Cybercrime and Cybersecurity in Africa

By: Nir Kshetri

Kshetri, Nir (2019). "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management*. DOI: 10.1080/1097198X.2019.1603527

Abstract:

Africa has been among the fastest growing regions in terms of cybercrime activities. The continent is also a source of significant cyberattacks targeting the rest of the world. However, a number of measures have been taken to address cyber-threats and improve cybersecurity in the continent. Many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measures. Private sector efforts have also been undertaken to strengthen cybersecurity.

Keywords: Africa | cybercrimes | cybersecurity | general data protection regulation

Article:

Introduction

According to the British consulting firm Ovumone, a billion people in Africa will have Internet access by 2022.[1] Analyzing the trend of cybercrimes across countries, analysts have suggested 10–15% Internet penetration as the threshold level for the generation of significant hacking activities (Kshetri, 2013). Internet penetration rates in many African economies have already reached this level. Bulent Teksoz, of Symantec Middle East noted: "Cybercrime is shifting towards the emerging economies. This is where the cyber criminals believe the low-hanging fruit is". Unsurprisingly many African economies have become important sources as well as victims of cyber-threats.

[1] See https://www.consultancy.africa/news/30/africa-will-break-through-1-billion-mobile-internet-connections-by-2022.

According to Kenya – based IT and business advisory firm Serianu, cybercrimes cost African economies $3.5 billion in 2017. In that year, annual losses to cybercrimes were estimated for Nigeria at $649 million, and Kenya at $210 million. Likewise, according to the South African Banking Risk Information Centre (SABRIC), South Africa loses $157 million annually to cyberattacks.

This editorial looks at cyber-threats originated from Africa and increasing cyber-victimization rates in the continent. It also discusses measures being taken at various levels to address increasing cyber-threats in African economies.

Increasing Cyber-Victimization in Africa

Commenting on Africa's increasing cyber-victimization, Hamadoun Toure, an ex-secretary-general of the International Telecommunications Union (ITU) put this issue this way: "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity".

Symantec had observed 24 million malware incidents that targeted Africa in 2016. In 2013, a Symantec report noted that cybercrime was increasing in Africa at a faster rate than any other region in the world.

In 2016, Ghana's financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails and 280,000 related to botnets.[2]

Some economies in the continent are becoming attractive to cybercriminals, thanks to the high degree of digitization of economic activities. For instance, 86% of South Africans regularly use online banking services. This proportion is higher than many countries in the Middle East and Turkey.[3]

Increasing cyberattacks in the continent can be attributed to vulnerable systems and lax cybersecurity practices. According to Business Software Alliance, two countries with the world's highest software piracy rates in 2017 were from Africa: Libya and Zimbabwe. The proportions of unlicensed software in the two countries were 90% and 89% respectively.[4] Since pirated software products cannot take advantage of updates from manufacturers, they accelerate the spread of malware.

Cybersecurity is considered to be as a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged in the continent. Cybersecurity budgets in many organizations are reported to be less than 1% and many organizations had a zero-budget allocated to cybersecurity (Kshetri, 2013).

---

[2] See https://www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions.
[3] See https://www.htxt.co.za/2018/11/12/kaspersky-lab-report-says-south-africans-most-susceptible-to-online-banking-attacks/.
[4] See https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf.

Even financial institutions, which face biggest cyber-threats, lack proper cybersecurity practices. One study in 2009 showed that 60% of Kenyan banks had insecure systems. According to a 2011 Deloitte study, only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber-threats (Karambu, 2011). Another survey conducted among banks in Kenya, Rwanda, Uganda, Tanzania and Zambia revealed that banks were at high risk from threats, such as hacking, employees with poor sense of security, malicious insiders.

Another problem is related to the lack of skills among Internet users to protect themselves from rapidly rising cyber-threats. Just like in other developing countries, many African Internet users are inexperienced and not technically savvy. A high proportion of them are getting computers and connecting to the Internet for the first time. A majority of them also lack English language. This later point is crucial due to the fact that most of the information, instructions, and other contents for security products are available in English language only. Many African Internet users cannot use cybersecurity products developed in English language.

The continent faces a severe shortage of cybersecurity manpower. It is estimated that Africa will have a shortage of 100,000 cybersecurity personnel by 2020.[5] Just like in the BRICS countries (Brazil, Russia, India, China, and South Africa) (Kshetri, 2015), African economies have faced economic and institutional barriers in developing cybersecurity manpower. For instance, Cameroon which is among the countries worst affected by cybercrime in Africa, was reported to be facing a dilemma to take measures to address the problem. It was reported in 2016 that policy makers in the country were in the process of launching cybersecurity skill development programs. Policy makers, however, feared that after completing the training program, the trainees could use the skills gained to commit cybercrimes.[6]

A final reason concerns weak legislation and law enforcement. Most African economies are characterized by permissiveness of regulatory regimes that provide a fertile ground for cybercrime activities. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. For instance, it was reported that government officials in Nigeria claimed that they were ignorant of cybercrimes originated from the country and some labeled it as Western propaganda. Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives for his alleged engagement in cybercrime-related activities (Kshetri, 2013).

Cybercriminals also benefit from inter-jurisdictional and intra-jurisdictional arbitrage. Following raids on cyber cafés in major cities in Nigeria, cybercriminals were reported to move to remote areas to carry out their operations. The porous national borders and a lack of states' controls on their territories mean that cybercriminals can easily migrate from one jurisdiction to another with a weaker rule of law and enforcement. A Barrister of Nogeria's Economic and Financial Crimes

[5] https://portswigger.net/daily-swig/how-africa-is-tackling-its-cybersecurity-skills-gap.
[6] See https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265.

Commission (EFCC) noted that when Nigeria strengthened its anti-cybercrime measures, cybercriminals were leaving the country and moving to other West African countries.

Global Cyber-Threats from Africa

Cyberattacks originated from African economies have a worldwide effect. Gady (2010) has put it most strongly in his argument that Africa's "Cyber [weapon of mass destruction] WMD" potentially poses a direct threat to the world. For instance, in 2010, 80% PCs used in Africa were infected with viruses and malware (Gady, 2010). Cybercriminals often use these unprotected computers to launch cyberattacks against targets all over the world.

An upshot of the above is that businesses from industrialized countries categorize online transactions originated from Africa as risky. An annual survey of CyberSource released in 2006 ranked Nigeria as the world's riskiest country for online transactions. CyberSource's 2008 similar survey showed that 76% of the North American merchants rejected orders from Nigeria and 58% did so for Ghana (Kshetri, 2013). Likewise, due to a large number of fraudulent clicks from Africa on Internet pay per click advertising, paid-search companies such as Overture have implemented "continental cut-off" services, which reportedly disregard clicks on adverting originated from Africa (Kshetri, 2010).

Measures at Various Levels to Address Cyber-Threats

Several initiatives have been launched and carried out at various levels to improve the continent's cybersecurity landscape. The most important of these is improving regulatory quality.

According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, 11 countries in the continent had specific laws and provisions in place to deal with cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. Additional 12 countries had taken at least some legislative measures, albeit limited. Draft cybercrime laws had been prepared in many other countries and bills had already been presented to national Parliaments in some of the countries.

As of November 2018, Kenya's new data protection bill was ready for review in the Parliament. On the plus side, the bill had many elements of Europe's General Data Protection Regulation (GDPR). For instance, the bill requires organizations to inform users about why their data is being collected, for what purpose that data is used and how long the organization would store the data. The bill also has a provision which gives consumers the right to request organizations to delete their data. In addition, it requires organizations to have a certain level of security standards for storing data. Some analysts expressed concerns about the data localization provision, which makes it illegal to send Kenyans' personal data outside the country. Critics have argued that if this provision is implemented, the Kenyan economy will not be able to benefit from the economic gains that arise from cross-border data flows (Frizell, 2018).

There are also sector-specific regulations. For instance, banking and financial institutions are the most affected sector. In October 2018, the Bank of Ghana issued a Cyber Security Directive for Financial Institutions. The Directive requires active involvement of senior executives and the board to strengthen cybersecurity. All banks in the country are required to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cybersecurity issues, and also formulate adequate measures to manage cyber and information security risks. The Central Bank of Nigeria (CBN) announced that it was developing a risk-based cybersecurity framework for banks and financial institutions. The idea in this framework is to identify the existing gaps and address them. In August 2018, the Central Bank of Kenya asked the country's payments service providers to submit their cybersecurity policies to the government.

Many African economies have also strengthened enforcement measures. In 2017, South Africa's Information Regulatory Authority started the investigation of that year's biggest data breach in the country, in which more than 60 million people's personal data was stolen. The agency also made formal requests to the concerned companies to provide explanations.

Private sector cybersecurity initiatives have also become prominent. In early 2017, Serianu established what it calls a Cyber Immersion Centre in Nairobi. The Center provides an environment for firms to experiment and test their cybersecurity capabilities. It also provides educational facilities to develop cybersecurity professionals. A similar center was opened in Mauritius in mid-2017.[7]

Foreign multinationals have also worked with local organizations to help consumers understand cybercrimes and help develop ethical standards. For instance, Microsoft teamed up with Paradigm Initiative Nigeria (PIN) to educate Nigerians on cybercrimes and to create economic opportunities. The country's EFCC announced in October 2009 that it shut down about 800 websites associated with cybercrimes and arrested 18 cybercrime gangs. The EFCC noted that "smart technology" provided by Microsoft helped.

Discussion and Implications

Businesses and consumers in African economies are facing increasing cyber-threats. This trend underscores the importance of strengthening cybersecurity measures. This means that organizations must increase investment in cybersecurity technologies, provide cybersecurity-related training to employees and appoint professionals such as CISOs. It is also important to create cybersecurity awareness among consumers.

Policy makers in the continent should focus on increasing public awareness of cybersecurity practices and strengthening regulatory and enforcement capabilities in this area. Regulations requiring strong cybersecurity measures in organizations need to be introduced and revised. Initiatives also need to focus on enhancing law enforcement capacities to increase certainty of punishment for those engaged in cybercrime activities.

---

[7] See https://www.consultancy.africa/news/821/it-services-firm-serianu-opens-cyber-security-training-centre-in-mauritius.

Before concluding, we suggest several potentially fruitful avenues for future research. Prior research has noted that cybercrimes targeting developing economies such as those in Africa exhibit a heavy concentration in specific industry sectors. Examples include the online gaming and e-commerce industries in China, the banking and financial sector in Brazil and the offshore outsourcing sector in India (Kshetri, 2013, 2015). In future conceptual and empirical work scholars need to compare and contrast economic sectors facing high profile cyberattacks in major African economies with those in non-African developing economies.

The above discussion indicates that states' control over cybercrime activities and the law enforcement reach of the states have expanded dramatically in recent years in some of the African economies. Some supra-national institutions such as the AUC have also shown interests in fighting cybercrimes. African economies, however, vary widely in their efforts on this front. A second area of future research might be to examine economic, political, and institutional determinants of cybercrime-related legal and regulatory frameworks in African economies.

Various actors are involved in controlling cybercrime activities in Africa. For instance, government agencies such as Nigeria's Economic and Financial Crimes Commission (EFCC), supra-national institutions such as the African Union Commission (AUC) and businesses in the private sector such as Serianu. Organizations and individuals are also strengthening technological and behavioral defense mechanisms to resist cybercrimes. In this regard, a final area of future research would be to compare relative effectiveness of these actors as well as potential challenges they face in controlling cybercrimes.

Concluding Comments

Cyberattacks targeting as well as originated from African economies are rising rapidly. However, there are many positive and encouraging signs. Cybersecurity legislation and enforcement measures in the continent are gradually improving. A variety of private sector initiatives have arisen that will help to strengthen the continent's cybersecurity landscape.

Nir Kshetri is Professor at University of North Carolina-Greensboro. He has authored eight books and more than 130 articles in various journals. In December 2018, he spoke at the Plenary Session, Digital Technology and Sustainable Development: South-South Cooperation in the Digital World at the Hong Kong Summit of the United Nations Office for South-South Cooperation (UNOSSC). Nir has been quoted/interviewed and/or his work has been featured by hundreds of media outlets worldwide. In 2018, he gave a TED Talk about the potential roles of cryptocurrencies in fighting poverty.

References

Frizell, S. 2018. How kenya's new data privacy bill could hurt its economy, Accessed November 8, 2018. https://www.cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy.

Gady, F. S. 2010. Africa's cyber WMD, Accessed March 24, 2010. http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd?page=0,0.

Kshetri, N. (2010). The economics of click fraud. *IEEE Security & Privacy Magazine*, 8(3), 45–53. doi:10.1109/MSP.2010.88

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global South*. Basingstoke, U.K: Palgrave Macmillan: Houndmills.

Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, 18(4), 1–5. doi:10.1080/1097198X.2015.1108093