KAIPTC
...where peace begins

KOFI ANNAN INTERNATIONAL PEACEKEEPING TRAINING CENTRE

POLICY BRIEF 1 | February 2017

Cyber Security in Ghana: Evaluating Readiness for the Future

[Adam Motiwala]

BACKGROUND

In recent years, Ghana has experienced a rapid expansion of access to the internet and current trends show no sign of slowing down. In January 2016, Ghana opened a multi-million dollar 600-rack National Data Centree in Accra, the largest of its kind in West Africa.[1] Fibre optic rings are also being rolled out to interconnect government ministries and provide all sectors of government with internet access.[2] At least 16 million Ghanaians now have some sort of internet access.[3]

While these developments promise tremendous opportunities for growth, they also introduce significant challenges as the pool of inexperienced and uneducated network users multiply. One of the big issues is likely to be cyber crime, defined by the Budapest Convention as intentional actions of illegal access, interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography and offenses related to copyright and neighbouring rights.[4] These acts come in a variety of forms, and because of the tremendous capacity to do harm, call for immediate action.

Although Ghana has embraced these technological advancements with open arms, it has yet to develop a legal framework to adequately deal with the proliferating problem of cyber security and cyber crime. Ghanaian laws remain antiquated and technical capacities plainly lacking. Confronting the myriad of challenges these issues present will be crucial for ensuring national security, maintaining consumer confidence in the safety of the internet, and strengthening the Ghanaian economy.

Objectives

This policy briefs seeks to analyze the nature of cyber security threats in Ghana and evaluate the progress that the government has made in readying itself for future challenges. The report will explore recent legislative efforts in Ghana, across West Africa, and in Africa as a whole. Finally, the report will provide recommendations to the Ghanaian government on how to structure a workable framework for dealing with future cyber security threats.

The Issues

The threats of cyber crime and cyber terrorism are no longer the exclusive concern of developed countries. In fact, the United Nations has noted that developing countries are at a higher risk than developed countries of being the target of coordinated cyber attacks.[5]

Historically, cyber crimes in Ghana have taken a rudimentary form of internet fraud targeting gullible foreigners, known locally as sakawa or "419". These crimes traditionally involved credit card and advanced fee fraud, and capitalized on the vulnerabilities and gullibility of internet users. More recently,

[1] Ashiadey, Bernard Yaw. 2016. *National Data Centre to spur economic growth*. January 27. Available at: http://thebftonline.com/business/ict/17079/national-data-centre-to-spur-economic-growth.html [Accessed 10 February 2016].
[2] George Nyavor, "Ghana Gets National Data Centre by 2015," JoyOnline, 2014. Available at: http://www.myjoyonline.com/news/2014/december-12th/ghana-gets-national-data-centre-by-2015.php. [Accessed 27 August 2015].
[3] "Mobile Data Subscription Figures for March, 2015," National Communications Authority, 2015. Available at: http://www.nca.org.gh/73/34/News.html?item=500. [Accessed 27 August 2015].
[4] Budapest Convention on Cybercrime, Council of Europe, 2001. Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. [Accessed 27 August 2015].
[5] "Developing countries most vulnerable to cyberattacks," United Nations News Center, 2011. Available at: http://www.un.org/apps/news/story.asp?NewsID=40692 [Accessed

however, cyber crimes have evolved into considerably more complex and sophisticated enterprises, targeting wealthier and more valuable victims inside and outside of Ghana.

Ghana has had prolonged experiences with the effects of cyber crimes. A 2013 report by the US Federal Bureau of Investigation (FBI) ranked Ghana as the second largest source of cyber fraud and financial scams in Africa.[6] As early as 2010, Ghanaian small and medium-size enterprises reportedly suffered frequent cyber attacks and Ghanaian banks have more recently become the target of hacking.[7] More frighteningly, many cyber attacks go undisclosed, as companies fear that revealing such vulnerabilities would cripple their popular image and undermine profits.[8]

These cyber crimes - both originating from and targeting Ghanaian netizens - have serious implications for the Ghanaian economy. A report by CyberSource Corp, a US payment processor, found that in 2008 over half of US merchants who accepted international orders refused to process purchases from Ghana, citing fraud concerns.[9] Continued perceptions of the insecurity of Ghanaian transactions will hinder key aspects of economic activity, particularly the growth of local credit and payment systems

The financial burden of a large cyber attack could also have a crippling impact on the public sector. A cyber attack targeting Ghanaian oil production, for example, could compromise the existing infrastructure and undo a $600 million investment made with IMF loan money.[10] It is not inconceivable that future loan payments become contingent on improving Ghana's cyber security capacity.

Moreover, cyber attacks present a threat not only to the economy, but also to fundamental national security. Recent years have seen the increasing sophistication of cyber criminals, shifting focus from the theft of financial information towards business espionage and accessing government information.[11] Insurgent groups are also starting to develop the capacity for sophisticated cyber attacks. For example, Boko Haram recently made clear its cyber expertise when it hacked into the Nigerian government's secret service database.[12] Similarly, Western intelligence agencies are increasingly expressing fear of a sophisticated cyber attack by the Islamic State.[13]

For Ghana, these are not simply theoretical concerns. In January 2015, the main government website was taken over by a rogue group of Turkish hackers that blocked access to official information, underscoring in dramatic fashion the need for a more modern approach to cyber security.[14] A future cyber attack could bring the Ghanaian military to its knees.

The Role of Law and the Current State in Ghana

A thorough and strongly enforced legal framework is critical for combating cyber crime. Given the transnational nature of these crimes, however, national laws that fail to consider international standards tend to prove myopic and thoroughly inadequate.[15] Moreover, the reality is that many legal systems have not yet developed a modern approach for dealing with cyber crime. Instead, they rely on traditional common law offenses to prosecute the cyber offense counterpart. This poses considerable problems as 19th century laws were focused more on physical objects and did not address intangibles, such as data or information.[16]

Ghana has fallen victim to many of these traps. Not until 2008 did Ghana pass any laws designed specifically to address crimes perpetrated through the internet. So far, these laws have been conspicuously inadequate, as portions copied from the Commonwealth Model Law - such as those on child pornography and illegal devices - include ambiguous and overlapping provisions that cripple the ability for authorities to apply the law.[17] As late as 2013, there had not been a single example of a successful prosecution under the 2008 Electronic Transactions Act - the primary cybercrime legislation - and such trials are still strikingly infrequent.[18] Indeed, the Ghanaian police still report relying on conventional criminal laws on false pretenses to prosecuting cyber offenses, some of which go back to as early as the 1960s.[19, 20]

[6] 2013 Internet Crime Report, US Federal Bureau of Investigation, 2013. Available at: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf [Accessed 27 August 2015].
[7] Ezer Osei Yeboah-Boateng and Reza Tadayoni, Cyber Security: Implications for SMEs in Developing Economies – The Case of Ghana,. Aalborg University, 2010
[8] Jeffrey Goldman, "Survey Finds Enterprise Data Breaches Are Significantly Underreported," eSecurity Portal, 2013. Available at: http://www.darkreading.com/attacks-breaches/survey-exposes-the-dirty-little-secret-of-undisclosed-breaches/d/d-id/1140847. [Accessed 27 August 2015].
[9] International eCommerce Presents Hazards for US/Canadian Merchants," CyberSource, 2009. Available at: http://www.cybersource.com/about/news_and_events/view.php?page_id=1726 [Accessed 27 August 2015].
[10] "CERT Research Annual Report," Software Engineers Institute, Carnegie Mellon, 2009. Available at: http://resources.sei.cmu.edu/asset_files/CERTResearchReport/2009_013_001_51315.pdf [Accessed 27 August 2015].
[11] John Herhalt, Cyber Crime: A Growing Challenge for Governments. KPMG International, 2011
[12] Ioannis Mantzikos, "Exploring Nigeria's Vulnerabilities in Cyber Warfare," Modern Diplomacy, 2013. Available at: http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=221:exploring-nigeria%E2%80%99s-vulnerability-in-cyber-warfare&Itemid=487 [Accessed 27 August 2015].
[13] Wesley Bruer, "FBI chief worries ISIS could use cyberattacks against U.S," CNN, 2015. Available at: http://edition.cnn.com/2015/05/20/politics/isis-cyberattack-fbi-director/ [Accessed 27 August 2015].
[14] Stephen Anti, "Hacking of Gov. of Ghana Websites: Turkish Hackers Claim Responsibility," JoyOnline, 2015. Available at: http://www.myjoyonline.com/news/2015/january-22nd/hacking-of-gov-of-ghana-websites-turkish-hacker-claims-responsibility.php. [Accessed 27 August 2015].
[15] "Comprehensive Study on Cybercrime," UNODC, 2013. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed 27 August 2015].
[16] Ibid.
[17] "Global Project on Cybercrime," Council of Europe, 2013. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb%20rev_final_CoE.pdf. [Accessed 27 August 2015].
[18] Ibid.
[19] Richard Boateng and Olumide Longe, "Sakawa—Cybercrime and Criminality in Ghana," Journal of Information Technological Impact, 11:2, 95 (2011).
[20] Albert Antwi-Boasiako, "Workshop on Cyber Security." KAIPTC. 10 July 2015. Speech.

More importantly, the government has made little headway in articulating a coherent strategy for dealing with most cyber crimes or future threats. The government has not developed an official cyber security strategy and has yet to create a framework for meeting international standards on cyber security.[21] Indeed, not a single government agency has been certified under international standards.[22] Furthermore, there are no recognized partnership agreements for sharing cyber security assets either between government agencies, or between the public and private sector.[23]

Nevertheless, some progress has been made through regional institutions in passing legal frameworks for dealing with cyber crime. ECOWAS passed a Draft Directive on Fighting Cybercrime in 2009 while the African Union adopted its own convention in 2014. Yet, to date, no African nation has ratified the AU convention and neither framework goes far enough or includes the requisite mechanisms for addressing the challenges faced by Ghana.[24]

The ECOWAS Draft Directive, for example, ignores widely recognized instruments for real-time collection of data and preservation of computer data.[25] In addition, it carries strikingly few provisions on international judicial cooperation on cyber crime cases, in stark contrast with the more widely observed Budapest Convention on Cybercrime.[26] Moreover, there is serious concern that some of the AU convention provisions could expand government powers, facilitating discrimination and leading to other human rights abuses.[27]

Recommendations

Ghana can take several measures to better equip itself to deal with cyber crime:

- Subscribe to the Budapest Convention on Cybercrime and begin the process of harmonizing laws with the rest of the international community. The Convention on Cybercrime is, to date, the most comprehensive and effective global treaty on cyber crime. Working with treaty members to harmonize laws—that is, promulgating similar though not necessarily identical laws—is necessary in order to remove Ghana from the potential or actual group of criminal safe havens and facilitate global evidence collection efforts.[28] Moreover, the institutional knowledge provided by the convention could prove useful as Ghana embarks on large-scale reforms. However, avoid the Additional Protocols on Xenophobia as they create unnecessary and problematic issues with free speech and human rights, and have been challenged by several of the treaty's members.
- Establish a central agency devoted to researching, articulating and coordinating cyber security policies. The new agency should develop a framework for implementing internationally recognized cyber security standards, conduct frequent benchmarking of the development of cyber security measures and consider establishing an accreditation process for certifying the preparedness of public and private organizations. Furthermore, there should be more efforts to coordinate and share cyber security assets between government agencies.
- Work with regional and international actors, including the US Department of State and Department of Justice, and the New Partnership for African Development, in capacity building to allow Ghana to bolster its cyber security capabilities. These institutions have been specifically tasked with helping countries close capacity gaps and meet international standards.[29] While the Ghanaian Police Service has been working closely with domestic consultants in improving its infrastructure, more can be done by the Ghanaian government with international collaboration to minimize vulnerabilities.[30]
- Create best practices guidelines in cooperation with the private sector to help Ghanaian industry deal with future criminal activities. This should include a streamlined, fully confidential pipeline of communication between government and business that allows the latter to report suspected criminal attacks without compromising the corporation's reputation, media image or financial interests. The priority should be on complete discretion and minimizing disruptions, so that private actors do not have a strong disincentive to report potential cyber attacks. The Ghanaian government can look to similar guidelines published

[21] "Cyberwellness Profile: Ghana." International Telecommunications Union, 2015. Available at:http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Ghana.pdf. [Accessed 27 August 2015].
[22] Ibid.
[23] Ibid.
[24] "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity." Council on Foreign Relations, 2015. Available at: http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity. [Accessed 27 August 2015].
[25] "Cybercrime directive: Explanatory notice – Economic Community of West African States (ECOWAS)," International Telecommunications Union, 2013. Available at: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/cybercrime_directive-explanatory_notice.pdf. [Accessed 27 August 2015].
[26] Ibid.
[27] "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity." Council on Foreign Relations, 2015. Available at: http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity. [Accessed 27 August 2015].
[28] "Cybercrime Model Laws," Council of Europe, 2014. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Reports/2014_Zahid/3021_model_law_study_v15.pdf. [Accessed 27 August 2015].
[29] "FACT SHEET: Administration Cybersecurity Efforts 2015," The White House, 2015 https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015 [Accessed 27 August 2015]
[30] CID signs MoU with e-Crime Bureau Inc. on Capacity Building," Ghana News Agency, 2012, http://www.ghananewsagency.org/human-interest/cid-signs-mou-with-e-crime-bureau-incorporated-on-capacity-building-45486 [Accessed 27 August 2015]

by foreign law enforcements agencies, such as the US Department of Justice.[31]

- Provide intensive training for law enforcement and military officials so they can identify cyber crime, understand how to collect the relevant evidence and data from computers and service providers, and properly evaluate them in a timely manner. While Ghana currently provides limited training in this area to the officer corps, these workshops are rudimentary and need to be if Ghana is to be seen to be taking seriously the threat posed by cyber terrorism.

Conclusion

The meteoric rise of information technologies in Ghana is contributing to economic growth and modernization. These changing conditions, however, necessitate a comprehensive reassessment of existing threats and technological vulnerabilities. Developing a thorough framework for dealing with current and future cyber security issues is integral to the economic vitality and national security of Ghana. While progress towards this objective has been made both domestically and regionally, current efforts have proven woefully inadequate. If Ghana is to realize its potential as the "Black Star of Africa," it must swiftly adapt to a changing world.

[31] "Best Practices for Victim Response and Reporting of Cyber Incidents," U.S Department of Justice, 2015, http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf [Accessed 27 August 2015]

About the Author

Adam MOTIWALA was an intern at the Faculty of Academic and Research, Kofi Annan International Peacekeeping Training Centre in 2015. He is a student at the University of Chicago Law School, Chicago, US and a Candidate for Juris Doctor in June 2017.

About the Centre

Kofi Annan International Peacekeeping Training Centre (KAIPTC) is an internationally preferred centre of excellence for research into and training for conflict prevention, management and resolution, research and innovative thinking in integrated peace support operations and sustainable delivery of enhanced regional capacity building for peace support operations.

How to Cite this Publication

Motiwala, Adam. February 2017. *Cyber Security in Ghana: Evaluating Readiness for the Future*. Policy Brief 1, Accra: KAIPTC.

KAIPTC ...where peace begins

THE GOVERNMENT OF DENMARK THE GOVERNMENT OF NORWAY THE GOVERNMENT OF SWEDEN