

# Cyber Security in Ghana

Key Issues and Challenges

Policy Brief June, 2017

This publication is available for public use. It can be reproduced or quoted provided Media Foundation for West Africa is quoted as the source.

Published by Media Foundation for West Africa (MFWA)  
30 Duade Street, Kokomlemle,  
P.O.Box LG 730 Legon, Accra-Ghana  
Telephone: +233(0) 2242470  
Twitter: @TheMFWA  
Facebook: Media Foundation for West Africa  
Email: info@mfw.org  
Website: www.mfw.org

©Media Foundation for West Africa 2017

Produced with support from e-Crime Bureau  
Tel: +233 (0) 207131646

Designed and Printed by Bluevyne Ltd  
Tel: +233 (0) 303 932 712  
+233 (0) 054 662 121  
www.bluevyne.com

#### **Disclaimer**

This report is made possible with funding support from UK-based Global Partners Digital. The content of this Report, however, are the sole responsibility of the author and do not necessarily reflect those of Global Partners Digital

# TABLE OF CONTENTS

<b>Executive Summary</b>	i
<b>Cyber Development &amp; Cyber [In] Security in Ghana</b>	1
1. Overview – Cyber Criminality in Ghana	1
2. Specific Cyber Developments in Ghana	2
3. The Cyber Threat Landscape	4
4. Specific Cybercrime Trends and Cyber Security Issues in Ghana	6
5. Other Recent Developments	9
<b>How Ghana is Ranked Globally in Terms of Cyber Security</b>	12
<b>Current Policy and Regulatory Framework in the Fight Against Cyber Criminality in Ghana</b>	14
1. Current Policy, Regulatory Framework And Initiatives	14
2. Issues with Awareness and Capacity, Legislation Deficiencies And Regulatory Enforcement	15
<b>Recommendations towards Tackling Cyber Security Challenges in Ghana</b>	16
<b>References</b>	18
<b>Glossary</b>	19

## Executive Summary

The Information and Communication Technology (ICT) environment in Ghana has recorded major developments in recent years. Both the public and private sectors have seen lots of developments and expansions, including the Eastern Corridor Fibre-optic Backbone infrastructure by government, implementation of 4G-LTE network, mobile financial services, e-banking products, e-commerce, among others.

These developments have, however, affected the cyber security landscape with cyber threats such as hacking, data leakages, social engineering schemes, cyber fraud, SIM Box fraud, etc. Recent reports of cyber-attacks in Ghana have been in the form of website defacement, attacks on state institutions such as a recent attack on Ghana's Electoral Commission, ransomware attacks, e-payment threats, social media threats, etc.

The government and relevant stakeholders have been taking steps to address these emerging threats including the adoption of the National Cyber Security Policy & Strategy (NCSPS) by Cabinet in 2016; the setting up of the Ghana Computer Emergency Response Team (CERT-GH); enactment of the Data Protection Act 2012 (Act 843); and the setting up of the Data Protection Commission, among others. However, cyber security challenges persist as a result of a number of factors such as lack of a culture of cyber security consciousness and limited awareness on cyber security issues among businesses and individuals; challenge of enforcement of legislation; as well as limited capacity among law enforcement agencies in the detection, investigation and prosecution of internet-facilitated crimes.

This policy brief, therefore, focuses on cyber security issues in Ghana. It highlights some of the developments and critical challenges within the cyber security environment in Ghana as well as some of the interventions needed to tackle them. The interventions proposed include a need to adopt a cyber security governance structure, build capacity of law enforcement and security agencies, develop an effective National Identification System, standardise and develop cyber security best practices for both public and private sector organisations, ensure private sector involvement and improve regional and international cooperation in fighting cybercrime.

# Cyber Developments & Cyber [In]Security in Ghana

## 1. Overview – Cyber Criminality in Ghana

Ghana was among the first countries in Africa to connect to the Internet and the country's Internet penetration rate is among the top in Africa [1]. There have been several developments in the Information and Communications Technology (ICT) sector in Ghana within the past 15 years with the country gradually transitioning into an emerging information technology society. Ghana continues to develop its Information and Communications Technology (ICT) sector and current developments in mobile financial services have significantly contributed to the rapid growth of the sector. The government's policy on ICT – *The Ghana ICT for Accelerated Development (ICT4AD) Policy* is the backbone of major ICT developments in the country.

While Information and Communications Technology (ICT) presents opportunities for development, there is a major setback that undermines the full realisation of ICT for social, political and economic transformation. The development and adoption of ICT have led to the emergence and the rise of cyber criminality in Ghana. Cyberattacks target confidentiality, integrity and available ICT assets. While the emergence of cyber criminality is a global phenomenon engineered by the development of ICT and Internet technologies, available study suggests that Ghana in particular and West Africa in general have become a hub for cyber criminality. For example, a study conducted by the United Nations Office on Drugs and Crime (UNDOC) – *The Globalization of Crime (2010)* – identifies West Africa as a major cybercrime-offending region. The *Global Internet Crime Report (2013)* by the Federal Bureau of Investigations (FBI) also labels Ghana as among the top 10 cybercrime-originating countries.

To further highlight the country's seemingly global recognition as a major cybercrime region, Ghana has contributed to the global cybercrime lexicon with the word 'sakawa' which refers to cybercrimes committed by Ghanaian perpetrators. Major international e-commerce operators and online merchants including Amazon, Paypal and other online retail outlets have blacklisted Ghana – residents in Ghana are unable to purchase goods and services online with their credit cards because of cyber fraud.

This policy brief seeks to highlight the Ghanaian cybercrime and cyber security landscape, the regulatory framework within which cyber security issues in the country are situated, and recommendations to tackle existing and emerging cybercrime trends – with emphasis on the role of government bodies, law enforcement and security agencies, private sector stakeholders and the Ghanaian public.

## 2. Specific Cyber Developments in Ghana

Before examining the cyber security threat landscape in Ghana, it is important to highlight major cyber developments in the country within the last few years. While these cyber developments underline Ghana's growth in ICT, it is essential to highlight the negative impacts in terms of cyber security issues. Below are highlights of specific cyber developments of interest:

- **Development in the Telecommunication Sector** – Ghana's Internet penetration rate is among the highest on the continent. Availability of mobile broadband to Internet users has contributed to improved access. Both 3G and 4G mobile broadband services are readily available - giving cybercriminals easy access and faster Internet connectivity. Government has also put in place the Eastern corridor fibre-optic backbone infrastructure of nearly 800 kilometres to help bridge the digital divide between urban and rural areas [2]. The Eastern corridor fibre-optic infrastructure is also expected to improve communication services in the country and accelerate development across the country through modern communication technology.
- **Mobile Penetration and Smartphone Usage** - Mobile phones are helping to bridge the digital divide by providing access to telecommunication and Internet services even in rural areas. Smartphone penetration keeps increasing according to data from the National Communications Authority (NCA) [3]. The growth of smartphone usage is fuelling other forms of cyber-attacks targeting mobile users.
- **E-Banking Products and Services/E-Payments** – Development of Internet technology in the country and Bank of Ghana's policy on cashless economy is driving innovation in the financial sector. Several Internet banking and mobile banking products and services, including the use of credit cards, are available to the public. Financially-motivated cybercriminals usually target users of these products and services for cyber-attacks.
- **Business use of ICT** – Most businesses, including SMEs in Ghana, rely on ICTs for their operations. Business functions have been automated with the availability of websites and software applications. Business automation provides the conduit for cyber criminals to target organisations. These attacks have contributed to several data breaches raising concerns about data protection and privacy issues.
- **Online Shopping/E-commerce Services** – Ghana is witnessing emergence of electronic commerce activities with organisations such as tonaton.com, cheki.com and zoobashop.com as active players. E-commerce is predicted to increase in the coming years and this anticipated cyber development has implications on cyber-attacks targeting ICT infrastructures and users in Ghana.

- **Mobile Financial Services** – Evidence suggests that the telecommunications sector is pioneering mobile money products and services in Ghana. The development is enhancing the participation of the unbanked population especially those in rural areas in the financial ecosystem. According to recent statistics by the Bank of Ghana (BoG), the sector from January to March 2017 recorded a growth of 9,262,376 active mobile money subscribers compared to 5,336,142 in the same period in 2016. This represents a growth of 73.58%. The value of transactions increased from GHS 13.76 million from January to March 2016 to GHS 31.03 million from January to March 2017 representing a growth rate of 125.39%. Further growth in the sector is expected with the anticipation of Mobile Money Inter-operability by September 2017, according to government sources. However, mobile money platforms are becoming attractive targets for cyber criminals.
- **E-Government Services** – Specific e-government initiatives have been activated to enhance service delivery to the public. An e-government portal ([www.eservices.gov.gh](http://www.eservices.gov.gh)) has been set up with the aim of providing a single service point for the public to access specific government services including driver's license, passport and other public services.
- **Social Media Usage** - Recent statistics by the National Communication Authority (NCA) show that Ghana's total mobile data subscription was 19,642,152 at the end of December 2016. The popularity of social media in Ghana is contributing to Internet access. While social media is enhancing Internet freedom and social communication, the increase in social media users in Ghana provides opportunity for cyber attackers.

### 3. The Cyber Threat Landscape



*[State of Cybercrime in Ghana]*

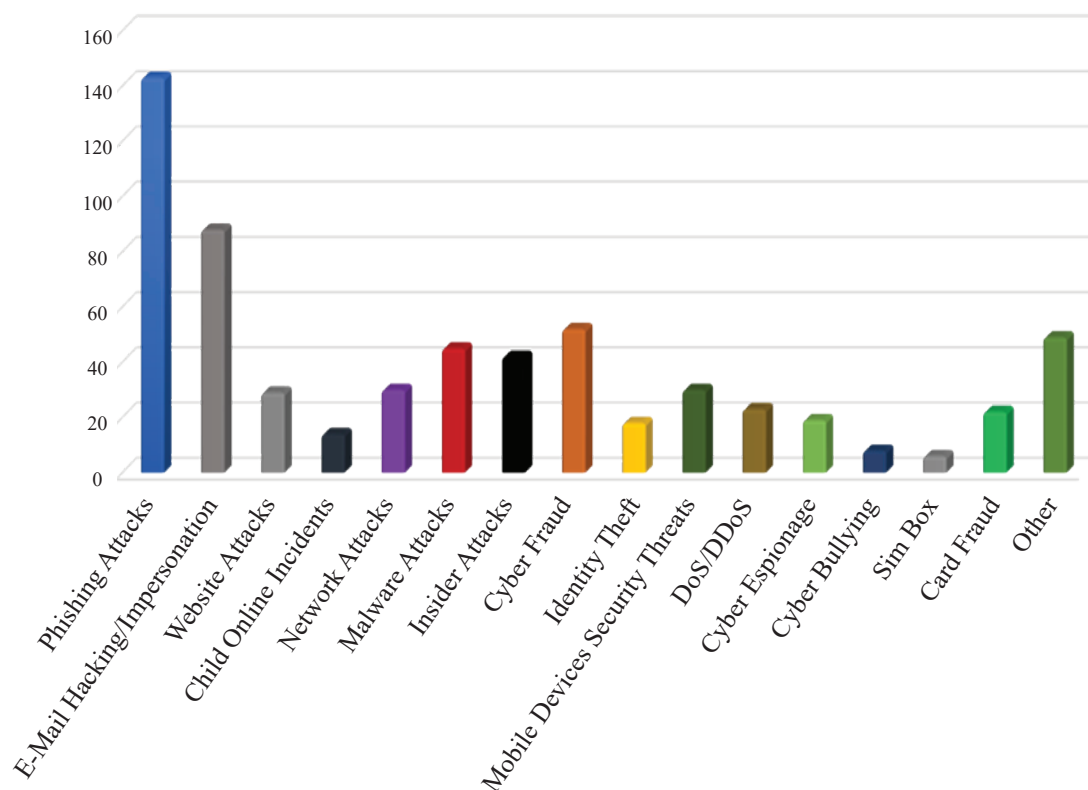
Analyses covering the IT environment of organisations within the public and private sectors in Ghana have identified the above as the major cyber threat areas targeting the IT landscape. Further analysis suggests existing internal and external control measures are inadequate to detect and prevent these technology-driven attacks. Various cybercrime cases have been reported across various sectors. Some of these attacks include Web attacks, IT-based network attacks, Data breaches, Malware attacks, E-mail attacks, Distributed Denial of Service (DDoS) incidents, Man-In-The Middle (MITM) attacks, insider related IT fraud and Phishing attacks, among others. Network intrusions resulting from system and application vulnerabilities, weak internal security controls and non-compliance of IT procurement and usage best practices have been reported.

In May 2017, a cyber-attack involving the “WannaCry” Ransomware affected many notable organisations globally. Experts rate this attack as the world’s biggest single cyber-attack incident in terms of the number of countries affected. The attack targeted at least 150 countries and close to 200,000 computers and databases of organisations were affected. Analysis of Ghana’s cyber environment suggests such attacks are likely to affect Ghana’s IT systems and networks due to specific vulnerabilities – including lack of a culture of cyber security awareness and significant usage of unlicensed (cracked) operating systems across the various sectors.



The following Statistics further highlight the above developments.

### DISTRIBUTION OF CYBERCRIME INCIDENTS REPORTED TO E-CRIME BUREAU - 2016



Cybercrime Incidents Reported	Number Of Reported Cases
Phishing Attacks	143
E-Mail Hacking/Impersonation	88
Website Attacks	29
Child Online Incidents	14
Network Attacks	30
Malware Attacks	45
Insider Attacks	42
Cyber Fraud	52
Identity Theft	18
Mobile Devices Security Threats	30
DoS/DDoS	23
Cyber Bullying	19
Cyber Espionage	8
Sim Box	6
Card Fraud	22
Other	49
<b>Total</b>	<b>618</b>

*[Distribution of Cybercrime Incidents]*

#### **4. Specific Cybercrime Trends and Cyber Security Issues in Ghana**

Cyber security issues have become national security issues for most countries and Ghana is no exception. The evolution of cyber-attacks including attacks targeting critical national infrastructures has contributed to the reasons why cyber-attacks are now considered not only a social or economic issue, but also a national security concern. This section highlights specific cyber security trends in Ghana as well as the perpetrators and victims of such attacks.

- **Cyber Fraud**

Cyber fraud is a classic form of cyber criminality in Ghana. Identity fraud, romance fraud, inheritance fraud, credit card fraud, advance fee fraud and business scams are different schemes being adopted by cybercriminals to target their victims. Perpetrators of cyber fraud – known in Ghana as Sakawa – normally adopt social engineering tricks to exploit the ignorance of their targets. Most foreigners are targeted with cyber fraud. One modus operandi usually adopted by cyber fraudsters is to set up a bogus website – either as a recruitment agency, real estate agency, or a business operating in the oil and gas sector specifically to defraud target victims. For example, when Ghana discovered oil in commercial quantities in late 2000, cyber fraudsters adopted deceptive modus operandi around oil and gas sector and many businesses including foreign firms were targeted and defrauded.

- **SIM Box Fraud**

SIM Box fraud, also known as Interconnect Bypass fraud is the most common fraud targeting the telecommunications sector. Perpetrators of SIM Box fraud divert international calls through SIM boxes effectively bypassing the interconnect gateway through the use of local pre-paid SIM Cards. Thus, international calls which attract higher rates are terminated through the use of SIM box devices using locally acquired pre-paid SIM cards. According to the National Communications Authority (NCA), Ghana lost more than US\$20 million from a SIM Box incident in which the Anti-Telecom Fraud Task Force arrested seven suspected SIM Box fraudsters [4]. The suspects arrested included foreign nationals such as Syrian and Pakistani citizens. In June 2016, the former Chief Executive Officer of the Ghana Real Estates Developers Association (GREDA), Dr. Alex Tweneboah, was sentenced to two years imprisonment by Accra Financial Crimes Court for engaging in SIM box fraud [5]. Addressing SIM Box fraud was one of the key arguments espoused by the government when it decided to introduce the Interconnect Clearing House (ICH) in 2014. Even though the Telecommunication Chamber objected to the implementation of the initiative, the project was awarded to Afriwave Ghana Ltd for implementation [6].

- **Mobile Money Fraud**

The mobile money sector in Ghana has recorded major fraudulent incidents usually categorised into system-related fraud, agent-driven fraud and customer-driven fraud. These mobile money fraud schemes including scams/impersonation, password compromises, interception of mobile money tokens, attacks on merchants, unauthorised SIM swaps, system breaches and unauthorized access to customer/merchant's transactional data have been reported to law enforcement agencies by customers and telecommunication companies. Lack of awareness on mobile money transaction risks remains the topmost vulnerability and subscribers are being targeted by attackers on daily basis. Some security firms and corporate organisations are working to bridge the knowledge/awareness gap on mobile money operations through active engagement with law enforcement agencies and the media.

- **Hacking**

Hacking incidents targeting both government ICT infrastructures and that of the private sector have been reported in recent times. The hacking of Ghana government websites in the early part of 2015 highlights some of the attacks targeted at government technology infrastructure [7]. In April 2017, several websites of media houses were targeted through Distributed Denial of Service (DDoS) attacks [8]. Assessment and investigations of such activities suggest that most active websites in Ghana are running on old technology platforms and sub-standard tools which have developed vulnerabilities. Unfortunately, few organisations conduct regular system security audits to identify these weaknesses to resolve them in time in order to prevent such attacks. It is predicted that, future hacking attacks could target Ghana's critical national infrastructures including data centres, technology infrastructure of financial institutions and e-government networks among others.

- **Botnets & Malware Attacks**

The use of bots and malware attacks represent advanced form of cyber threats in Ghana. The use of bots by cybercriminals is becoming very popular because the crime-ware allows cyber criminals to take control of many infected computers to commit cyber-attacks on a large scale. Generally, most of the target computers are not protected with appropriate security applications such as antivirus while others run pirated software programmes. Unfortunately, most computer users in Ghana are unaware of this sophisticated cyber threat as they are unable to detect the presence of bots or malware on their computer systems themselves. Computer systems in Ghana are vulnerable to such attacks which are usually designed to steal users' confidential information.

- **Data Breaches**

Data breaches especially across the business sector have been recorded even though such incidents are not usually reported by telecommunication providers

despite legal requirements by the Data Protection Act (Act 843) for such breaches to be reported to the Data Protection Commission. Several investigations have been conducted into data-breach incidents involving organisations that collect personal data about customers/users. In one incident, details including bank account details, date of birth, details of children, residential addresses and other personal information belonging to users were obtained by an adventurous hacker who targeted the IT infrastructure of telecommunication providers. Another incident reported involved a technical employee – an insider who used his legitimate user account to illegally access confidential information of customers. There are other instances where computer and mobile phone repairers have illegally accessed confidential and sometimes sensitive data from laptops and mobile phones of target customers. Despite these incidents, there is generally lack of a culture of reporting cyber breaches to the Data Protection Commission. The Commission on its part, tries to use available platforms, such as the Data Protection Conference held in Accra in April 2017, to encourage data subjects to report incidents of personal data breaches.

- **Child Online Safety Issues**

Child online safety has become a major cyber security concern especially for parents. Social media in particular and availability of smartphones and other handheld devices are driving children online in Ghana. Cyber predators are taking advantage of Internet anonymity to target young and vulnerable children. Children’s innocent exposure to the risks online remains the most critical safety concern for parents and stakeholders. There are several examples where children have been exposed to group sex online, violent rape involving minors, and other harmful contents. Reports suggest Internet pornography use is widespread among children and juveniles. Children are vulnerable to the negative effects because their brains get ‘rewired’ when exposed to such harmful materials online. Because of the current risks associated with Children on the Internet, Child Online Protection (COP) was integrated into the National Cyber Security Policy & Strategy as one of the main focus areas. Subsequently, the Ministry of Communications in 2016 setup up a National COP Steering Committee to develop a National COP Framework for implementation [9].

- **Smartphone Security threats**

The proliferation in the use of Smartphones to access the Internet is changing the cyber-threat landscape globally. In Ghana, smartphone devices continue to permeate all aspects of our social and business environments. It appears that most Ghanaians have “dropped the yam’ with many people using smartphone devices.’ These developments are fuelling cyber security attacks targeting smartphone users. Phishing attacks, smartphone data leakages, spyware and adware attacks, malware infections of mainly Android devices as well as covert monitoring by criminals are examples of smartphone security issues targeting users in Ghana. Based on several complaints received from the corporate sector, the Ghana

Chamber of Commerce & Industry has, for instance, undertaken some seminars to create awareness on smartphone security issues for corporate executives.

While other forms of cyber security attacks such as denial of service attacks, phishing attacks, website defacements and ATM fraud have been reported, the above highlights the major cyber security trends in Ghana that require technical, policy and legal considerations.

## 5. Other Recent Developments

### • Cyber Security & Emerging Political Space

Evidence suggests that the political space is gradually becoming another centre of attraction for cyber-attackers. Apart from fake news reporting involving political activities, there is also a growing connection between cyber threats and political processes such as the reported cyber-attack targeting the electronic transmission system of Ghana's Electoral Commission (EC) during the 2016 elections. This incident is believed to have compelled the EC to solely rely on the manual method of transmitting election results.

### Our electronic results transmission system was compromised – EC



Category: Lead, Politics    DECEMBER 8, 2016    2,518



Charlotte Osei – EC Boss

The Electoral Commission (EC) says it is early yet after voting for anyone to stampede it to declare results, moreover, its electronic result transmission system has been compromised.

Speaking at a press conference this afternoon, Charlotte Osei, the Chair of the EC said, "Prior to the elections we announced that we were going to use two methods of results transmission. We were going to use both the electronic and manual systems.

The electronic would have enable us to see results of all the 29,000 polling stations at the same time as recommended by the reform committee after the 2012 elections before we declare results.

Unfortunately, we had problems with the system, we have reason to believe that the system has been compromised and so we advised our returning officers at the collation centres to stop using it and revert solely to the manual."

24 hours after the polls have ended, certified results are trickling in at snail pace, not as expected by the population.

Mad. Osei stated that there were some challenges with some few constituencies.

"For instance there was an error in collation at Team East and for a while there were some outstanding polling stations results. Those issues have been resolved," she said.

In another incident, the former Inspector-General of Police (IGP), John Kudalor, raised the political temperature when he suggested a ban on social media during Ghana's 2016 elections. The IGP's remark was based on credible information relative to the dangers that social media posed to the security of the

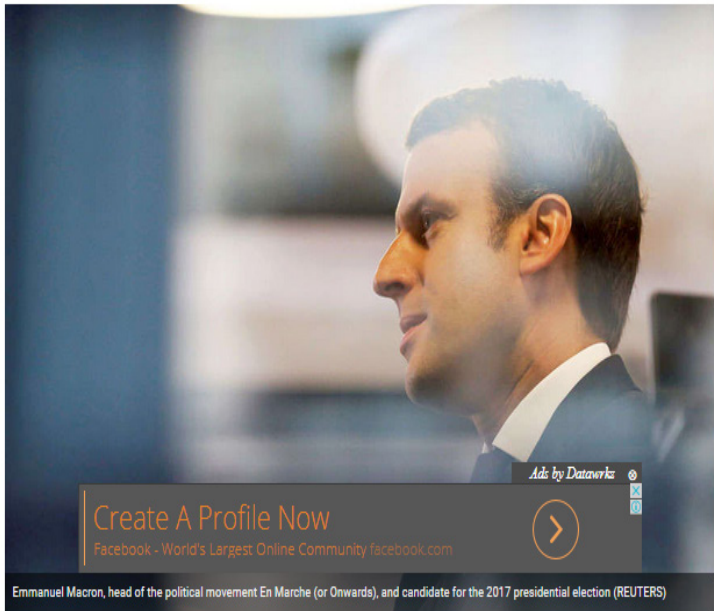


country during the election period. However, following public outcry about the suggestion, government intervened and assured the public that social media was not going to be banned.

Analysis of global incidents and trends suggest that the political space will continue to be targeted by cyber-attackers and the resilience of the electoral institutions and processes shall be tested through cyber-based attacks.

**'Massive' Cyber Attack Hits French Presidential Polls, Macron Mails Leaked**

Reuters  
Updated: May 6, 2017, 9:03 AM IST



Paris: Leading French presidential candidate Emmanuel Macron's campaign said on Friday it had been the target of a "massive" computer hack that dumped its campaign emails online 1-1/2 days before voters choose between the centrist and his far-right rival Marine Le Pen.

ive' Cyber Attack Hits French Presidential Polls, Macron M... | Philippines Launches Offensive in Hope of Recapturing Marawi... | Taliban Kill 6 Afghan Guards Working...

The United States, Russia and France have dominated global news in recent times relative to cyber-attacks targeting electoral systems.

- **Cyber Security & Social Development Issues**

The impact of cyber development in Ghana is making significant impacts on social developments in Ghana. The abusive use of social media is impacting negatively on the social dimensions of the country. Recently, video recordings showing a mob attack on a military officer were trending on social media. The videos were shared among social media users and the impact on the moral conscience of the country was significant. A statement issued by the family of the murdered officer emphasised the emotional impact of the act on the family. A statement read by a family representative said “We are not happy with the way the videos and

pictures are shared on social media. After the Manchester Arena bombing, we did not see any images and videos being circulated on YouTube, but our late son's visuals are all over social media. This has got the family crying," This showed the irresponsibility and extent to which the internet space was abused with total disregard for the psychological and emotional state of the family.

The government consequently ordered a shutdown and begun removal of internet links which circulated pictures and videos of the murdered officer through a collaborative effort between the National Communications Authority (NCA), local telecom operators, Facebook and Google. The government further issued a warning to prosecute persons involved in the continuous sharing of the videos. Other incidents involving leakage of sensitive videos and pictures of individuals on social media have been widely reported. A case in point is the sex video of a policewoman which was leaked on WhatsApp platform according to several reports on various media platforms in Ghana [10].

- **The Fight Against Illegal Mining & Cyber Attacks targeting the Media**  
Media organisations in Ghana have been under cyber-attacks in recent times. In April 2017, web portals belonging to some media houses were targeted through Distributed Denial of Service (DDoS) attack. While exact facts into the various incidents are not readily available, data from the various incidents, patterns of the attacks and timeline analyses associated with the attacks suggest a correlation between media campaigns against illegal mining and the cyber warfare targeting the media houses. This development has proven to be a threat to media organisations who operate with vulnerable IT infrastructure. Such attacks are anticipated as the media continue to report on, and engage in such national campaigns.

## How Ghana is Ranked Globally in terms of Cyber Security

### Global Cybersecurity Index and Cyberwellness Profiles

Country	Index	Global Rank
Kenya	0.412	15
Mongolia	0.412	15
Sri Lanka	0.412	15
Thailand*	0.412	15
Brunei Darussalam	0.382	16
Chile*	0.382	16
Moldova*	0.382	16
Montenegro	0.382	16
Myanmar	0.382	16
South Africa	0.382	16
Costa Rica*	0.353	17
Ecuador	0.353	17
Malta*	0.353	17
Philippines	0.353	17
Switzerland	0.353	17
Ukraine*	0.353	17
United Arab Emirates*	0.353	17
Burkina Faso	0.324	18
Mexico*	0.324	18
Peru*	0.324	18
Viet Nam*	0.324	18
Bahrain	0.294	19
Bangladesh	0.294	19
Cyprus*	0.294	19
Ghana*	0.294	19
Iran*	0.294	19
Libya	0.294	19
Panama	0.294	19



**Table 2: Africa Region Ranking by Index**

Africa	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Mauritius	0.7500	0.6667	0.6250	0.5000	0.5000	0.5882	1
Uganda	0.7500	0.5000	0.8750	0.2500	0.5000	0.5588	2
Rwanda	1.000	0.5000	0.5000	0.3750	0.5000	0.5294	3
Nigeria	0.2500	0.333	0.5000	0.5000	0.5000	0.4412	4
Cameroon	0.7500	0.5000	0.3750	0.5000	0.1250	0.4118	5
South Africa	0.2500	0.5000	0.6250	0.2500	0.2500	0.3824	6
Burkina Faso	0.0000	0.5000	0.7500	0.0000	0.2500	0.3235	7
Ghana*	0.7500	0.3333	0.2500	0.2500	0.1250	0.2941	8
Togo	0.0000	0.3333	0.3750	0.2500	0.2500	0.2647	9
Cote d'Ivoire	0.7500	0.3333	0.1250	0.1250	0.1250	0.2353	10
Liberia	0.0000	0.0000	0.2500	0.3750	0.2500	0.2059	11
Tanzania	0.5000	0.3333	0.0000	0.1250	0.2500	0.2059	11
Benin*	0.5000	0.0000	0.2500	0.1250	0.1250	0.1765	12
Botswana	0.7500	0.1667	0.2500	0.0000	0.0000	0.1765	12
Malawi	0.0000	0.0000	0.1250	0.3750	0.2500	0.1765	12
Senegal*	1.0000	0.0000	0.1250	0.0000	0.1250	0.1765	12
Zambia	0.2500	0.3333	0.1250	0.1250	0.0000	0.1471	13
Burundi	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	14
Seychelles*	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	14

*[Cyber Security Index And Cyber-wellness Profiles (Africa Index)]*

The Cyber-wellness profile by the International Telecommunications Union (ITU) is a representation of each country's level of cyber security development. The assessment is aimed at providing a clear perspective on prevailing cyber security landscape based on the five pillars of the Global Cyber Security Agenda which are legal, technical, and organisational measures, capacity building and cooperation. According to statistics by ITU issued in April 2015, Ghana is ranked 8th with an index of 0.294 (29.4%) in Africa and 19th globally based on overall assessment in the aforementioned areas.

This assessment means that Ghana's performance in terms of our cyber readiness is below average. It is, however, important to recognise the efforts that have been made in the assessment areas. Specific legislation has been made to ensure effective regulation and compliance in the cyber security environment with the enactment of the Electronic Transactions Act (Act 772). National Information Technology Agency – Computer Emergency Response Team (NITA Cert) and Cert-GH have

been set-up to implement technical measures to control cyber-threats in Ghana. Ghana, however, lacks a credible cyber security framework for the certification and accreditation of national agencies and public-sector professionals. The index also emphasises the need for a national governance roadmap for cyber security in Ghana. It is imperative to develop a national benchmark or reference to measure cyber security development in the country. To maintain standards within the cyber security domain, government needs to develop a recognised national or sector-specific research and program/project for cyber security standards, best practices and guidelines across public and private sectors of the economy.

## Current Policy and Regulatory Framework in the Fight Against Cyber Criminality in Ghana

### Current Policy, Regulatory Framework And Initiatives

- *Ghana has adopted a National Cyber Security Policy and Strategy (NCSPS)*. The Policy was approved by Cabinet in November 2016. The policy document does not only identify specific policy initiatives aimed at addressing cybercrime and cyber security issues, but it also provides a strategy to implement specific cyber security initiatives. The policy document addresses issues relative to legislative and regulatory framework, cyber security technology framework, culture of security and capacity building, research & development towards self-reliance, compliance and enforcement, child online protection, cyber security emergency readiness, and international cooperation. The national strategy identifies key stakeholders within the cyberspace ecosystem for the implementation of the various policy initiatives.
- The Ministry of Communications in 2014 inaugurated the *Ghana Computer Emergency Response Team (CERT-GH)* which was set up to coordinate national cyber security incidents. The establishment of CERT-GH is a critical component of the cyber security emergency readiness of the NCSPS.
- Apart from the NCSPS, specific legislations which address cyber security related issues have been passed by parliament. The Electronic Transactions Act – 2008 (Act 772), Data Protection Act - 2012 (Act 843), Economic & Organised Crime Act (EOCO) Act – 2010 (Act 804) and Anti-Money Laundering Act - 2008 (Act 749) are examples of available legal instruments. Act 772, for instance, identifies specific cyber offences including unauthorised access to protected information, child pornography, charlatanic advertisement, stealing and electronic forgery. The Data Protection Act requires organisations which collect personal data from customers to report data breaches to the Data Commission immediately any cyber breach occurs. The Act also requires such organisations to undertake

regular vulnerability and system audit to ensure robustness of IT systems that store, process or transmit personal data. The Data Protection Commission has recently been very proactive in its enforcement actions which has compelled many data controllers to register and comply with the requirements of the Data Protection Act.

- Recently, various training programmes targeting stakeholders operating within the criminal justice system have been organised. The programmes were mainly designed and sponsored by the Council of Europe through its Global Action on Cybercrimes Extended (GLACY+) Project. Ghana is a beneficiary of the GLACY+ project because of the country's intention to accede to the Budapest Convention.

## **Issues with Awareness And Capacity, Legislation Deficiencies And Regulatory Enforcement**

Despite the above policy framework and available legislations, cybercrime in Ghana seems to be thriving. Specific factors account for this, including the following:

**1. Cyber Security Culture** – Reports show that cyber security awareness of businesses and individuals is very low with most people unable to detect basic cyber threats. Cyber security culture has not been appreciably integrated into the ‘Ghanaian thinking’ and this reflects on low investment in cyber security technology.

**2. Limited Understanding of Cybercrimes** – understanding of cybercrimes among key stakeholders including policy makers, the judiciary and the police are very limited. The practice of relying on industry players and subject matter experts has also not been explored by state institutions.

**3. Evidence Act (Act 29) Not Responsive to Modern Crimes** – The Evidence Act (Act 29) which was passed in 1960 is the legislation which identifies specific criminal offences and punishment for these offences. The law, which was enacted before computers were manufactured, is not responsive in addressing cybercrime cases especially relative to the handling of electronic evidence. Nigeria passed a new Evidence Act in 2011 which has facilitated the use of electronic evidence in criminal prosecutions in their country.

**4. Enforcement of Existing Legislations** – Despite the existence of various legislations – including the Electronic Transactions Act – there seems to be little enforcement aimed at addressing cybercrime and cyber security challenges. For example, Section 103 of Act 772 requires telecommunication providers to store electronic activity logs of a subscriber for a period of twelve months. However, there are several instances where the operators have failed to provide such information to the police citing unavailability of such electronic records.

**5. Ill-Equipped Law Enforcement** – Cybercrimes are technology-facilitated crimes which require technical skills and technology for detection, investigations and prosecutions. Law enforcement agencies are generally not well-equipped with the skills and technology required to investigate and prosecute cyber related offences.

## Recommendations towards Tackling Cyber Security Challenges in Ghana

Based on the above assessment of Ghana's cybercrime and cyber security threat landscape, we propose the following recommendations to tackle the problem:

- **Need for Cyber Security Governance Structure**  
Ghana requires a national cyber security governance structure to effectively implement its National Cyber Security Policy and Strategy. There is the need to establish the various structures and protocols outlined in the policy document in order to effectively drive the nation's cyber security agenda.
- **Awareness Campaign towards a Culture of Cyber Security**  
To address cyber security issues, awareness campaign aimed at highlighting cyber risks is fundamental. This awareness campaign should be designed to contribute to developing a cyber-security culture among Ghanaians. All stakeholders – government, NGOs, private sector and the media should be involved in creating cyber risks awareness among Internet users.
- **Building Capacity of Law Enforcement and State Security Agencies**  
Capacity building in the form of training and technology support is fundamental to equip law enforcement agencies in tackling cybercrimes. National Cybercrime Lab should be set up at the CID Forensic Science Lab to facilitate digital forensics. Stakeholders within the Criminal Justice System – judges, prosecutors and personnel from security agencies should be trained on cybercrime investigations and prosecutions.
- **Need for National Identification System**  
Credible national identification system is essential to facilitate identification of residents even in the cyberspace. SIM Box fraud in particular is thriving partly because criminals are able to acquire fraudulent identity documents to register pre-paid SIM Cards to facilitate the fraud. The current national identification system is a mess and this has contributed to identity fraud. A single national identification card is required to enhance identification of Internet users and subscribers of electronic services.

- **Enforcement of Existing Legislations and Review of Evidence Act (Act 29)**  
An organic Computer Misuse Act or Cybercrime legislation which holistically addresses cybercrime offences and legal procedures is required going forward. However, enforcement of existing legislations is paramount to tackle the problem. There is the need for legislative review of the Evidence Act (Act 29) to ensure offences cover cyber criminality. The country's laws must be responsive to technological advances.
- **Standardisation and Development of Cyber Security Best Practices**  
The National Information Technology Agency (NITA) which is the government IT agency should engage with industry players to develop standards for IT systems, applications and processes. Cyber security best practices including user policies should be developed to guide ICT users especially in the public sector.
- **Collaboration with Stakeholders and the Involvement of the Private Sector**  
Collaboration is indispensable in tackling cybercrime. The nature of cybercrimes requires engagement with different stakeholders including law enforcement agencies, prosecutors, judiciary, Internet service providers, technology developers & service providers, cyber security and digital forensics organisations and the public at large. A multi-stakeholder group is recommended to be set up to facilitate on-going engagements and discussions on cybercrimes and cyber security issues.
- **Investment in Cyber Security**  
Cybercrimes are technology-driven crimes and therefore cyber security technology solutions are required to address cyber threats. The government, businesses and individuals are encouraged to invest in cyber security technology such as encryption, monitoring systems, anti-malware, etc. in order to protect and secure their electronic assets. Local initiatives aimed at developing cyber security technology and solutions should be encouraged, supported and patronised by government and businesses.
- **Regional/International Cooperation**  
Finally, cybercrime is a borderless crime and, therefore, international cooperation is required to facilitate investigations and prosecutions of cyber offenders. For example, cyber fraud can be perpetrated against an individual or an organisation based in Ghana by an attacker who is based in Nigeria. To successfully investigate and prosecute the case, collaboration between Ghana and Nigeria is vital. We recommend that existing ECOWAS directives on cybercrimes should be enhanced to ensure greater cooperation among member states. The Africa Union Convention on Cyber Security should be operationalised by member states to facilitate cross-border cooperation on matters relative to cybercrime. Ghana also stands to benefit from other international cooperation frameworks such as the Budapest Convention in addressing cybercrime and cyber security challenges if the country signs up to such international treaties.

## References

1. Internet World Stats

<http://www.internetworldstats.com/af/gh.htm>

2. thebftonline.com

<http://thebftonline.com/business/ict/14188/Eastern-corridor-fibre-project-goes-live-...120-communities-to-access-high-speed-broadband.html>

3. National Communications Authority (NCA)

<http://www.nca.org.gh/73/34/News.html?item=500>

4. Daily Graphic (published on April 10,2015)

<http://graphic.com.gh/news/general-news/41424-7-arrested-for-sim-box-fraud-following-nca-telcos-police-subah-collaboration.html>

5. citifmonline.com

<http://citifmonline.com/2016/06/09/ex-greda-boss-jailed-2yrs-over-sim-box-fraud/>

6. ghanaweb.com

<http://www.ghanaweb.com/GhanaHomePage/NewsArchive/ICH-cannot-fight-SIM-box-fraud-Chamber-of-Telecom-425755>

7. myjoyonline.com

<http://citifmonline.com/2015/01/21/govt-of-ghana-website-hacked/#sthash.MxO4I9km.dpbs>

8. graphic.com.gh

<http://www.graphic.com.gh/news/general-news/hackers-on-rampage-target-media-websites.html>

9. graphic.com.gh

<http://www.graphic.com.gh/news/general-news/committee-set-up-to-provide-mechanisms-for-online-child-protection.html>

10. peacefmonline.com

<http://www.peacefmonline.com/pages/local/social/201605/279821.php>



## Glossary

**Adware:** Is software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

**Bots:** A bot is self-propagating malware designed to infect a computer and connect back to a central server that can be controlled by the cybercriminal.

**Botnets:** A botnet is a number of Internet computers that have been infected with Bots to carry out a specific action by the creator (cybercriminal).

**DoS:** Short for Denial-of-Service attack, a type of attack on a network that is designed to make a network or system inaccessible to legitimate users.

**Hacking:** Is the process of gaining unauthorized access to data in a system or computer.

**Malware:** Is any computer application that is design with a malicious intention to disrupt or damage a computer system.

**Phishing:** Is the attempt to acquire sensitive information such as usernames, passwords, and credit card details often for malicious reasons, by concealing as a trustworthy entity in electronic communication such as e-mails.

**SIM Box Fraud:** Is a kind of fraud in the telecommunication industry in which a fraudster terminate international calls to make it appear as if the call is a local call.

**Dropped the yam:** Is a ghanaian description of a shift from use of analog mobile devices to use of digital mobile devices

