in a perfect score (1.0) on cybersecurity capacity building, as measured by the Global Cybersecurity Index (GCI) of the International Telecommunications Union (ITU 2014), and contributed to the advanced cybersecurity readiness rank that Egypt achieved in 2015 (28th among 195 countries) (ITU 2015). This experience illustrates that, despite limited resources, some degree of leapfrogging is possible with investments in human capital and policy infrastructure in place. Nevertheless, like Nigeria, the loss of human capital in cybersecurity due to challenging economic conditions is a perennial problem. Egypt's national cybersecurity strategy, adopted in 2017, identifies seven key domains of critical information infrastructure, and the protection of CII has been a focal point for the country's cybersecurity institutions. Article (31) of the Egyptian constitution, adopted in 2014, states 'a safe and secure cyberspace is essential for the Egyptian economy and is a main pillar of Egypt's national security.' Shortly after the constitution was completed, the government formed a ministerial-level Supreme Council for Critical Information Infrastructure Protection and Cybersecurity (often called the Egyptian Supreme Cybersecurity Council, or ESCC). The ESCC is chaired by the Minister of Communications and Information Technology and has members from the critical sectors as well as the key security agencies (ESCC 2017). The ESCC is the lead body charged with the protection of CII and in 2017 drafted, and since has been charged with implementing, the country's National Cybersecurity Strategy. A key goal of this strategy is to 'confront cyberthreats and enhance confidence and security of the ICT infrastructure, and its applications and services in various critical sectors, in order to create a safe, reliable, and trusted digital environment for Egyptian society.'

Egypt also has yet to spell out in detail the CII in each sector worthy of protection. The 2017 National Cybersecurity Strategy mentions the seven 'Most-Targeted Critical Sectors' that are the main focus of CII protection efforts: ICT, financial services, energy, transportation, health and emergency services, government services, and information and culture (ESCC 2017, 5–6).

Egypt's cybersecurity policies have aimed to follow international norms and best practices recommended by the UN Government Group of Experts (2015) and the ITU's five working areas: legal/regulatory, technical, organisational, capacity building, international cooperation (Hashem 2019). This, in part, may help explain the country's relatively high GCI ranking.

Egypt does appear to have made more progress than Nigeria in operationalising its CII protection architecture. Since its founding EG-CERT has grown from a staff of six to a staff of over 80, writes hundreds of yearly reports, leads a national cyber drill, and has trained teams from 30 entities across the Egyptian government and the critical sectors. Progress has been particularly rapid in the financial sector where the country's first sectoral level CERT was established in 2018 by the Central Bank of Egypt (CBE). Amid rising digitisation and threats to the sector due to the COVID-19 pandemic, the Central Bank developed a Financial Cybersecurity Framework and established a Cybersecurity Division with a staff of 90. It has completed a cybersecurity readiness assessment at the 10 largest Egyptian banks, trained 200 financial sector cybersecurity professionals, and is aiming to bring the cybersecurity posture into compliance with international standards such as the NIST Cybersecurity Framework, ISO 27001/27002, CIS controls, and PCI-DSS. This training programme was financially supported by participating banks, which were increasingly becoming subject to cyberattacks.

Even as authorities move to secure Egypt's traditional banking sector, authorities face similar questions to their counterparts in Nigeria with questions concerning how to reconcile the cyber risk posed by the adoption of mobile money with the need for financial inclusion and access. In the wake of the COVID-19 pandemic, mobile money and e-transactions grew rapidly, by 175 per cent between 2020 and 2021 (Mazloum 2022). This growth has been driven because of the mobile money's utility in providing financial access to Egypt's adult population, a majority of which is unbanked (World Bank 2022). The growth of mobile money, in turn, has led to an explosive growth in fraud and phishing. According to the cybersecurity research firm Kaspersky, over 50 per cent of digital wallet users in Egypt have been attempted victims of phishing via text message, phone calls, or fake websites, though users surveyed expressed a high degree of awareness regarding these threats (Daily News Egypt 2022). This strongly suggests that, as in Nigeria, Egyptian authorities will need to calibrate their efforts to protect the financial industry to both meet the needs of a large unbanked population and address the somewhat specific kinds of cyber risk posed by the spread of mobile banking.

If the Egyptian financial sector faces a threat environment that in many ways mirrors that of Nigeria, Egypt's geography means that authorities are more concerned about externally motivated cyberthreats. One reason why Egypt possesses relatively robust cyber defence capabilities may be explained by the fact that 16 undersea cables, or 17 per cent of the world's internet traffic, passes through its borders (Burgess 2022). With a reasonable amount of frequency, Egypt's critical infrastructure has been caught up, targeted or compromised by cyberattacks from Iran, widely recognised to possess among

the world's most sophisticated offensive cyber capabilities. Hackers working for Iran or its proxy, Hezbollah, have been attributed to cyberattacks against Egypt's health ministry, telecommunications companies, internet service providers, and political and military organisations (ClearSky Cyber Security 2021; Center for Strategic and International Studies 2022, 22; Council on Foreign Relations 2022).

Despite these threats, Egypt possesses no known, publicly acknowledged offensive cyber capabilities. Though it ranks high on the ITU index, it ranked the lowest in Harvard's National Cyber Power Index, which ranked 30 cyber mature countries according to 'cyber intent and capability' (Voo et al. 2020). One possible explanation for this is that Egypt's emerging economy status means that it lags behind wealthier neighbours in terms of the investments in national ICT infrastructure, human capital, and resources. According to one analyst, 'the existence of sophisticated cyber weapons seems highly unlikely, as there is little evidence to suggest Egypt has the capacity or resources necessary to develop these capabilities in-house' (Shea 2021).

Egyptian authorities may also be reluctant to claim responsibility for cyberattacks or publish information about their cyber capabilities (Voo et al. 2020, 33). Attacks by the Egypt-based Cyber Horus Group on Ethiopian government websites over the filling of the Nile Grand Renaissance Dam, a hot button political issue between the two nations, would certainly appear to align with broader Egyptian foreign policy goals, even if there is no known linkage between the Cyber Horus Group and the Egyptian government (Shea 2021). Likewise, Egypt has invested heavily in tools of surveillance to monitor terrorists and cybercriminals. However, there are speculations that their use extends to suppress internal dissent, particularly in the aftermath of the Arab Spring (Hassib and Shires 2021). In this sense, Egypt's broad, and expansive definition of CII may be deliberate, allowing authorities to include the content produced by citizens as broader threats to information security (Shires 2018). Unfortunately, digital surveillance has become widespread at a global level (Zuboff 2019).

As with Nigeria, Egypt's experience with CII protection suggests that emerging economies have been informed by the experience of early digitising countries, but have also adapted these norms to suit their specific threat environment. Like Nigeria, Egypt's experience as an emerging economy means that, to some degree, the protection of CII must be balanced with or subsumed into broader efforts to build out economic infrastructure in key sectors. Given Egypt's geography, expansive definition of critical infrastructure, and perceived internal and external threat environment, it is perhaps of little surprise that Egypt has made the protection of CII a priority. Finally, Egypt's rapid rise up the global cybersecurity commitment rankings demonstrates how the human factor is central to cybersecurity efforts. In the banking and telecom sectors, concerted efforts by Egyptian authorities to set up robust institutional structures, train and provide career paths for cybersecurity professionals, and provide funding through public-private partnerships with banks or other private sector institutions appear to have been crucial in enabling Egypt to build cyber capacity despite limited resources. So far, other critical sectors have not launched similar initiatives, and are thus lagging behind in cybersecurity capacity building efforts.

Conclusion and policy implications

The experiences of Nigeria and Egypt offer several important lessons for scholars and policymakers seeking to improve and update CII protection across the world. Firstly, is the

need for existing CII norms and standards to become better informed by the realities faced by emerging economies, and for emerging economies to carefully interpret and adapt existing standards to their local context. Though both Nigeria and Egypt have succeeded in some important respects in adapting formal institutional architectures, such as computer emergency response teams, cyber coordination centres, and trusted information sharing networks into their CII protection architecture, they face a different mix of risks and challenges than most countries in the Global North. For example, evidence from both cases suggests that emerging economies may need to adopt novel policy and institutional frameworks to address the cybersecurity risks to their financial sectors posed by the spread of mobile money. Experience from both countries also suggests that emerging economies may need to place specific policies in place to address the issue of brain drain through measures such as devising appropriate career paths, financial incentives and networking opportunities, as Egypt's efforts to build cybersecurity resilience in its banking and telecom sectors can attest. Both cases illustrate a compelling need for states to tailor their national cybersecurity strategies to cyberthreats that are specific to their environment: in Nigeria's case, the cyber-enabled threat posed by armed non-state actors, and in Egypt's case, the protection of strategically important undersea cables.

Secondly, both countries, in various ways, face duelling imperatives of the need to upgrade their critical infrastructure, prioritise, and ensure cybersecurity in an environment of limited financial resources and human capital compared to wealthier regions of the world. Without either massive investments in cyber capacity building efforts or prioritising resources towards the protection of potential single points of failure in the most vulnerable sectors, evidence from both cases suggest that emerging economies may struggle to adequately protect their CII. Innovative funding models that leverage public-private financing or international partnerships are needed. The Central Bank of Egypt's reliance on banks to fund cybersecurity training provides one potential model. Another relevant experience comes from another African country, Togo, whose National Computer Emergency Response Team achieved financial independence by choosing a public-private partnership (PPP) model to raise funding (Hountomey et al. 2022b).

Finally, and perhaps most importantly, the experiences of both countries illustrate how much global CII protection efforts have to gain by more closely examining the experiences of emerging economies in less digitising regions of the world rather than aspiring to the standards of wealthy, early digitising economies. Evidence from both countries suggests that while 'leap-frogging' can be challenging in countries with limited resources to invest in advanced technology, efforts to invest in human capital and policy processes can yield big dividends. Organisations that consider themselves to be global standard-setters, such as the NIST, the Internet Society or the ITU, should in partnership with regional organisations, such as the African Union, the Forum of Incident Response and Security Teams (FIRST) and the Global Forum on Cyber Expertise (GFCE), offer more concrete guidance and capacity building assistance policymakers in emerging economies, seeking to adopt contextualised approaches to CII protection within their countries.

Despite their challenges, both countries have undertaken relatively robust CII protection efforts in comparison to peer nations. Other countries might learn from Nigeria's relatively inclusive approach to devising and implementing its national cybersecurity strategy and policy, as well as efforts to prioritise the protection of the nation's most vulnerable CII

and single points of failure. Likewise, Egypt's approach of starting with a relatively small group of technical experts and using that as a starting point to leverage innovative models of funding to train a cadre of cybersecurity experts and build national-level technical capacity to protect CII might also offer an important lesson learned for countries seeking to jump-start their CII protection efforts.

Notes

1. The opinions expressed in this article represent those of the authors and not the institutions at which they are affiliated. The authors would also like to thank Marian 'Ify' Okpali for the excellent research assistance she provided for this article.
2. Though the terms 'critical infrastructure' and 'critical information infrastructure' are at times used interchangeably, for the purposes of this article, we follow the distinction proposed by Maglaras et al. (2018), taking 'critical information infrastructure' to specifically refer to interconnected digital systems whose operation is necessary for the functioning of critical infrastructure across multiple sectors.
3. For an exception, see Hountomey et al. (2022a, 2022b).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Nate Allen is Associate Professor of Security Studies at the Africa Center for Strategic Studies at the National Defense University. His expertise includes cyber issues, emerging technology, civil–military relations, and regional security partnerships, primarily in North and West Africa. His work has appeared in a wide range of peer-reviewed and leading policy-oriented publications, including *Armed Forces and Society*, *The Washington Quarterly*, *Democratization*, *Orbis*, *War on the Rocks*, *The Washington Post*, and *Foreign Affairs*. He oversees the Africa Center's academic programming on cyber issues and emerging technology. He is a term member of the Council on Foreign Relations, and has received fellowships from American University, the Robertson Family Foundation, and the U.S. Institute of Peace. He holds a PhD in African Studies from Johns Hopkins University's School of Advanced International Studies and an MPA in development studies from Princeton University's School of Public and International Affairs.

Sherif Hashem is a Full Professor at GMU's Information Sciences and Technology Department. He is interested in interdisciplinary academic and professional activities, with a special focus on cybersecurity and artificial intelligence applications, Management of Technology, Data Analytics, Digital Transformation, Cyber Strategies and Policies, and Cyber Diplomacy. He has 5 published book chapters and over 60 refereed articles in international journals and conference proceedings, with more than 2500 citations. Dr Hashem is currently a member of the Board of Directors of FIRST (Forum of Incident Response and Security Teams), and a member of the African Union's Cybersecurity Expert Group (AUCSEG). He is a Senior IEEE member and an ISACA Certified Information Security Manager (CISM). Dr. Hashem received a Ph.D. in Industrial Engineering from Purdue University-USA, a M.Sc. in Engineering Mathematics and a B.Sc. in Communication & Electronic Engineering from Cairo University-Egypt.

Elizabeth Kolade is a Ph.D. candidate at the University of Bristol and a former team lead of Nigeria National Space Defense Administration's computer emergency response team. Elizabeth served as a member of a committee to review Nigeria's National Cybersecurity policy and strategy (NCPS) 2015 and produce the NCPS 2021. Elizabeth is a Fellow of the Young African Leaders Initiative (YALI) and has been a part of several multi-stakeholder engagements on Cyber Security within and beyond

Africa. She was listed as one of the Top 50 Women in Cybersecurity in Africa in 2020. In 2021, she was named a Global Influencer in the IFSEC Global Awards under the 'Security – One to Watch' Category. She is a long-serving member of the Cyber Security Experts Association of Nigeria (CSEAN) and remains an avid advocate for the education of women in technology.

ORCID

Nate Allen http://orcid.org/0000-0002-1126-4306

References

African Union. 2014. "African Union Convention on Cyber Security and PersonalData Protection." https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Al-Monitor. 2022. "Ethiopia Faces New Cyberattacks on its Nile Dam." *Al-Monitor*, May 17.https://www.al-monitor.com/originals/2022/05/ethiopia-faces-new-cyberattacks-its-nile-dam.

Allen, Nathaniel. 2021. "The Promises and Perils of Africa's Digital Revolution." *Brookings*, March 11. https://www.brookings.edu/articles/the-promises-and-perils-of-africas-digital-revolution/.

Allen, Nate, and Abdul-Hakeem Ajijola. 2022. "African Lessons in Cyber Strategy." *Africa Center for Strategic Studies*, March 8. https://africacenter.org/spotlight/african-lessons-in-cyber-strategy.

Allen, Nathaniel, and Matthew La Lime. 2021. "How Digital Espionage Tools Exacerbate Authoritarianism Across Africa." *Brookings Techstream Blog*, November 19. https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/.

Allen, Nathaniel, and Noëlle van der Waag-Cowling. 2021. "How African States Can Tackle State-backed Cyber threats." *Brookings Techstream Blog*, July 15.https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/.

Augustine, Abraham. 2022. "How Cybercriminals Target Africa's 500 Million Mobile Subscribers." TechCabal, July 5.https://techcabal.com/2022/07/05/how-cybercriminals-target-africas-500-million-mobile-subscribers/.

Bailey, Bunmi. 2022. "Mobile Money Adoption Drives Nigeria's Banking Penetration to Record High." *Business Day*, July 6. https://businessday.ng/financial-inclusion/article/mobile-money-adoption-drives-nigerias-banking-penetration-to-record-high/.

Baynes, Chis. 2018. "Entire Country Taken Offline for Two Days After Undersea Internet Cable Cut." *Independent*, April 11.https://www.independent.co.uk/tech/mauritiana-Internet-cut-underwater-cable-offline-days-west-africa-a8298551.html.

Browdie, Brian. 2020. "South Africans Under Lockdown Have to Deal with Slow Internet After Another Undersea Cable Break." *Quartz*, March 30. https://qz.com/africa/1828436/lockdown-south-africa-Internet-slows-as-submarine-cable-snaps.

Brown, Shelby, and Attila Tomaschek. 2022. "Learn Cybersecurity Skills with These 4 Online Courses." *cent*, Aug 1. https://www.cnet.com/tech/services-and-software/learn-cybersecurity-skills-with-these-4-online-courses/.

Burgess, Matt. 2022. "The Most Vulnerable Place on the Internet." *Wired*, November 2. https://www.wired.com/story/submarine-Internet-cables-egypt/.

Bursztynsky, Jessica. 2021. "Bank of America Spends over $1 Billion per Year on Cybersecurity, CEO Brian Moynihan Says" *CNBC*, June 14. https://www.cnbc.com/2021/06/14/bank-of-america-spends-over-1-billion-per-year-on-cybersecurity.html.

Center for Strategic and International Studies. 2022. "Significant Cyber Incidents Since 2006." https://csis-website-prod.s3.amazonaws.com/s3fs-public/221212_Significant_Cyber_Events.pdf?5RVe0CgIJK0dJqGjbIIJeHORD95oJ_QW.

Chainalysis. 2022. "Global Crypto Adoption Index." *Chainalysis*, September 14. https://www.chainalysis.com/blog/2022-global-crypto-adoption-index/#top-20.

CIA. 2023. *The World Factbook*. https://www.cia.gov/the-world-factbook/countries/egypt/#economy.

ClearSky Cyber Security. 2021. "'Lebanese Cedar' APT." January. https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf.

Council on Foreign Relations. 2022. "Cyber Operations Tracker." https://www.cfr.org/cyber-operations/.
Daily News Egypt. 2022. "More than Half of Egypt's Users Encountered Phishing Attempts During Electronic Payments: Kaspersky." *Daily News Egypt*, July 28.https://dailynewsegypt.com/2022/07/28/more-than-half-of-egypts-users-encountered-phishing-attempts-during-electronic-payments-kaspersky.
Davison, Robert, Doug Vogel, Roger Harris, and Noel Jones. 2000. "Technology Leapfrogging in Developing Countries–An Inevitable Luxury?" *The Electronic Journal of Information Systems in Developing Countries* 1 (1): 1–10.
de-Jong-Chen, Jing, and Bobby O'Brien. 2017. "A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China." *The Wilson Center*. https://www.wilsoncenter.org/publication/comparative-study-the-approach-to-critical-infrastructure-protection-the-us-eu-and-china.
ECOWAS. 2021. *ECOWAS Regional Critical Infrastructure Protection Policy*. https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf.
Egypt Ministry of Communications and Information Technology. 2023. *ICT Indicators Quarterly Bulletin.* https://mcit.gov.eg/Upcont/Documents/Publications_832023000_ICT_Indicators_Quarterly_Bulletin_Q4_2023.pdf.
El Sherif, Hisham, and Omar El Sawy. 1988. "Issue-based Decision Supports Systems for the Egyptian Cabinet." *MIS Quarterly* 12 (4): 551–569. Management Information Systems Research Center: MN-USA.
Elemide, Ada. 2021. "Nigeria: Energy Sector Prone to Cyber Attacks." *The Electricity Hub*, October 27. https://theelectricityhub.com/nigeria-energy-sector-prone-to-cyber-attacks-monguno/.
Ellefsen, Ian, and Sebastian von Solms. 2010. "Critical Information Infrastructure Protection in the Developing World." In *International Conference on Critical Infrastructure Protection*. Berlin, Heidelberg: Springer. https://link.springer.com/chapter/10.1007978-3-642-16806-2_3.
ESCC (Egypt Supreme Cybersecurity Council). 2017. *Egypt National Cybersecurity Strategy 2017-*2021**.** Arab Republic of Egypt. http://www.escc.gov.eg/.
Fidler, Mailyn. 2018. "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts."*Council on Foreign Relations Net Politics Blog*, March 7. https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.
Fidler, Mailyn. 2023. "Infrastructure, Law, and Cyber Stability: An African Case Study." In *Cyberspace and Instability*, edited by James Shires, Robert Chesney, and Max Smeets, 281–288. Edinburgh University Press.
Fong, Michelle. 2009. "Technology Leapfrogging for Developing Countries." In *Encyclopedia of Information Science and Technology*. 2nd ed., 3707–3713. IGI Global.
GFCE (Global Forum on Cyber Expertise), and Meridian. 2017. *The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-makers.* https://thegfce.org/wp-content/uploads/2020/06/gfce-meridian-gpg-to-ciip-1.pdf.
Gosh, Agamoni, and India Ashok. 2017. "WannaCry: List of Major Companies and Networks Hit by Ransomware Around the Globe." *International Business Times*, April 15. https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587.
Gupta, Sakshi. 2022. "How to Learn Cybersecurity on Your Own [get started guide]." *Springboard*, July 19, https://www.springboard.com/blog/cybersecurity/how-to-learn-cybersecurity/.
Hashem, Sherif. 2017. "Establishing a National CERT/CISRT in Egypt." The Proceedings of the 23rd World Multi-Conference on Systemics, Cybernetics and Informatics. *WMSCI* 2019 II:38-43. International Institute of Informatics and Systemics.
Hashem, Sherif. 2019. "Towards a National Cybersecurity Strategy: The Egyptian Case." *Journal of Systemics, Cybernetics and Informatics* 17 (3): 88–94. https://doaj.org/article/bdb9fd2cdd214f56aee0490355dcc37f.
Hassib, Bassant, and James Shires. 2021. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity* 7 (1): 1–16. https://doi.org/10.1093/cybsec/tyaa026.
Hountomey, J., H. Bahsi, U. Tatar, S. Hashem, and E. Dubois. 2022a. "Cyber Incident Management in Low-income Countries - Part 1." Global Forum for Cyber Expertise and AfricaCERT. https://

cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/.
Hountomey, J., H. Bahsi, U. Tatar, S. Hashem, and E. Dubois. 2022b. "Cyber Incident Management in Low-income Countries - Part 2." Global Forum for Cyber Expertise and AfricaCERT. https://cybilportal.org/wp-content/uploads/2022/01/CSIRTs-In-Low-Income-Countries-Final-Report-part-2-v16.pdf.
Idowu, Bukola, and Royal Ibeh. 2022. "Mass Resignation of Software Engineers Disrupts Banks Digitisation Move." *Leadership*. https://leadership.ng/mass-resignation-of-software-engineers-disrupts-banks-digitisation-move/.
Internet Engineering Task Force (IETF). 2007. *Internet Security Glossary, Version 2.* https://www.rfc-editor.org/rfc/rfc4949#page-9.
Internet Society and the African Union. 2017. *Internet Infrastructure Security Guidelines for Africa*. https://www.internetsociety.org/wp-content/uploads/2017/08/AfricanInternetInfrastructureSecurityGuidelines_May2017.pdf.
INTERPOL. 2020. *Mobile Money and Organized Crime in Africa*. INTERPOL/ENACT Analytical Report. https://enact-africa.s3.amazonaws.com/site/uploads/2020-06-23-interpol-mobile-money-in-africa-report.pdf.
ISC2. 2022. *(ISC)^2 Cybersecurity Workforce Study*. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.
ITU (International Telecommunications Union). 2008. *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts*. ITU-D Secretariat.https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.
ITU (International Telecommunications Union). 2014. *Global Cybersecurity Index Results for Arab Region*. ITU-D Secretariat. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_2014_Results_for_Arab_Region.pdf.
ITU (International Telecommunications Union). 2015. *Global Cybersecurity Index and Cyberwellness Profiles*. ITU-D Secretariat. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.
ITU (International Telecommunications Union). 2021. *Global Cybersecurity Index (GCI)* 2020. ITU-D Secretariat. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.
Kamel, Sherif. 2021. "The Potential Impact of Digital Transformation on Egypt." Economic Research Forum Working Paper. September 2021. https://erf.org.eg/publications/the-potential-impact-of-digital-transformation-on-egypt/.
Kemp, Simon. 2022. "Digital 2022: Global Overview Report." We Are Social / Hootsuite. https://datareportal.com/reports/digital-2022-global-overview-report.
KPMG. 2022. *Africa Cyber Security Outlook*. KPMG. https://home.kpmg/za/en/home/insights/2022/09/africa-cyber-security-outlook-report-2022.html.
KuCoin. 2022. "Into the CryptoVerse Report: Nigeria Edition 2022." *KuCoin*. https://www.kucoin.com/blog/kucoin-is-into-the-cryptoverse-report-reveals-35-percent-of-nigerian-adults-are-crypto-investors.
Lopez, Oscar, and Ephrat Livni. 2021. "In Global First, El Salvador Adopts Bitcoin and Currency." *New York Times*, September 7. https://www.nytimes.com/2021/09/07/world/americas/el-salvador-bitcoin.html.
Maglaras, L.Leandros, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J. Cruz. 2018. "Cyber Security of Critical Infrastructures." *ICT Express* 4 (1): 42–45. https://doi.org/10.1016/j.icte.2018.02.001.
Mazloum, Alaa. 2022. "Expanding Use of E-wallets in Egypt: Strengthening the Social Contract One Transaction at a Time." *Middle East Institute*, March 3. https://www.mei.edu/publications/expanding-use-e-wallets-egypt-strengthening-social-contract-one-transaction-time.
Morgan, Steve. 2019. "Humans on the Internet Will Triple From 2015 to 2022 and Hit 6 Billion." *Cybercrime Magazine*, July 18. https://cybersecurityventures.com/how-many-Internet-users-will-the-world-have-in-2022-and-in-2030/.
Mouton, Jean, and Ian Ellefsen. 2013. "*The Identification of Information Sources to Aid with Critical Information Infrastructure Protection*." 2013 Information Security for South Africa, 1–8. IEEE. https://ieeexplore.ieee.org/abstract/document/6641038.

Musarurwa, Alfred, and Husin Jazri. 2015. "*A Proposed Framework to Measure Growth of Critical Information Infrastructure Protection in Africa*." 2015 International Conference on Emerging Trends in Networks and Computer Communications. IEEE. https://ieeexplore.ieee.org/document/7184813.

Mwai, Peter, and Anita Nkonge. 2023. "Kenya Cyber-attack: Why is eCitizen Down?" *BBC*, July 28. https://www.bbc.com/news/world-africa-66337573.

O'Flaherty, Kate. 2018. "The Nigerian Cyber Warfare Command: Waging War in Cyberspace. *Forbes*, November 26. https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=6febc38d2fb.

OECD (Organisation for Economic Cooperation and Development). 2008. *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures.* https://www.oecd.org/sti/ieconomy/ciip.htm.

OECD (Organisation for Economic Cooperation and Development). n.d. "Trusted Information Sharing Network for Critical Infrastructure in Australia." OECD Toolkit for Risk Governance. https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/trustedinformationsharingnetworkforcriticalinfrastructureinaustralia.htm#tab_results.

Ogundari, Ibikunle, Funso Otuyemi, Abiodun Momodu, and Leye Salu. 2021. "Cyber Security Assessment of Nigeria's Electric Power Infrastructure." *African Journal of Science Policy and Innovation Management* 1 (2): 87–104. https://ajspim.oauife.edu.ng/index.php/ajspim/article/view/79.

Onyago, Seth. 2022. "Africa Accounts for 70% of the World's $1 Trillion Mobile Money Market." *Quartz*, May 4. https://qz.com/africa/2161960/gsma-70-percent-of-the-worlds-1-trillion-mobile-money-market-is-in-africa.

Panetta, Leon. 2012. "Remarks on Cybersecurity to the Business Executives for National Security, New York City." *US Department of Defense News Transcript*, October 12.https://www.hsdl.org/?view&did=724128.

Republic of Nigeria. 2014. National Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf?page=2.

Republic of Nigeria. 2021. *National Cybersecurity Policy and Strategy*. https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf.

Reva, Denys. 2021. "Cyber Attacks Expose the Vulnerability of South Africa's Ports." *Institute for Security Studies*, July 29. https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

Seawright, Jason, and John Gerring. 2008. "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options." *Political Research Quarterly* 61 (2): 294–308. http://www.jstor.org/stable/20299733.

Segal, Adam. 2022. "Cyber Week in Review." *Council on Foreign Relations Net Politics*, October 7. https://www.cfr.org/blog/cyber-week-review-october-7-2022.

Sengupta, Caesar. 2020. "Building a More Inclusive Internet Beyond COVID-19." *Google Blog*, October 28. https://www.blog.google/technology/next-billion-users/new-Internet-users-covid-19/.

Shea, Joey. 2021. "Egypt's Digital Foreign Policy." *Tahrir Institute for Middle East Policy*, February 2. https://timep.org/commentary/analysis/egypts-digital-foreign-policy/.

Shires, James. 2018. "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States." *War on the Rocks*, October 12. https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/.

Soete, Luc. 1985. "International Diffusion of Technology, Industrial Development and Technological Leapfrogging." *World Development* 13 (3): 409–422.

United Nations. 2015. *Report of* the *Governmental Experts on Developments in the Field of Information and Communications Technology in the Context of International Security* UN General Assembly Report A/70/174, July 22. https://daccess-ods.un.org/tmp/8010839.81990814.html.

United Nations. 2021a. *Final Substantive Report of* the *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* UN

General Assembly Report A/AC/290/2021/CRP.2, March 10. 76/135, July 14. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

United Nations. 2021b. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. UN General Assembly Report A/76/135, July 14. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

United States. 2013. *Presidential Policy Directive – Critical Infrastructure Security and Resilience. PDD-21: The White House*, February 12. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/.

United States Department of Homeland Security. 2003. *National Strategy to Secure Cyberspace*. https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf.

van der Waag-Cowling, Noëlle. 2020. "Living Below the Cyber Poverty Line: Strategic Challenges for Africa." *ICRC Humanitarian Law and Policy Blog*, June 11. https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/.

Vanguard Nigeria. 2021. "Fraud in Banking Sector, Mostly Insider Perpetrated – EFCC." *Vanguard*, November 24. https://www.vanguardngr.com/2021/11/fraud-in-banking-sector-mostly-insider-perpetrated-efcc/.

von Solms, Basie, and Elmarie Kritzinger. 2012. "Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa – Has the CIIP and Cyber Security Rubicon Been Crossed?" In *International Conference on e-Infrastructure and e-Services for Developing Countries*, edited by Radu Popescu-Zeletin, Karl Jonas, Idris A. Rai, Roch Glitho, and Adolfo Villafiorita, 116–124. Berlin: Springer. https://link.springer.com/chapter/10.1007978-3-642-29093-0_11.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. 2020. "National Cyber Power Index 2020." https://dash.harvard.edu/handle/1/37372389#:~:text=The%20Belfer%20National%20Cyber%20Power%20Index%20%28NCPI%29%20measures,there%20is%20no%20single%20measure%20of%20cyber%20power.

World Bank. 2021. "Nigeria to Improve Electricity Access and Services to Citizens." *World Bank Press Release*, February 5. https://www.worldbank.org/en/news/press-release/2021/02/05/nigeria-to-improve-electricity-access-and-services-to-citizens.

World Bank. 2022. "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19." https://www.worldbank.org/en/publication/globalfindex.

Zuboff, Shoshana. 2019. "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power." *Public Affairs*.