RESEARCH BRIEF 06/2024
Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Author: Associate Professor N. Allen
(Africa Center for Strategic Studies)

Series Editor: Professor F. Vreÿ (SIGLA)

Advancing critical information infrastructure protection efforts in Africa

Introduction

Africa's critical infrastructure is becoming more dependent on information technology and therefore more vulnerable to cyber sabotage. In recent years, hackers and undersea cable cuts have disabled or degraded service across much of the continent for weeks at a time, West African banks have lost tens of millions of dollars after suffering targeted attacks from sophisticated cybercriminals, and ransomware attacks have disabled electricity grids in Ghana and ports in southern Africa.

The increasing vulnerability of critical information infrastructure (CII) to cyberattack is a world-wide phenomenon. Good practices and standards laid out by entities such as the United States' National Institute of Standards and Technology and the OECD Council's Recommendation for the Protection of Critical Information Infrastructure are meant to inform global CII protection efforts. While these standards can provide a starting point for CII protection policies and strategies in the Global South, not every country's critical information infrastructure protection (CIIP) policies follows the same trajectory or benefits the same lessons learned. A recent study of CII protection policies and practices in Nigeria and Egypt highlights how crucial it is for every country to adopt a context specific approach to CII protection.

Discussion

The experiences of Nigeria and Egypt suggest that in some respects critical infrastructure challenges and opportunities in late digitizing nations in the Global South differ fundamentally from wealthier, early digitizing nations. There are at least three reasons why.

The first reason has to do with the types of technologies and information security resources that need protecting. In much of the Global South, the primary means through which individuals connect to the internet is through mobile devices rather than personal computers. While 'leapfrogging' opportunities such as the adoption of 4G enabled phones and financial payments rather than landlines and credit cards is often perceived as a net benefit, it creates unique challenges in thinking about how best to secure those devices. This has been a problem in Nigeria and Egypt's financial sector, where mobile payment networks are growing faster than traditional banks. With the fintech sector in these two nations and across Africa more broadly a growing target

for cyberattacks, a fundamentally distinct set of CII protection solutions is needed than in wealthier nations, where most financial accounts and transactions are managed by large, multinational banks.

A second reason is that low- and middle- income countries often lack resources to invest in the latest technology and to buy the newest infrastructure. On the one hand, the relative lack of cyber-dependent critical information infrastructure in the Global South lessons what cyber security experts call the 'attack surface' and may make CII easier to protect. On the other hand, the critical infrastructure that does exist often serves significant portions of the population, may rely on outdated software that is particularly vulnerable, and may be single points of failure that, once attacked, can have critical consequences. This was the case with Transnet, South Africa's state-owned port operator that suffered a 2021 ransomware attack that crippled its port navigation software. Because this crucial software was crippled, ports shut down or became constrained across the entire southern African region.

Finally, due to geography or armed conflict, countries may prioritize threats to their CII as emanating from dissimilar sources. Egypt's was one of the first countries in Africa to take steps to protect critical information infrastructure by establishing a national computer emergency response (CERT) in 2009. In part, these early efforts may be because 16 undersea cables compromising a sixth of the world's internet traffic pass through its borders, as well as Egypt's vulnerability to cyberattacks from an aggressive Iran. Both Egypt and Nigeria are also concerned about internal threats to their CII from non-state armed actors. Nigeria's cyber warfare command is one of the few, and perhaps the only, such command explicitly established to combat internal threats, in Nigeria's case from the insurgent group Boko Haram. By contrast, the cyber commands of the world's largest cyber powers, such as the United States and China, tend to conduct operations outside of their borders.

Both Egypt and Nigeria are ahead of other countries with similar income levels in establishing CII protection policies, and there are some more generalizable lessons to be learned from their experiences. Nigeria's multistakeholder approach to cybersecurity strategy and policy has led to a reasonably robust set of institutions designed to mitigate attacks against CII. This includes a national computer emergency response team and trusted information sharing networks (TISN) to protect Nigeria's CII efforts, most of which is in the private sector. Egypt began by investing in international accreditation in 2009-2010 of individuals across its ICT sector and its efforts to create professional opportunities and networks among its cybersecurity community resulted in its CERT growing from 6 to 80 professionals, and the establishment of a sectoral level CERT in 2018 in the banking sector – one of the region's first sectoral CERTs.

Synthesis and conclusions

Like Nigeria and Egypt, countries across Africa who are taking steps to secure their critical information infrastructure need to adopt a context specific approach. While international standards provide an important starting point, each country's approach will be different depending on the type of critical infrastructure it owns and operations, what critical infrastructure investment it would like to make in the future, the nature of that country's threat environment, and available resources and human capital. Countries who adopt CII policies that copy directly or closely mirror standards adopted by the world's early digitizing countries will likely find themselves with significant gaps that neither make wise use of limited resources nor address some of their most significant threats. Prior to establishing CII policies, it is imperative that countries both take steps to define and identify their critical infrastructure assets and assess their vulnerabilities.

In developing and implementing CII protection policies, it is equally important that countries also look for good practices and recommendations from around their region as part of the process. For example, the African Union and regional organizations such as ECOWAS have adopted CII guidelines and resources filled with lessons in CII protection from across Africa. And as the experiences of both Egypt and Nigeria can attest, sound investments in people and processes to secure critical information infrastructure can go a long way in making up deficits African countries may face in wealth and technological resources.

For information: See interactive submarine cable map of the world available at https://www.submarinecablemap.com/

Dr. Nate Allen is Associate Professor with the Africa Center for Strategic Studies and a Research Fellow at SIGLA.

Email: nathaniel.d.allen.civ@ndu.edu