CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 44 — NOVEMBER 2016

Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study

Caroline Baylon and Albert Antwi-Boasiako

INCREASING INTERNET CONNECTIVITY WHILE COMBATTING CYBERCRIME: GHANA AS A CASE STUDY

Caroline Baylon and Albert Antwi-Boasiako

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

vi About the Global Commission on Internet Governance

vi About the Authors

1 Acronyms

1 Executive Summary

1 Introduction

1 Internet Infrastructure Development

5 The Link Between Internet Infrastructure Development and Cybercrime

6 Combatting Cybercrime

11 A Possible Overarching Strategy

11 Conclusions

12 Acknowledgement

12 Works Cited

16 About CIGI

16 About Chatham House

16 CIGI Masthead

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Caroline Baylon served as the lead researcher on cyber security at Chatham House in London, United Kingdom, from 2013 to 2015, and was also editor of the institute's *Journal of Cyber Policy*, a peer-reviewed academic journal published by Routledge, Taylor & Francis. Caroline recently worked as an independent contractor carrying out research projects on cyber security for the UK Foreign and Commonwealth Office, looking at cyber proxy actors and at limiting cyber weapons proliferation. She is currently the information security research lead within the research-and-development section at AXA in Paris, France, and London, United Kingdom, which is establishing an internal think tank on cyber security. Her work there includes a research stream on cyber security issues impacting Africa. She has also worked as an independent consultant for a number of intelligence providers on cybercrime issues involving Sub-Saharan Africa. Caroline holds an M.Sc. in social science of the Internet from Balliol College, University of Oxford, and a B.A. in economics from Stanford University.

Albert Antwi-Boasiako is the founder of e-Crime Bureau, a cyber security firm based in Ghana, and a cyber security expert with the Interpol Global Cybercrime Expert Group. A graduate of the University of Trento, Italy, and the University of Portsmouth, United Kingdom, Albert is currently a Ph.D. research fellow with the University of Pretoria, South Africa. Albert has conducted different cyber-security capacity-building projects for a number of international organizations including the Council of Europe, United Nations Office on Drugs and Crime, United Nations Conference on Trade and Development, Commonwealth Cybercrime Initiative and the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). Albert is a visiting lecturer in cybercrime, cyberterrorism and cyber security at the Kofi Annan International Peacekeeping Training Centre, Accra, Ghana, and a research associate with the African Centre for Cyberlaw and Cybercrime Prevention based in Kampala, Uganda.

ACRONYMS

CET	Common External Tariff
CID	Criminal Investigations Department
DDoS	distributed denial of service
ECOWAS	Economic Community of West African States
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
ISPs	Internet service providers
IT	information technology
SAT-3/WASC	South Atlantic 3/West Africa Submarine Cable
USB	universal serial bus
VAT	Value Added Tax

EXECUTIVE SUMMARY

Furthering Internet growth in Sub-Saharan African countries is central to the region's economic development. Yet increases in Internet connectivity are generally accompanied by an increase in cybercrime. With more widespread, faster and cheaper Internet connectivity, cybercriminals have greater opportunities to engage in online crime. For instance, fraudsters engaged in Nigerian-type scams or romance fraud are able to reach a greater number of potential victims around the world. In addition, many computers in the region are not patched regularly and do not have antivirus protection installed, forming a mass of unprotected or underprotected machines that cybercriminals can easily herd together into botnets. The reliance on mobile phones to access the Internet in the region also makes it a particularly attractive target for cybercriminals since mobile devices tend not to have firewalls, antivirus, encryption and other defensive mechanisms that computers do. Using Ghana as a case study, this paper explores how to best promote Internet development in the country while simultaneously keeping cybercrime levels in check.

The first section of this paper considers how to promote the growth of Internet infrastructure in the region, looking at the current state of Internet connectivity in Ghana, root causes of Internet development challenges in the country and potential solutions to these challenges. The second section further details the link between increased Internet connectivity and a growth in cybercrime. The third section focuses on how to combat cybercrime, examining the current state of cybercrime in Ghana, root causes of cybercrime challenges in the country and potential solutions to these challenges. Given the interlinked nature of Internet development and cybercrime, the fourth section considers whether policy makers can develop an overarching strategy to tackle these problems. This includes making use of multiplier effects by concentrating efforts on the root causes of Internet development and cybercrime challenges that are common to both, such as poverty and corruption. It also includes taking a joint approach by holding regular meetings that bring all stakeholders together to discuss solutions to both challenges in a holistic manner.

INTRODUCTION

Despite the steady development of Internet infrastructure in recent years in Ghana, the country still faces considerable obstacles to achieving widespread connectivity. Ghana's economy has been growing consistently, and measures to further foster Internet penetration are central to Ghana's continued economic development. But along with the Internet's tremendous benefits for business and commerce comes a challenge: greater Internet connectivity in the country is correlated with an increase in cybercrime. Ghana is already one of the top 10 sources of cybercrime in the world, and faster and more reliable Internet will provide cybercriminals with greater opportunities to engage in illicit activities online — and with a larger number of potential victims (Sikiti da Silva 2014). This paper looks at how to best help foster Internet growth in Ghana while simultaneously working to contain cybercrime levels.

The first section of this paper focuses on Internet infrastructure development, examining the current state (and evolution) of Internet connectivity in Ghana, the root causes of the challenges to Internet infrastructure development and potential solutions to these challenges. The second section elaborates on the link between growth in Internet connectivity and increases in cybercrime. The third section centres on combatting cybercrime, looking at the current state (and evolution) of cybercrime in Ghana, the root causes of cybercrime and potential solutions to these challenges. The fourth section considers whether policy makers can develop an overarching strategy to tackle these interlinked problems. The paper draws on the existing academic literature, local news sources in Ghana and data gathered by reports made to the e-Crime Bureau.

INTERNET INFRASTRUCTURE DEVELOPMENT

THE CURRENT STATE AND EVOLUTION OF INTERNET INFRASTRUCTURE DEVELOPMENT IN GHANA: A SNAPSHOT

The First Wave of Connectivity: Internet Cafés

Ghana was one of the earliest countries in Africa to gain Internet connectivity in 1994 (Foster et al. 2004). The first wave of connectivity in the country came through fixed-line access. Until 2010, Ghana had only one submarine fibre optic cable, the SAT-3/WASC (South Atlantic 3/West Africa Submarine Cable), which it shared with other West African countries. With such a limited fixed-line network,

the primary method of Internet access was shared connectivity, mostly in Internet cafés. This also included other public access places such as the workplace, schools and universities. Fixed-line connectivity in homes remains rare: only three percent of households in Ghana had a working Internet connection in 2012 (Calandro, Stork and Gillwald 2012).

Poor Quality, an Urban-Rural Digital Divide and Last-mile Connectivity Issues

Moreover, connectivity in the country is often of poor quality. The network experiences frequent outages as well as slow Internet speeds. According to a 2012 survey, more than 40 percent of respondents reported that "slow Internet" limited their use (Frempong 2012).

Ghana also has a significant urban-rural digital divide, with the majority of the country's Internet connectivity (and especially faster fibre optic connections) concentrated in the capital city of Accra and other large cities. Rural areas often lack sufficient economic incentives for investment: Wages are lower and, since they tend to be agricultural communities, there is less market demand for connectivity. The cost of providing Internet to rural areas is significantly higher as well. They typically lack last-mile infrastructure and thus may need satellite or other connections, which are expensive. Rural areas are less likely to have electricity, compounding the challenge.

The Second Wave of Connectivity: Mobile Internet

Given the challenges involved in providing Internet in the region, Ghana has increasingly turned to mobile broadband, which has formed the second wave of connectivity in the country. Smartphones and access dongles (i.e., universal serial bus [USB] modems with a SIM card inside that can be plugged into a computer) are now the main means of Internet access in Ghana. The country's mobile broadband penetration rate recently reached 62 percent (National Communications Authority 2015). Internet cafés, once the primarily place for Ghanaians to access the Internet, have been declining in popularity (Acquaye 2013).

The rise of mobile broadband is in large part due to its increased affordability. While fixed-line Internet in Ghana requires a subscription, mobile Internet in the country is primarily based on prepaid services. (More than 97 percent of mobile phone owners in Ghana are on a prepaid plan.) Since many Ghanaians hesitate to sign up for subscription-based services out of concern that they will not be able to pay in subsequent months, the prepaid nature of mobile broadband is much more attractive for them (Calandro, Stork and Gillwald 2012). And for those accessing the Internet via smartphone, mobile phones are much less expensive than computers as well.

Another advantage of mobile Internet is that it does not require users to have electricity at home. Of course, mobile phones need charging, but they can be charged at regular intervals at a venue where there is electricity and then taken elsewhere. Mobile broadband is also helping to bridge the digital divide by bypassing the last-mile connectivity problem — although many villages are still grappling with the challenges stemming from lack of electricity.

However, a number of obstacles still remain. The experience of viewing the Internet via smartphone is not akin to accessing the Internet from a computer; the devices' small screen size and limited computing power mean that users cannot access information as readily. And with access dongles, the coverage is often spotty; nor do they provide enough capacity. It is thus important for Ghana to continue to develop its fixed-line connectivity too.

The Coming Third Wave? Recent Developments in Fixed-line Connectivity

In the past five years, Ghana has acquired four additional submarine fibre optic cables: Main One Cable in 2010, GLO-1 (Globacom-1) and WACS (West Africa Cable System) in 2011, and ACE (African Coast to Europe) in 2013. This has considerably increased the bandwidth available, from 320 gigabytes to 12 terabytes. It has also resulted in "a dramatic fall in the wholesale cost of capacity. Today, the cost of an E1 connection in Ghana is around $1,200, down from as much as $12,000 in 2006" (Boakye 2014). That is, the cost for Internet service providers (ISPs) to purchase bandwidth is now roughly one-tenth of what it was less than 10 years ago. These cost savings are starting to be passed on to consumers, although this has not yet been fully accomplished.

As part of its Project Link, Google announced in October 2015 that it plans to lay 2,000 km of fibre in Accra and the major cities of Tema and Kumasi (Abdul-Jalil 2015). Meanwhile, the government is taking steps to enhance Internet connectivity in rural areas: it recently finished building an 800-km fibre optic cable backbone traversing the Eastern corridor of the country and is starting a similar project for the Western corridor (IT News Africa 2015; Acquaye 2015).

CHALLENGES FOR INTERNET INFRASTRUCTURE DEVELOPMENT: IDENTIFYING THE ROOT CAUSES

Cost Factors, including High Poverty Levels

Cost factors have long precluded the greater development of the Internet in Ghana, especially fixed-line connectivity. Given that 54 percent of the population lives on less than GH¢7 (US$2) per day, computers remain unaffordable for the majority, and only 9 percent of households in Ghana had a computer in 2012 (Dela Klutse 2015; Calandro, Stork

and Gillwald 2012). For many, the cost of Internet access alone is prohibitive; over 55 percent of those interviewed in a 2012 survey said that their main reason for not accessing the Internet was because it was "expensive to use" (Frempong 2012). Concerns about the size of the market have thus made some telecommunications companies reticent to invest the tens or hundreds of millions of dollars needed for laying down cables, including in rural areas.

Electricity Shortages

The insufficiency and unreliability of the electricity supply, even in Accra, is a major challenge for Internet development too. Only 73 percent of households in Ghana had electricity in 2012, and those that do experience frequent power cuts (Calandro, Stork and Gillwald 2012). In December 2014, for example, the capital experienced weekly blackouts that lasted for up to 12 hours at a time.

This is because much of Ghana's energy comes from hydroelectric power. The country's rainfall is unpredictable, so at times the lake that supplies the country's main hydroelectric power plant does not contain enough water. These electricity shortages are a major obstacle to the use of computers needed for fixed-line Internet access. It also raises the cost of providing Internet, since ISPs must have electrical or diesel generators or other backup methods to provide power when there are cuts.

Accidental Cable Cuts during Road Construction and Repairs or Illegal Mining

Ghana also has a major problem with unintentional cuts to both fibre optic and copper cables, resulting in poor quality and outages that can last days or even weeks. In 2014, 1,370 fibre optic cable cuts were reported in a six-month period, or more than 200 cuts per month. This represents a 400 percent increase since 2011, in which there were only 480 cuts total for the year, an average of 40 cuts per month (Naphtal 2015). The cable cuts result in considerable expense for telecommunications companies, in both the cost of replacing the cables and the labour required to repair them. Repairing one cut costs an estimated GH¢17,000 (US$4,500). Moreover, the labour spent repairing the cables could have been used to improve Internet service or lay additional cables instead (Kunateh 2015).

Repairs to fibre optic cables involve slow and delicate work. Just identifying the location of a cable cut can take five to six hours. The fibre optic cables themselves are very sensitive: each cable contains more than 46 glass fibre strands and each strand has to be cut to the right shape in order to be spliced back together. Moreover, if the protective coating has been damaged, the cables must be carefully cleaned of dust particles before being reconnected; otherwise, it will create interference on the line. Another complication is that if a fibre optic cable experiences too many cuts, this eventually causes "attenuation." That is, the signal will meet resistance when it passes down the fibre, degrading the communication quality. Repeated cuts may require telecommunications companies to replace a whole section of cable, which is costly (Adam 2014).

The majority — an estimated 75 percent — of cuts are caused by workers carrying out road construction and repairs (BiztechAfrica 2013). Ironically, many of these workers are contractors of the Ministry of Roads and Highways, which has been actively improving and expanding the road network. Although recent efforts have been made to ensure that the locations of the cables are signposted and that blueprints are filed with relevant agencies such as the Ghana Highway Authority, some managers do not ask for the blueprints. Moreover, the managers generally do not explain the importance of the cables to the workers or make sure that they know how to recognize the signposts. Instead, they give them key performance indicators, so the workers rush to complete their tasks without considering the cables (Graphic Online 2012). The expansions of some roads from one lane to two may also disrupt the existing cable infrastructure. In other instances, the cables may not have been buried deep enough or the blueprints may be unclear. Despite the numerous reports that telecommunications companies have made to the Ministry of Roads and Highways, this problem persists (Mustapha 2014).

Other culprits include contractors installing road signs or working for utility companies to lay water pipes and electrical lines. The contractors sometimes cut through roads in the process, damaging the roads, which then require further repair, further perpetuating the cycle of cable damage (Ghana Business News 2015). About 10 percent of cable cuts are caused by illegal miners, or "galamsayers," who are digging for minerals in the ground (Acquaye 2014). They, too, often do not understand the importance of the cables.

Theft of Cables and Other Elements of the Internet Infrastructure

Cable theft is a major challenge. The relatively high price of copper means that thieves are increasingly digging up and stealing copper cables, then selling them to scrap dealers who resell them abroad. In January 2013, Vodafone experienced the theft of 1 km of copper cable in the Madina area, which was estimated to cost GH¢200,000 (US$53,000) in damages and to take three weeks to repair. And in the month of May 2013 alone, Vodafone experienced about 30 cable thefts, with outages affecting Osu Castle (the seat of government at the time) and Parliament House in Accra, the capital (JOY Online 2013).

The theft of copper cables also contributes to cuts to (and sometimes the theft of) fibre optic cables. While costing millions to make, fibre optic cables fetch little on the black

market. They are primarily made of glass, and thus have limited scrap resale value. When purchased, the glass is primarily reused to make jewellery. However, thieves looking for copper cables sometimes find the fibre optic cables and think that they might contain copper, so they cut them open to check. On discovering that they do not, the thieves sometimes steal the fibre optic cables anyway, thinking that even the small amount of money they will fetch is better than none.

ISPs also have to guard against the theft of other elements of the infrastructure required to provide Internet. For example, there have been numerous incidences of theft of the diesel from the diesel generators used to provide backup power. Similarly, the telecommunications provider Tigo has seen an increase in thefts of batteries, which are also used as a backup power source, and has had to increase security in response (Ghana News Agency 2014). This entails additional costs, both in terms of replacing materials and providing security, and thus also raises the cost of providing Internet.

Corruption

The high incidence of corruption within the country is also a factor in cable theft and impedes Internet development. Corruption is pervasive even within major companies. In one instance, four employees of Vodafone — including a team manager and a senior customer engineer — were jailed for stealing cables from the company. The company had sent the employees to recuperate some 200 m of redundant Vodafone underground cables for use in repair works, but instead the employees took almost seven times that amount and sold the extra to a scrap dealer. When those within a company, who — in the words of the trial judge — "ought to protect the company and not engage in such acts that would make the company run at a loss" are corrupt, this compounds the challenge of further developing Internet infrastructure (GhanaWeb 2015a).

POTENTIAL SOLUTIONS

Tax Incentives

One method of increasing Internet penetration is to lower or eliminate taxes on equipment needed for access, which would make it more affordable for individuals. Doing so for smartphones may prove effective. Ghana has employed such tactics with mobile phones (not just smartphones) in the past: it removed import duties on all mobile phones in 2008. Although the government later reintroduced tariffs in 2013 due to its need to raise additional funds at the time, the increase in uptake of mobile phones during the tax-free period demonstrates the success of the policy (Citifmonline 2016b).

With this in mind, Ghana has recently reduced taxes on smartphones specifically. It had initially intended to repeal all of the customs charges that had been placed on smartphones: in November 2014, the country's finance minister announced that he planned to remove import duties on smartphone handsets, stating that this would bolster smartphone penetration rates and thus also help close the digital divide (Ogundeji 2014). He also expressed his view that, despite the loss in revenue from import duties, the measure would result in an increase in overall tax revenue; a reduction in the smuggling of handsets into the country combined with an increase in the number of smartphones sold would increase revenue from other taxes, such as the Communication Service Tax, Value Added Tax (VAT), and corporate taxes.

However, the tariff removal never went into effect since it subsequently became apparent that, as a member of the Economic Community of West African States (ECOWAS), Ghana was expected to implement the Common External Tariff (CET) when it came into force in early 2016 (Citifmonline 2016a). Instead, the government has therefore recently reduced the customs tariffs on handsets from 20 percent to 10 percent, so that they are in line with the CET. It also removed the VAT on imported handsets. While not as effective a measure as removing taxes on smartphones entirely, the tax reduction should nonetheless contribute to a significant increase in smartphone penetration and hence in mobile Internet connectivity.

The government should consider repealing or lowering import duties on computers too. There is currently an import tax exemption on computers used for educational purposes. However, broadening this to include all computers would help promote fixed-line access.

Another effective tactic would be to reduce or remove taxes on Internet infrastructure equipment, making investment more affordable for companies. Telecommunications companies are petitioning the government to remove taxes on modems (also called terminal equipment) used to access the Internet, including access dongles. This will reduce the cost for these companies to provide Internet. They point out that the tax reduction on smartphones favours the provision of Internet via mobile. Since each type of Internet access has important advantages and both are needed, reducing taxes on modems and computers as well as on smartphones would stimulate both fixed-line and mobile connectivity.

Renewable Energy

To increase the reliability of the energy supply, greater development of solar power (and other renewables such as wind and biomass power) could serve as an ideal complement to hydro power. The current challenge in Ghana is a lack of expertise on how to implement renewable energy. However, there have been some promising steps in recent years. In November 2015, the Energy Commission organized a first conference on renewable energy that

brought together key stakeholders including the private sector, financiers, government and consumers. It held a second conference in August of this year together with the United Nations Development Programme and the Ministry of Power.

Engaging All Stakeholders in Preventing Accidental Cable Cuts and in Fighting Cable Theft

Solutions to accidental cable cuts will require the cooperation of all stakeholders: government ministries, contractors, workers and telecommunications companies. Positive measures have been taken, but are far from being adequately implemented. In March 2013, the Ghana Chamber of Telecommunications and the Association of Road Contractors agreed to jointly engage in a sensitization program to ensure that workers could recognize and protect cables and other telecommunication infrastructure when they saw it in the field, that telecommunications companies provide the latest blueprints to road agencies and that road agencies pass them on to their contractors. A May 2013 letter from the National Security Council Secretariat to the minister of roads and highways called for contractors to be given cable blueprints and for them to sign an agreement to protect cables from damage, with copies of all documents sent to the National Security Council Secretariat. The minister of roads and highways consequently issued a directive in December 2014 requiring contractors to engage with telecommunications companies before doing road work and for them to share blueprints and technical plans. The Ministry of Roads and Highways plans to establish a Standing Technical Committee (made up of the Telecoms Chamber, the National Communications Authority and the ministry itself) to act as an advisory body to help identify cable markings before work on a road begins.

Solutions to cable theft will also require the government, police, members of the community and telecommunications companies to cooperate. In October 2012, community volunteers undertook to patrol the town of Ashaiman after a spate of cable thefts; they caught two individuals trying to steal cables and turned them in to police (GhanaWeb 2012a). In June 2013, the Ministry of Communications announced that, working together with Vodafone and other telecommunications providers, it was implementing a year-long awareness program to educate the population about the consequences of cable thefts. Vodafone also launched a community vigilance campaign, working closely with the police. The campaign underlines the key role of the community in stopping cable thefts, and Vodafone provides a dedicated phone number for citizens to report any suspicious activity near cables (GhanaWeb 2012b).

Technical Solutions

ISPs are also looking at technical solutions. For instance, Tigo began a project mounting fibre optic cables on concrete poles in the Western and Ashanti regions in November 2014 (CRU Wire and Cable News 2014). Similarly, telecommunications provider MTN has built in redundancy to existing routes to mitigate the effects of cable cuts (JOY Online 2014). Some telecommunications companies have suggested to the World Bank and other funders of road projects that the projects should include utility ducts so that companies can lay cables in a manner that reduces the risk of cuts. Other technical solutions might involve alarm systems when cable lines are disturbed.

Regulatory Measures

Regulatory solutions are also being considered. In November 2015, one of MainOne's senior executives called on the government to pass laws to protect undersea cables, given their key role in delivering Internet to the country. Such a law would complement an existing industry initiative on the topic, which includes an annual Cable and Pipeline Protection Awareness Workshop founded by MainOne to raise the issue's profile with relevant stakeholders (GhanaWeb 2015b).

Better enforcement of existing laws is also key. In April 2016, at the urging of Vodafone, the Ghana Police Service and the Judicial Services department set up special "cable courts," designed specifically for prosecuting cases of cable destruction and theft. The cable courts are currently established in Accra and Kumasi, but the intention is to establish additional such courts in other parts of the country as well (Ampomah 2016; Abbey 2016). In addition, in August 2016 the Ministry of Trade and Industries granted permission to Vodafone to inspect all scrap exports out of the country to ensure that they do not contain copper cables (GhanaWeb 2016; Ghana News Agency 2016).

THE LINK BETWEEN INTERNET INFRASTRUCTURE DEVELOPMENT AND CYBERCRIME

Greater Resources and Lower Barriers to Entry: Email Scams and Crimeware

Yet as Ghana's Internet infrastructure continues to expand, more widespread, cheaper and faster Internet connectivity is giving cybercriminals greater resources to engage in illegal activity, including providing them with access to a larger number of potential victims. The ability to send a large number of emails to a global pool rapidly and without any postage costs enables Ghanaian cybercriminals to more effectively engage in email scams, targeting both victims in Ghana and comparatively wealthy foreigners abroad.

Moreover, there are relatively low barriers to entry to commit cybercrime — and they are getting lower still (Kavanagh 2013). Although more than 80 indigenous languages are spoken in Ghana, English is the official language and the lingua franca. This means that a number of cybercriminals in the country have English language skills that they can employ in email scams that target the large part of the world population that speaks English — notably individuals living in wealthy countries such as the United States and United Kingdom. Further, the rise in crimeware, or malware designed to automate and facilitate cybercrime, means that engaging in cybercrime involves less and less technical skill. For instance, cybercriminals can use exploit kits with pre-written exploit code that do not require expertise to use.

High Vulnerability to Attack: User Inexperience and Underprotected Machines

As increasing numbers of computers in Ghana connect to the Internet, they form a mass of vulnerable machines that are particularly attractive targets for cybercriminals. Many computers in Ghana are not patched regularly and do not have antivirus software installed. This is partly because of a lack of user education: users are typically unaware of the importance of downloading update patches or running antivirus, so their machines often lack basic security protections.

Even when users are aware of the need for updates and antivirus, slow connection speeds and limited bandwidth are an obstacle to installing them. Another factor is that many users in Ghana use pirated software, which means that their software does not receive automatic security patches in response to newly discovered vulnerabilities. (In contrast, genuine software automatically receives updates to install.) Low income levels in Ghana are a key part of the challenge, as many users cannot afford genuine software. In addition, users often do not have access to antivirus software in their native language, making it harder for them to use. Even developing versions for a few of the most commonly spoken languages — for example, Akan, Ewe and Ga — may not be economically viable.

Botnets

Cybercriminals (both within Ghana and abroad) can infect these unprotected or underprotected machines and herd them together into botnets, or "robot networks" of tens or hundreds of thousands of compromised computers that they can remotely control. By harnessing the combined power of the computers in a botnet, cybercriminals can launch distributed denial of service (DDoS) attacks to take down websites and other targets by directing a large volume of traffic against them in order to overwhelm them. Cybercriminals can also use such botnets to send malware to infect other computers in order to steal passwords, login credentials, bank details, credit card information and other data from victims both within Ghana and around the world.

Mobile Phone Vulnerabilities

Ghanaians' heavy reliance on cell phones for Internet access also renders them especially vulnerable given that mobile devices have fewer cyber security protections than computers. They typically do not have defensive measures such as firewalls, antivirus software and encryption. Mobile phones' operating systems are also not updated as frequently as those on personal computers.

COMBATTING CYBERCRIME

THE CURRENT STATE AND EVOLUTION OF CYBERCRIME IN GHANA: A SNAPSHOT

Initial Focus on Scamming: Nigerian Letter Hoaxes, Business Fraud, Credit Card Fraud and Romance Fraud

The earliest form of cybercrime in Ghana, known as "sakawa," focused on scamming attacks. Of the 217 incidents reported to the e-Crime Bureau for investigations assistance in 2014, scamming attacks accounted for nearly 65 incidents — the largest category. One of the oldest tactics is advance fee fraud, in which a fraudster promises a victim a large sum of money (which never materializes) in exchange for a smaller upfront payment. Originally perpetuated via postal mail, such scams began to be conducted through email once the country gained Internet connectivity in 1994. The most famous type of advance fee fraud is "Nigerian letter hoaxes," thus named because of the country in which they originated. (They are also sometimes referred to as "419" scams after the section of the Nigerian penal code that they violate.) For instance, a typical scam might involve a fake inheritance scenario. A fraudster purporting to be a lawyer contacts a victim to tell them that they have inherited millions of dollars from a distant relative, but they need to pay taxes or other fees in order to obtain the money; of course, no such inheritance actually exists.

Another type involves fake business transactions associated with the sale of gold. A scammer claiming to be from a gold mining company may contact a victim to offer them gold for sale at an advantageous price. The buyer must send money beforehand for shipping or other costs; of course, he will never receive any gold. Similar tactics exist involving the sale of oil at below market prices.

Credit card fraud is another early feature of electronic fraud in Ghana. Incidents first occurred in 1999, in which the staff in international hotel chains stole the credit card numbers of Western tourists and sold them to scammers. The scammers used the card numbers to make online

purchases and have the goods shipped to Ghana (Warner 2011).

Identity fraud, in which a fraudster obtains and uses a victim's personal data to make use of their identity for economic gain, is also common. Romance fraud is especially frequent. Typically, scammers use stolen photos to pose as Westerners on Internet dating sites such as Match.com or eHarmony. They develop romantic relationships with victims living abroad, then ask for money for an emergency, plane tickets to visit the victim or other fabricated reasons. Individuals can lose large sums of money: one recent UK victim of a romance fraud lost £250,000 (US$330,000) (National Crime Agency 2014).

The Modus Operandi: Roots in Traditional Juju Beliefs and Crime Bosses

Those engaging in sakawa often believe that the use of juju — a term that encompasses a number of traditional West African religions involving the use of black magic or witchcraft — is essential for their scams to be successful[1] (Abubakar 2012). The premise of juju beliefs is that individuals can make payments to "mallams," or priests, to bargain with the spirits on their behalf in order to acquire wealth or power (Morton 2011). When engaging in cybercrime, a number of scammers therefore consult mallams, who — in exchange for money, of course — give the scammers a series of rules and rituals to follow, such as wearing a magic ring or sleeping in a coffin alongside a corpse[2] (Warner 2011). If they carry out the mallam's instructions, the scammers believe, they will be protected from being caught by the police and will also acquire the power to control the minds of their victims, who will send the money that they ask for (Danquah and Longe 2011; Armstrong 2011). If they disobey the mallam, however, they will be cursed with bad luck (Graphic Online 2009).

These cybercriminals are typically young men aged 16 to 30. In many cases, they do not act alone but instead work for crime bosses who are thought to run both country-specific teams and broader regional ones across the West Africa region (Kavanagh 2013). For example, it appears that 419 scams have gone from national-level operations to regional syndicates, and some Nigerians engaged in 419 scams in their own country may have relocated some of their activities to Ghana as part of this expansion (ibid.).

An Evolution toward More Technically Sophisticated Attacks: Phishing and Mobile Banking Hacks

While cybercriminal groups in Ghana are still actively engaged in scamming, they are also adopting some of the new forms of cybercrime emerging around the world that make use of more technologically sophisticated techniques. There are currently a high number of phishing attacks in Ghana. These make up the second-largest category of reports to the e-Crime Bureau, accounting for more than 50 incidents. Phishing consists of cybercriminals sending emails made to appear as if they are from legitimate sources in order to trick victims into clicking on a link in the message. The links typically direct victims to fake websites that ask them to input passwords or credit card details, enabling the cybercriminals to steal confidential information on business networks, access individuals' bank accounts or use their credit cards, or other forms of theft.

Cybercriminals in Ghana are also increasingly making use of malware that targets smartphones, given that smartphones are the prime means of Internet access for many in the country. Security threats to mobile devices and malware attacks combined make up the third-largest category of reports to the e-Crime Bureau, accounting for more than 40 incidents in total. In particular, there has been a recent spate of incidents involving mobile banking. The mobile banking sector in Ghana has expanded considerably in recent years, with many of the country's major banks now offering some form of mobile banking. The potential to steal significant funds from banks, combined with the relative cyber security weaknesses of mobile devices, has thus made mobile banking a particularly attractive target for cybercriminals.

Other common attacks include website defacements and DDoS attacks to shut down websites. There are also a large number of botnets emanating in the region. These account for a small proportion of reports to the e-Crime Bureau, however.[3]

1 Juju priests have been involved from the beginning, when these scams were perpetuated by postal mail. For instance, juju priests would "bless" letters sent to Westerners, the letter writers believing that the recipients would then be magically compelled to send larger amounts of money (Warner 2011).

2 In some instances juju may involve elements of child sacrifice and cannibalism.

3 Other types of crimes committed using the Internet in Ghana include use of social media for propaganda by terrorist groups, such as Boko Haram and Al Qaeda's use of the dark web for communication; human trafficking rings posting of false recruitment ads online to lure victims; and online child pornography. However, discussion of these activities is beyond the scope of this paper, which focuses on cybercrime carried out for direct economic gain.

CHALLENGES FOR COMBATTING CYBERCRIME: IDENTIFYING THE ROOT CAUSES OF THE PROBLEM

Poverty and Unemployment

High poverty and unemployment levels in the country are driving some Ghanaians to engage in cybercrime. With close to one-third of young people unemployed in the country, Internet crime offers the possibility of earning large sums of money (Morton 2011). A distinctive sakawa culture, in which cybercriminals engage in lavish displays of their wealth, further entices them. Sakawa fraudsters typically wear flashy clothes and drive expensive cars. Observing this, other young men want to engage in cybercrime in order to enjoy this same lifestyle.

Engaging in cybercrime also enables those who feel powerless and live in poverty to enact retribution against the groups that they believe have been or are exploiting them. Some hold the West — and notably the legacy of colonialism and slavery — responsible for the ills that they suffer today. Others blame the government and wealthy Ghanaians, who are often corrupt. By targeting these groups, cybercriminals may feel that they are obtaining justice.

Electronic Waste

Actions by developed countries are also contributing to cybercrime in Ghana. The sending of electronic waste, which consists of old computers, monitors, cell phones and other electronic devices, to Ghana for disposal has provided cybercriminals with ready access to the data remaining on these devices — data that they can use to engage in cybercrime. To reduce the cost of recycling or disposing of electronic waste, companies in developed countries are increasingly shipping it to the developing world for handling. Ghana is one of the main recipients and receives some 215,000 tons of electronic waste each year, much of it consisting of computers and monitors (Amoyaw-Osei et al. 2011). The majority of these imports come from the United Kingdom (up to 60 percent), with the United States a close second (Doyon-Martin 2015).

Upon arrival in Ghana, the used computers and other electronics are sorted into categories: those that still work or can be repaired are reconditioned and then sold in markets for used goods. Those that cannot be are sent to dump sites. Agbogbloshie, located in a suburb of Accra, has become one of the world's largest dumping grounds for used computers and other electronic waste. At the dump sites, a secondary industry exists in which workers — typically children living in slums — sort through the electronic waste to extract copper, aluminum and other materials.[4]

This creates an opportunity for cybercriminals because the hard drives of these computers and other devices often contain credit card numbers, bank account information, business or personal documents, email addresses of colleagues and family and other confidential information belonging to the previous owners of the machines. The memories of mobile phones, too, often contain large amounts of data — particularly as they increase in computing power.

In many instances, obtaining data from these devices is made easier for cybercriminals because the data has not been wiped from the machines. This might be either because the previous owner did not erase the hard drive before disposing of the machine or else because the companies to whom they entrusted their devices for recycling assured them that they would clean them properly and then failed to do so. Moreover, even when a hard drive has been expunged, it is generally still possible to retrieve information from the hard drive if the hard drive has not been physically destroyed.

In one case, a media investigation found a computer in Ghana that had belonged to Northrop Grumman, one of the largest US military contractors. It contained confidential data about $22 million in US government contracts (Klein 2009). Used machines formerly owned by the US Army, Homeland Security and other US government departments have also been found in Ghana.

The data on such machines has provided a boon for cybercriminals, who can purchase computers from second-hand vendors for as little as US$27 to $40 or comb through dump sites to find them (Stewart 2011). They then use the information they have found to target the original owners or their business associates and relatives. In one of the most well-publicized examples, a Ghanaian cybercriminal obtained the discarded hard drive of US Congressman Robert Wexler and threatened to sell his social security number to identity thieves if Wexler did not pay him (Warner 2011).

Insufficient Institutional Expertise and Funding

Institutions in Ghana — including law enforcement, the judiciary and government agencies — often have a limited understanding of cybercrime and thus lack the expertise to effectively combat the problem. For example, the Commercial Crime Unit of the Ghana Police Service's Criminal Investigations Department (CID) is tasked with investigating and prosecuting cybercriminals. However,

4 This activity typically involves working in hazardous conditions. To extract the materials, workers often burn the electronic waste, releasing toxic chemicals in the process.

it often does not have the necessary technical skills to carry out digital forensics, which involve recovering and analyzing electronic evidence and preserving it in its most original form (Boateng et al. 2011).

Insufficient funding for law enforcement is a related challenge. This includes not enough funding for training police officers. Some recent training programs in digital forensics, cyber fraud detection and other cyber security-related skills have been beneficial, but more are needed. Lack of equipment is a key issue as well. For instance, the police force does not have an adequate computer lab in which to conduct digital forensics.

When law enforcement is able to find and hire technically skilled personnel, retaining them has proved difficult. Some officers, after having undergone a recent cyber-security training program, left shortly afterwards to join the private sector, which offered them significantly higher salaries for their newly acquired skills.

An Insufficient and Unclear Legal Regime

The country's current laws are insufficient and often unclear with respect to cybercrime. This makes it difficult for police, prosecutors and judges to determine how the law applies to various offences. For example, the Economic and Organised Crime Office Act (Republic of Ghana 2010), which established a specialized government body to investigate and prosecute economic and organized crime, tasked the body with investigating a host of crimes including "prohibited cyber activity." However, the act does not specify which particular cyber offences this might include. As another example, the Electronic Transactions Act (Ghana Trade Portal 2008), which is intended to facilitate electronic communications, does define the specific cyber offences covered by the act — but it does not specify procedures to ensure the integrity and admissibility of electronic evidence. As a result, members of the police force, prosecutors and judges often have different and frequently conflicting interpretations of the law regarding cybercrime.

Limited Collaboration

The problem is compounded by limited collaboration between institutions that should be working together to address the challenge. For instance, the Electronic Transactions Act requires ISPs to provide law enforcement with technical assistance in response to a court order (such as a suspect's Internet Protocol address history), but ISPs rarely do so. And when business, academia or government run projects or initiatives to combat cybercrime, they seldom coordinate with one another.

There have been attempts by foreign governments and agencies to help tackle the cybercrime challenge through training and other capacity-building initiatives, but most of these initiatives have failed to generate concrete results. One reason for this is that some capacity-building initiatives target only one specific group. For instance, one recent program provided training for prosecutors without providing complementary training for CID detectives, who investigate cybercrime cases before sending them to prosecutors for trial.

Enforcement Challenges, including Corruption

Even in instances where there is legal clarity, enforcement of cybercrime laws is often weak. The large number of victims located abroad makes prosecution more difficult (Darko 2015). Corruption, too, contributes to the lack of enforcement and is also fuelling the cybercrime challenge. For instance, fraudsters may sometimes bribe law enforcement or judges to overlook their activities. Furthermore, the government has an incentive to ignore cybercrime since it provides Ghanaians with a source of income (Morton 2011).

POTENTIAL SOLUTIONS

Job Training and Development Programs for Youth

Given the number of unemployed young men turning to cyber fraud, there is a need for development programs targeted at youth. As evidenced by their success in committing online crime, fraudsters do have some technical skills, so such schemes could foster and utilize this information technology (IT) talent (Boateng 2011). One possibility might be for the government to sponsor training programs for youth geared at preparing them to work in online outsourced roles for international companies.

Destroying or Wiping Data on Devices Before They Are Exported as Electronic Waste

To tackle cybercrime stemming from electronic waste, there must be greater efforts to destroy or wipe clean the memories of devices before they are exported. The best way to do this is to physically destroy the hard drives with a hammer or other blunt instrument. Software that erases the hard disks can also be effective. The first step is for governments of countries that export electronic waste to launch a public education campaign. Many people are unaware that the data remaining on their used devices could end up in the hands of cybercriminals. They may also not know how to safely destroy or wipe the information on these devices. It is thus essential to encourage individual responsibility in the proper disposal of used devices and to share the knowledge of how to do so.

Companies also need to behave responsibly regarding the safe disposal of used devices. The second step is therefore for governments to sensitize recycling firms that export

electronic waste to the associated cybercrime dangers; they must be made more aware of the importance of destroying or wiping all hard drives before shipping them. If necessary, governments may need to require them to do so.

Further Restricting the Export of Electronic Waste

Firms — not just recycling firms that export electronic waste but those that manufacture devices — should also be encouraged to recycle used devices instead of exporting them, as this is the most effective way to ensure that cybercriminals cannot obtain and exploit them. Recycling firms lack economic incentives to do this, however. It is significantly cheaper for them to send the devices intact to the developing world as electronic waste rather than go through the costly process of disassembling the devices, disposing of toxic substances and recuperating the materials that can be reused.

Public opinion can play an important role in incentivizing manufacturers, however. Apple, extremely conscious of its brand, has developed one of the largest recycling programs for used devices in the industry in order to bolster its "green" image. Governments can mandate that companies recycle a certain percentage of used devices or, if they already do require it, can increase the amount required. In the United States, for instance, most states have legislated that device manufacturers must pay the cost of recycling part of their electronic waste, but that percentage is often too low (Risen 2016).

Tightening regulations on the export of electronic waste will be essential too. Although many countries ostensibly ban electronic waste exports, in practice this is often flouted: the 1992 Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal, which 182 countries are party to, prohibits developed countries from exporting hazardous waste, including electronic waste, to developing countries in most instances. Many companies, however, skirt national regulations by classifying electronic waste as "donations of second-hand goods." Governments must close this loophole if the Convention is to be effective.

Moreover, the biggest exporter of electronic waste to Ghana — the United States — is not bound by the Convention. Although the United States signed the agreement, ratification has been gridlocked in Congress. It is the only industrialized country in the world not to have ratified the Convention (Risen 2016). The United States needs to do so to stem the flow of electronic waste to Ghana and the cybercriminal activity that derives from it.

Regulatory Measures

To address the insufficiency of current legislation regarding cybercrime, Ghana should consider incorporating new measures into law such as the legal right to asset seizure of the proceeds of cybercrime, either by introducing new legislation or by amending existing legislation. Doing so would not only give law enforcement and judges greater power to punish known cybercriminals but also serve as a deterrent to others.

In order to tackle the lack of clarity of current laws involving cybercrime, Ghana should also sign the Convention on Cybercrime (the Budapest Convention), an international treaty on Internet and computer crime that harmonizes national laws. This would align Ghanaian law with international norms and improve the coherence of the country's legislation. In June 2016, Ghana was invited to accede to the Budapest Convention; doing so is essential if the country is to effectively curb cybercrime.

Increasing Knowledge and Understanding of Cybercrime among All Stakeholders, including Bolstering Technical Skills and Funding for Law Enforcement

Increasing knowledge and understanding of cybercrime among all stakeholders is essential. Given that law enforcement personnel often have insufficient technical knowledge, more training programs in digital forensics and other related areas are needed. It is also essential to recruit professional IT experts when possible.

To achieve this, the government must allocate greater funding to the CID. This, in turn, will require persuading the government to make the fight against cybercrime a key priority. The government has begun to pay increased attention to the issue since some international companies restricted the use of credit cards in Ghana because of high incidences of cyber fraud. As a result, the government is beginning to realize that cybercrime is a problem for the country's burgeoning e-commerce industry and its international business reputation, and thus for the economy as a whole. Despite this, greater efforts are needed to increase the government's awareness of the cybercrime threat. One way to do so would be to conduct an economic study to attempt to quantify the business revenue lost to Ghana because of cybercrime.

Engaging All Stakeholders

Effectively tackling cybercrime will require the cooperation of all stakeholders: police, prosecutors, the judiciary, government ministries and agencies, parliament, the private sector (including ISPs) and civil society. The government has made important progress recently: the Ministry of Communications launched the country's National Cyber Security Policy and Strategy

in 2015 and held a validation workshop with a range of stakeholders, including ISPs. With the help of the International Telecommunication Union, Ghana also set up a Computer Emergency Response Team in 2014 to coordinate cyber-security incident response. However, much more remains to be done.

There is a need for greater collaboration between all stakeholders, including for improved information sharing between ISPs and law enforcement as well as between law enforcement and the judiciary. Steps to achieve this might involve either the government or civil society convening regular forums on cybercrime that bring together all stakeholders to discuss the challenges.

An additional method of enhancing coordination between law enforcement and the judiciary could involve developing a best practices document on the handling of electronic evidence. Such a document is needed in order to standardize the process of handling cybercrime evidence across the country and to ensure the integrity of electronic evidence in cybercrime investigations and prosecutions.

International cooperation is key as well. Given that cybercrime transcends national borders, the Ghanaian police needs to work more closely with members of ECOWAS as well as with the broader international community in order to more effectively conduct cross-border investigations and evidence collection.

A POSSIBLE OVERARCHING STRATEGY

The closely linked nature of Internet infrastructure development and cybercrime means that policy makers may want to consider deploying an overarching strategy that encompasses both. In particular, they should consider the following measures.

LEVERAGING MULTIPLIER EFFECTS

This analysis has pointed to certain root causes that are common to both Internet infrastructure development challenges and the cybercrime problem. Specifically, poverty and corruption feature as root causes of both. This suggests that, when determining where to invest limited resources, one beneficial strategy for policy makers may be to concentrate their efforts on some of the shared root causes of both problems because this will have a multiplier effect. Thus, investing in programs that target poverty alleviation or anticorruption — which tackle shared causes of both issues — are likely to have a larger impact on the country's well-being than programs that focus on independent causes.

A JOINT APPROACH

Taking a joint approach to solving these problems in discussions and workshops could prove highly beneficial. For example, this analysis has also pointed to a solution that is common to both Internet infrastructure development challenges and cybercrime problems: that is, the need to bring all stakeholders in each case together. Not only are the problems interlinked, but there is also significant overlap in terms of the major stakeholders who are involved. In addition to regular meetings between stakeholders for each issue suggested earlier in this paper, it might also be beneficial to hold a number of joint meetings so as to approach these issues in a holistic manner.

Joint meetings would generate ideas on how best to tackle these challenges together in order to be most effective. For example, if a lack of legitimate jobs is a significant factor contributing to cybercrime and if developing Internet infrastructure is key to the country's economic growth, then it might make sense to launch a public works program that employs people to work on large Internet infrastructure projects. In this way, it would be possible to provide employment that would help reduce cybercrime and simultaneously improve the country's Internet infrastructure, which would in turn stimulate economic growth.

CONCLUSIONS

Further promoting the development of Internet infrastructure in Ghana is central to the country's continued economic growth and prosperity. Yet increases in Internet connectivity will — if corresponding measures are not employed to keep cybercrime at bay — also result in an increase in cybercrime. This paper suggests that an overarching strategy that combines leveraging multiplier effects (i.e., concentrating efforts on some of the shared root causes of both problems) and a joint approach (i.e., holding a number of joint meetings and workshops to approach these interlinked issues in a holistic manner) would be the most effective means of improving well-being.

Some areas for further study include additional research into common root causes — beyond poverty and corruption — of both Internet infrastructure development challenges and cybercrime problems. Supplementary work is also needed to consider potential joint solutions as well. Joint meetings bringing together all major stakeholders would be an ideal venue in which to do this sort of brainstorming.

Although this paper focuses on Ghana, many of the findings can likely be applied to neighbouring countries in the West Africa region — including Nigeria and Cameroon, which have markedly similar characteristics. In some cases, they can be extrapolated for developing

nations more broadly, given that a number of emerging countries are facing similar issues. Given that cybercrime impacts all countries around the world, irrespective of their level of development, it is clear that addressing the dual challenges of Internet infrastructure development and cybercrime is an urgent priority.

ACKNOWLEDGEMENT

The authors are grateful to the UK Foreign and Commonwealth Office for funding this paper.

WORKS CITED

Abbey, Emelia Ennin. 2016. "Vodafone bemoans rising cable theft." Graphic Online, April 26. www.graphic.com.gh/business/business-news/vodafone-bemoans-rising-cable-theft.html.

Abdul-Jalil, Yakubu. 2015. "Google Ghana Launches Metro Fibre Project." Graphic Online, October 3. http://graphic.com.gh/news/general-news/50586-google-ghana-launches-metro-fibre-project.html.

Abubakar, Zulaihatu. 2012. "Sakawa Guy Confesses." Modern Ghana, September 22. www.modernghana.com/news/419261/1/sakawa-guy-confesses.html.

Acquaye, Nana Appiah. 2013. "The Rise and Fall of Ghana's Biggest Internet Café." BiztechAfrica, February 14. www.biztechafrica.com/article/rise-and-fall-ghanas-biggest-Internet-cafe/5320/#.VoH31FK_Gbg.

———. 2014. "Ghana Roads Ministry: Cable Cuts a Concern." BiztechAfrica, February 4. www.biztechafrica.com/article/ghana-roads-ministry-cable-cuts-concern/7647/#.VoCPZVK_Gbg.

———. 2015. "NCA to Auction Infrastructure License." BiztechAfrica, August 7. www.biztechafrica.com/article/nca-auction-infrastructure-license/10434/#.VoL9UVK_Gbg.

Adam, Basiru. 2014. "What Fibre Cuts Do to You." *B&FT Online*, July 30. http://thebftonline.com/business/ict/11896/what-fibre-cuts-do-to-you-.html.

Amoyaw-Osei, Y., O. O. Agyekum, J. A. Pwamang, E. Mueller, R. Fasko and M. Schluep. 2011. *Ghana e-Waste Country Assessment: SBC e-Waste Africa Project*. Coordinated by the Basel Convention. March.

Ampomah, Eunice Hilda. 2016. "Vodafone sets up cable theft courts." Ghana News Agency, April 20. www.ghananewsagency.org/social/vodafone-sets-up-cable-theft-courts-102918.

Armstrong, Alice. 2011. "Sakawa Rumours: Occult Internet Fraud and Ghanaian Identity." Working Paper No. 8/2011. University College London, Department of Anthropology. www.ucl.ac.uk/anthropology/research/working-papers/082011.pdf.

BiztechAfrica. 2013. "Ghana Telecoms, Roads Collaborate to Minimise Cable Cuts." March 13. www.biztechafrica.com/article/ghana-telecoms-roads-collaborate-minimise-cable-cu/5659/#.VRgjvGbZfAo.

Boakye, Kojo. 2014. "Affordable Internet in Ghana: The Status Quo and the Path Ahead." A4AI (Alliance for Affordable Internet). https://a4ai.org/wp-content/uploads/2014/07/Ghana-Case-Study_FINAL.pdf.

Boateng, Richard, Longe Olumide, Robert Stephen Isabalija and Joseph Budu. 2011. "Sakawa — Cybercrime and Criminality in Ghana." *Journal of Information Technology Impact* 11 (2): 85–100. www.jiti.com/v11/jiti.v11n2.085-100.pdf.

Calandro, Enrico, Christoph Stork and Alison Gillwald. 2012. "Internet Going Mobile: Internet Access and Usage in 11 African Countries." Policy Brief No. 2. Research ICT Africa. www.researchictafrica.net/publications/Country_Specific_Policy_Briefs/Internet_going_mobile_-_Internet_access_and_usage_in_11_African_countries.pdf.

Citifmonline. 2016a. "Govt backtracks on withdrawal of 20% tax on mobile phones." Citifmonline.com, February 4. http://citifmonline.com/2016/02/04/govt-draws-back-on-20-tax-on-mobile-phones/.

———. 2016b. "Telecom analyst demands tax cuts on imported phones." Citifmonline.com, August 11. http://citifmonline.com/2016/08/11/telecom-analyst-demands-tax-cuts-on-imported-phones/.

CRU Wire and Cable News. 2014. "Ghana Solves Theft Problems with Overhead Fibre Optic Cable," November 18. http://wireandcablenews.crugroup.com/wireandcablenews/news/free/2014/11/2071615/.

Danquah, Paul and O. B. Longe. 2011. "Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective." *Journal of Information Technology Impact* 11 (3): 169–82. www.jiti.net/v11/jiti.v11n3.169-182.pdf.

Darko, Sammy. 2015. "Inside the World of Ghana's Internet Fraudsters." BBC Africa, May 10. www.bbc.com/news/world-africa-32583161.

Dela Klutse, Felix. 2015. "7.5m Ghanaians live on GH¢3 daily." JOY Online, March 16. www.myjoyonline.com/business/2015/march-16th/75m-ghanaians-live-on-gh3-daily.php.

Doyon-Martin, Jacquelynn. 2015. "Cybercrime in West Africa as a Result of Transboundary E-Waste." *Journal of Applied Security Research* 10 (2): 207–20. www.tandfonline.com/doi/pdf/10.1080/19361610.2015.1004511.

Foster, William, Seymour Goodman, Eric Osiakwan and Adam Bernstein. 2004. "Global Diffusion of the Internet IV: The Internet in Ghana." *Communications of the Association for Information Systems* 13: 654–81.

Frempong, Godfred. 2012. "Understanding What Is Happening in ICT in Ghana: A Supply- and Demand-side Analysis of the ICT Sector." Evidence for ICT Policy Action Policy Paper 4, Research ICT Africa. http://researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_4_-_Understanding_what_is_happening_in_ICT_in_Ghana.pdf.

Ghana Business News. 2015. "Ghana Road Fund Carries forward over GH¢230m Indebtedness — Minister." March 28. www.ghanabusinessnews.com/2015/03/28/ghana-road-fund-carries-forward-over-gh%C2%A2230m-indebtedness-minister/.

———. 2014. "MTN Worried over Fibre Optic Cuts." July 4. www.ghananewsagency.org/science/mtn-worried-over-fibre-optic-cuts--76839.

———. 2016. "Trade Ministry empowers Vodafone to fight cable theft." Modern Ghana, August 30. www.modernghana.com/news/716068/trade-ministry-empowers-vodafone-to-fight-cable-theft.html.

Ghana Trade Portal. 2008. *Electronic Transactions Act (Act 772), 2008*. www.ghanatrade.gov.gh/Laws/electronic-transactions-act-act-7722008.html.

GhanaWeb. 2012a. "Community Members Act to Stop Theft of Vodafone Cables." October 31. www.ghanaweb.com/GhanaHomePage/regional/artikel.php?ID=254912.

———. 2012b. "Vodafone Cable Thieves Arrested by Ghana Police." October 10. www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=252728.

———. 2015a. "Four Vodafone Staff Jailed over Cable Theft." May 19. www.ghanaweb.com/GhanaHomePage/crime/4-Vodafone-staff-jailed-over-cable-theft-358740.

———. 2015b. "Fibre-optic Operators Call for Cable Protection Law." November 30. www.ghanaweb.com/GhanaHomePage/NewsArchive/Fibre-optic-operators-call-for-cable-protection-law-397325.

———. 2016. "Vodafone cracks down on cable theft." April 25. www.ghanaweb.com/GhanaHomePage/crime/Vodafone-cracks-down-on-cable-theft-433623.

Graphic Online. 2009. "Sakawa rituals paralyses student." Modern Ghana, March 27. www.modernghana.com/news/208469/1/sakawa-rituals-paralyses-student.html.

———. 2012. "Telcos Co-Share Ducts to Lay Fibre Cables." Modern Ghana, August 28. www.modernghana.com/news/414121/1/telcos-co-share-ducts-to-lay-fibre-cables.html.

IT News Africa. 2015. "Ghana: Alcatel-Lucent Completes Fibre Backbone Project." May 20. www.itnewsafrica.com/2015/05/ghana-alcatel-lucent-completes-fibre-backbone-project/.

JOY Online. 2013. "Government to Ban Copper Export — Minister." Modern Ghana, June 4. www.modernghana.com/news/467023/1/government-to-ban-copper-export-minister.html.

———. 2014. "MTN Delivers Digital Advantage to Customers through Aggressive Network Investments." May 8. www.myjoyonline.com/business/2014/May-8th/mtn-delivers-digital-advantage-to-customers-through-aggressive-network-investments.php.

Kavanagh, Camino, ed. 2013. "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries." New York University, Center for International Cooperation. Report, June. http://cic.nyu.edu/sites/default/files/kavanagh_crime_developing_countries_report_w_annexes.pdf.

Klein, Peter. 2009. "Ghana: Digital Dumping Ground." FrontlineWorld.www.pbs.org/frontlineworld/stories/ghana804/video/video_index.html.

Kunateh, Masahudu Ankiilu. 2015. "Ghana: Telcos Welcome New Directive to Halt Fibre Cuts." *All Africa/The Chronicle*, January 7. http://allafrica.com/stories/201501071449.html.

Morton, Thomas. 2011. "The Sakawa Boys: Inside the Bizarre Criminal World of Ghana's Cyber-Juju Email Scam Gangs." Motherboard, April 5. http://motherboard.vice.com/read/the-sakawa-boys-inside-the-bizarre-criminal-world-of-ghanas-cyber-juju-email-scam-gangs.

Mustapha, Suleiman. 2014. "Engage Telcos in Road Construction." Graphic Online, December 15. http://graphic.com.gh/news/general-news/35454-engage-telcos-in-road-construction.html.

Naphtal, Akin. 2015. "Telcos in Ghana Welcome New Directive to Minimise Fibre Cuts." *Mobile World Mag*, January 8. http://mobileworldmag.com/telcos-ghana-welcome-new-directive-minimise-fibre-cuts/.

National Communications Authority. 2015. "News Item: Mobile Data Figures for the Month of July 2015." www.nca.org.gh/downloads/Data_Market_Figures_July2015.pdf.

National Crime Agency. 2014. "Romance Fraud Mastermind Jailed in Ghana." National Crime Agency, October 31. www.nationalcrimeagency.gov.uk/news/478-romance-fraud-mastermind-jailed-in-ghana.

Ogundeji, Olusegun Abolaji. 2014. "Ghana's Import Tax Removal on Smartphones Expected to Boost Local Africa Production." PCWorld.com, December 10. www.pcworld.com/article/2858172/ghanas-import-tax-removal-on-smartphones-expected-to-boost-local-africa-production.html.

Republic of Ghana. 2010. *Economic and Organised Crime Office Act (Act 804), 2010*. http://fic.gov.gh/wp-content/uploads/2015/11/EOCO-Act-804.pdf.

Risen, Tom. 2016. "America's Toxic Electronic Waste Trade." US News and World Report, April 22. www.usnews.com/news/articles/2016-04-22/the-rising-cost-of-recycling-not-exporting-electronic-waste.

Sikiti da Silva, Issa. 2014. "Ghana Govt Worried about Rising Cybercrime." BiztechAfrica, June 5. www.biztechafrica.com/article/ghana-govt-worried-about-rising-cybercrime/8250/#.V4fuUhiG6T8.

Stewart, Samantha. 2011. "Ghana's e-Waste Dump Seeps Poison." Newsweek.com, July 25. http://europe.newsweek.com/ghanas-e-waste-dump-seeps-poison-68385?rm=eu.

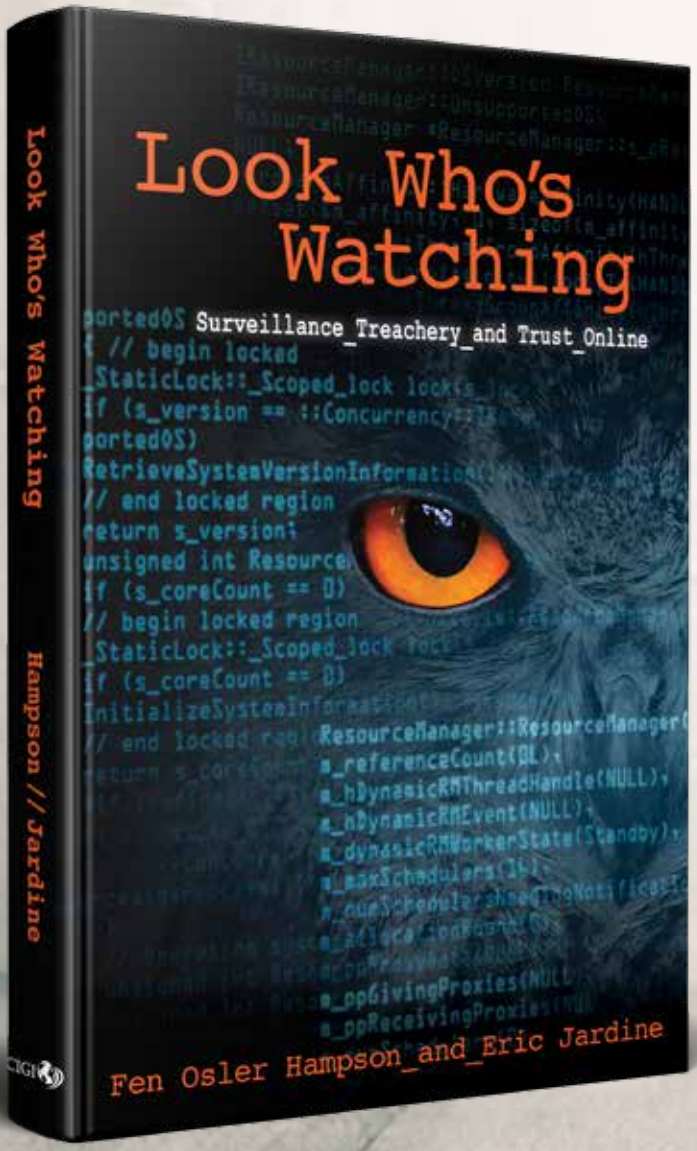
Warner, Jason. 2011. "Understanding Cyber-Crime in Ghana: A View from Below." *International Journal of Cyber Criminology* 5 (1): 736–49.

CIGI PRESS

ADVANCING POLICY IDEAS AND DEBATE

cigionline.org

AVAILABLE NOW



Look Who's Watching

Surveillance, Treachery and Trust Online

Fen Osler Hampson and Eric Jardine

Edward Snowden's revelations that the US National Security Agency and other government agencies are spying on Internet users and on other governments confirmed that the Internet is increasingly being used to gather intelligence and personal information. The proliferation of cybercrime, the sale of users' data without their knowledge and the surveillance of citizens through connected devices are all rapidly eroding the confidence users have in the Internet.

To meet the Internet's full potential, its users need to trust that the Internet works reliably while also being secure, private and safe. When trust in the Internet wanes, users begin to alter their online behaviour. A combination of illustrative anecdotal evidence and analysis of new survey data, *Look Who's Watching* clearly demonstrates why trust matters, how it is being eroded and how, with care and deliberate policy action, the essential glue of the Internet — trust — can be restored.

October 2016
978-1-928096-19-1 | hardcover
CDN $32 + shipping

> *The authors have produced a clear, timely and essential book about the importance of trust as an engine for the Internet. We must foster that trust if the global Internet is to continue to flourish.*
>
> — Michael Chertoff, Executive Chairman and Co-Founder, Chertoff Group, and former secretary of the US Department of Homeland Security

Centre for International Governance Innovation

CIGI Press books are distributed by McGill-Queen's University Press (mqup.ca) and can be found in better bookstores and through online book retailers.

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of Finance	Shelley Boettger
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief of Staff and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Sharon McCartney
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org