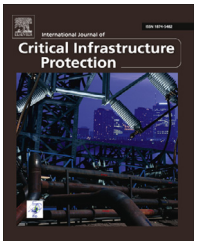
International Journal of Critical Infrastructure Protection 17 (2017) 49–59

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP



Cyber resilience preparedness of Africa's top-12 emerging economies

Ada S. Peter

Department of Mass Communication, Covenant University, Km. 10 Idiroko Road, Canaan Land, Ota, Ogun State 112212, Nigeria

ARTICLE INFO

Article history:
Received 16 March 2015
Revised 20 June 2016
Accepted 15 January 2017
Available online 27 March 2017

Keywords:
Emerging Economies
Africa
Cyber Resilience Preparedness
Cyber Resilience Preparedness Index

ABSTRACT

This paper proposes the Cyber Resilience Preparedness Index for monitoring and comparing the cyber resilience of Africa's top-12 emerging economies. The index covers five critical areas that incorporate a total of 24 indicators derived or adapted from the International Telecommunication Union's 2014 Cyber Wellness Profiles, a Depository Trust and Clearing Corporation white paper on global cyber risk and the well-known Cyber Readiness Index. The final Cyber Resilience Preparedness Index is a simple average of the five area (sub-index) scores; the score for each sub-index is also the simple average of the scores of the composing indicators. This computation assumes that all the sub-indices contribute equally to national cyber resilience preparedness.

The results indicate that six countries, namely Sudan, Ghana, Libya, Zimbabwe, Algeria and Angola, are at risk to compromises of their critical systems. In contrast, Egypt tops the chart of six countries, Egypt, Kenya, Nigeria, Tunisia, Morocco and South Africa, that demonstrate preparedness against compromises to their critical systems, industries and classified documents, as well as against industrial espionage. This study also argues that assessments of the progress of Africa's fastest-growing economies should be conducted periodically using evolving evaluation criteria.

1. Introduction

Africa's economic growth and commercial opportunities are reported as stirring and attractive in the international media. The business attraction is usually attributed to the 300-million-strong and growing middle class concentrated in urban areas, coupled with a youth bulge across the continent [16,21]. These developments bolster the case for Afro-optimism, since the numbers create an internal market of global scale. Africa is home to five of the world's dozen fastest-growing economies and the *per capita* spending income is close to the levels of India and China. This comparatively strong performance over the recent past is beyond the commodity super cycle and boon of debt relief. Improved macroeconomic management has played its part and, increasingly, so has the rise of the African consumer [21].

Despite the optimism generated by the continent's growth and commercial opportunities, there is reason for concern – the increasing reliance of Africa's modern society on networked computer systems. Most countries in the continent are embracing the economic and social potential of the Internet of Everything – the intelligent interconnectivity of people, processes, data and things. The Internet of Everything captures a vast mosaic of social and economic activities in the continent, ranging from millions of daily online transactions, communications and smartphone downloads of TV

E-mail addresses: ada_peter@biari.brown.edu, ada.peter@covenantuniversity.edu.ng

http://dx.doi.org/10.1016/j.ijcip.2017.03.002
1874-5482/

shows and music albums to initiatives such as e-government, e-banking, e-health, e-learning, next generation power grids, air traffic control and other services. All of these are in the agendas of Africa's top emerging economies such as Nigeria, South Africa, Angola, Morocco, Algeria, Tunisia, Egypt, Libya and Sudan. Unfortunately, the reliance on networked computer systems creates unprecedented vulnerabilities coupled with numerous pathways to exploit the vulnerabilities [14].

At least five of the top emerging economies in Africa are listed in the global top-30 countries with the highest Internet penetration [6]. The continent leads in mobile banking – the number of mobile subscribers doubled from 2008 to more than 500 million in 2010 [18]. By 2020, projections indicate that there will be more than 50 billion Internet-connected devices [11]. Moreover, the total data traffic generated by mobile devices is expected to surpass that of wired devices by 2015 [7].

However, these growing statistical estimates imply increased cyber vulnerabilities and dangers that can halt the economic and social development of emerging African economies. Since no nation, agency, industry or company connected to the Internet of Everything is isolated from the new forms of harm (e.g., cyber crime, cyber espionage, cyber terrorism and cyber warfare), cyber weaknesses amidst the increasing Internet penetration could be exploited by criminals, terrorists and possibly nation states to crash critical systems.

It is imperative to prioritize cyber resilience, especially at the public and regional/international policy levels. Indeed, Africa's fastest-growing economies need to be prepared to secure critical documents, systems and industries from cyber threats.

This study adapts the Cyber Readiness Index [9] and the International Telecommunication Union's National Cybersecurity Strategy Guide Framework/Country Profiles [15] to assess the cyber weaknesses of the top-12 emerging economies in Africa that have embraced information and communications technologies and to evaluate the future risks they may face. This study also compares the maturity and commitment of these countries to protecting their cyber investments using an initial objective assessment with regard to cyber security across five areas: (i) availability of a well-articulated national cyber security strategy and legislation; (ii) collaborations, cooperation and partnerships; (iii) technical measures; (iv) capacity building; and (v) availability of information sharing mechanisms. Two research questions are examined:

- What is the cyber resilience preparedness of each country and the future risks it may face?
- What is the maturity and commitment of each country to protecting its cyber investments?

In this paper, cyber resilience refers to the evolving ability to oppose cyber attacks and mitigate the risks. This is essential for individual and interconnected economies to maximize the value inherent in technological innovation. The importance of cyber resilience cannot be overemphasized. It is a key strand of national security. Several studies [3,13,15,20] have linked the importance of cyber resilience to protecting government systems, building partnerships to secure essential non-government cyber systems and helping individual citizens protect themselves online. Indeed, an adequate level of cyber resilience is essential to realizing the full potential of the Internet economy and the digital future [14].

2. Conceptual framework

The recognition and implementation of cyber security initiatives and investments that can preserve the economic and social promise of the Internet economy dividend are critical to emerging economies [24] that have relatively high Internet penetrations [6] and networked readiness [4]. The lack of such cyber initiatives and implementation efforts poses risks that can affect the public and private sectors.

The International Telecommunication Union, which assists stakeholders in building confidence and security in the use of information and communications technology at the national, regional and international levels, has identified five areas necessary for a safer and more secure information society [15]. The five areas are: (i) legal; (ii) technical; (iii) organizational; (iv) capacity building; and (v) cooperation.

While specific approaches and objectives vary by jurisdiction, efforts to date, according to the Depository Trust and Clearing Corporation [9], have focused on four main areas of concern: (i) enhanced protection of national critical infrastructures; (ii) improved information sharing between the public and private sectors; (iii) data breach notifications; and (iv) data privacy.

Hathaway [14] identifies five critical elements for protecting the value and integrity of information and communications technology investments that enable the Internet economy of a country. These critical elements are: (i) articulation and publication of a national cyber security strategy; (ii) availability of an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) to protect against cyber crime; (iii) availability of information sharing mechanisms; (iv) investment in basic and applied cyber security research; and (v) funding for cyber security initiatives.

This study adapts work areas and elements that appear in at least two of the three frameworks mentioned above to create the Cyber Resilience Preparedness Index. The index is a composite indicator that aggregates a number of adapted individual indicators. Specifically, as described below, cyber resilience preparedness is analyzed using five sub-indices that incorporate a total of 24 indicators. Africa's top-12 emerging economies are ranked against the benchmark provided by each indicator. Note that this study only measures the existence of each indicator in a country. Thus, the ranking is based on the existence – not the quality, extent or effectiveness – of the indicators for protecting each nation's cyber investments and critical infrastructure.

3. Methodology

The twelve fastest-growing economies in Africa were selected based on the 2014 World Bank ranking of countries by GDP [24] and the World Economic Forum's 2014 Networked Readiness Index [4]. The Networked Readiness Index measures how countries are embracing information and communications