


Unveiling Cybercrime in a Developing Country

Richard Boateng

 <https://orcid.org/0000-0002-9995-3340>

University of Ghana Business School, Ghana

Jonathan Nii Barnor Barnor

University of Ghana Business School, Ghana

INTRODUCTION

Information and communication technology (ICT) networks, devices and services are increasingly critical for day-to-day activities (ITU, 2015). These ICTs arguably have therefore become necessary elements in our everyday lives and businesses for the past few decades (Bankole & Bankole, 2017). Despite the enormous benefits of ICTs, there exist a myriad of malicious use of these technologies which translate into financial loss to individuals, organizations and States. Unmistakably, cybercrime poses the biggest threat to the digital society (van de Weijer & Leukfeldt, 2017). Whereas the cost of cybercrime in 2015 was valued at \$3 trillion (Cybersecurity Ventures, 2017), Forbes (2017) conjecture that that figure will double to approximately \$6 trillion per year on average through 2021.

Extant literature have discussed cybercrime in various perspectives, for example, its impact (Ananthakrishnan, Li, & Smith, 2015; Riek, Abramova, & Böhme, 2017), detection and defensive measures in the fight against cybercrime (Biswas, Pal, & Mukhopadhyay, 2016; Tapanainen, 2017; Zhang, Lee, & Wang, 2016), law enforcement, strategies and prevention (Alanezi & Brooks, 2014; Ju, Cho, Lee, & Ahn, 2016; Kolini & Janczewski, 2017). Even though these studies are only a few of what exists in the respective themes, a preliminary review indicated that very few of these studies had been done with particular focus on the socioeconomic drivers behind the commission of cyber offences especially in developing economies.

According to the ITU (2012) The term “cybercrime” is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, while excluding traditional crimes that are just facilitated by using hardware. Such crimes may include hacking, bullying, identity theft, confidence romance, advanced fee fraud, among others. Riek and Böhme (2018) for instance posited that losses as a result of cybercrime are driven mainly by scams and extortion in Germany and identity thefts in the UK. Italian, Estonian, and Polish consumers on the other end, lose considerably less money to cyber-criminals, even though they spend less money and time on protection. Whereas this development is relative to the western countries, the situation is not entirely different in Africa. Cross (2018) for instance asserts that Nigeria has become synonymous with online fraud, with advance fee fraud (AFF) dominating in recent decades.

Consequently, Nigeria ranked as the leading State in the region for the conducting of malicious Internet activities (Aransiola & Asindemade, 2011; Longe & Chiemeke, 2008; Quarshie & Martin-Odoom, 2012). That notwithstanding, many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measure as well as engage private sector efforts to enhance cybersecurity (Kshetri, 2017). In East Africa for example, a task force comprising government, industry and civic groups have been set up to deal with cybersecurity at the three levels of legal, policy, and regulation. While the Economic Community of West African States (ECOWAS) have initiated policies in capacity-building, prioritising cybercrime issues and developing networks across the borders as a definite way in fighting cybercrime (Quarshie & Martin-Odoom, 2012).

Ghana, our country of focus formulated two policies; ICT for Accelerated Development Policy of 2003 and the National Telecommunications Policy of 2005 both aimed at facilitating the country's development into an information society. The sub-Saharan country also has a vision of developing its economy to a middle-income level, and thus requires the development and exploitation of ICT both as a business sector and as an enabler of other sectors (Frempong, 2012). Further, Internet penetration in the country for the past few years has been on the ascendancy. Hootsuite (2018) for instance reports that about 10.11 million representing 35% of the population are active internet users with 32% active phone internet users. With this statistics in perspective, it will arguably not be out of place to contend that as more and more people get access to data, we expect cases of cybercrime to escalate (National Communications Authority, 2017). With this backbone, this chapter seeks to answer these research questions. First, what are the motivating factors to the commission of internet crimes in developing countries and second, what are the perceptions of stakeholders in the fight against cybercrime?

This paper is in eight sections with the first giving a broad overview of cybercrime by way of introduction, review of cybercrime literature and the theoretical foundation of cybercrime. The fourth and fifth sections explain the methodology of the research and further presents the findings of cybercrime in Ghana. The final two sections include the conclusion and the summary of the findings indicating implications for research, practice and policy and pointers for future research.

LITERATURE REVIEW

There exists a significant volume of research on cybercrime and its attendant effects on countries and the social stigmatization that accompanies them. These literature cover a number of relevant themes which include but not limited to the fight against cybercrime (Cassim, 2011; Adomi & Igun, 2008; Malgwi, 2005; Jamil, 2012; Huey, Nhan & Broll, 2012), credit card fraud or financial crimes (Barker, D'Amato & Sheridan, 2008; Gottschalk, 2010; Prabowo, 2012), Advance fee fraud (Durkin & Brinkman, 2009; Dobovsek, Lamberger & Slak, 2013; Salu, 2005), Law enforcement (Davis, 2012) and Confident Romance and dating (Fair, Tully, Ekdale & Asante, 2009).

Onwuegbuzie, Leech and Collins (2013) postulate that a thorough, sophisticated literature review is the foundation and inspiration for substantial, useful research. It is therefore helpful in two ways; thus, it does not only help researchers glean the ideas of others interested in a particular research question, but it also lets them read about the results of other (similar or related) studies. The definition of the spectrum of cybercrime has also been an issue of contention especially considering the dynamics of the phenomenon (see Table 1) (ITU, 2012). Adomi and Igun (2008) defined cybercrime as *any unlawful conduct carried out with the use of computers, electronic and ancillary devices*. Cassim (2011) also contends that

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/unveiling-cybercrime-in-a-developing-country/248033

Related Content

Tech That, Bully!: Defeating Cyberbullying With Its Own Weapons

Maria Rosa Miccoli, Giulia Gargaglione, Simone Barbato, Lorenzo Di Natale, Valentina Rotelliand Valentina Silvestri (2020). *Encyclopedia of Criminal Activities and the Deep Web* (pp. 668-685).

www.irma-international.org/chapter/tech-that-bully/248076

Interpreting for Victims of Violence: Its Impact on Victims and Interpreters

Lois M. Feuerle (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 779-811).

www.irma-international.org/chapter/interpreting-for-victims-of-violence/301184

Gender-Specific Burden of the Economic Cost of Victimization: A Global Analysis

Samuel Kolawole Olowe (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 763-778).

www.irma-international.org/chapter/gender-specific-burden-of-the-economic-cost-of-victimization/301183

Psychological Violence

Maria Gabriella Cairo (2020). *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support* (pp. 42-59).

www.irma-international.org/chapter/psychological-violence/241464

"What We Need Is Bullet Control": Could Regulation of Bullets Reduce Mass Shootings?

Selina E.M. Kerr (2020). *Handbook of Research on Mass Shootings and Multiple Victim Violence* (pp. 432-446).

www.irma-international.org/chapter/what-we-need-is-bullet-control/238590