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 Centre in Accra, the largest of its kind in West Africa.

Fibre optic rings are also being rolled out to interconnect government ministries and provide all sectors of government with internet access. At least 16 million Ghanaians now have some sort of internet access.

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.

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 brief 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.

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, ...
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. 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.

More frighteningly, many cyber attacks go undisclosed, as companies fear that revealing such vulnerabilities would cripple their popular image and undermine profits.

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.

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. 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. 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. Similarly, Western intelligence agencies are increasingly expressing fear of a sophisticated cyber attack by the Islamic State.

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. 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. 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.

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. 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. Indeed, the Ghanaian police still report relying on conventional criminal laws on false pretenses to prosecuting cyber offenses, some of which go back as early as the 1960s.


15 Ibid.


17 Ibid.


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. Indeed, not a single government agency has been certified under international standards. Furthermore, there are no recognized partnership agreements for sharing cyber security assets either between government agencies, or between the public and private sector.

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.

The ECOWAS Draft Directive, for example, ignores widely recognized instruments for real-time collection of data and preservation of computer data. 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. 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.

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.

- 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

---

22 Ibid.
23 Ibid.
26 Ibid.

- 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.

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