Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system

Norman Mugarura
Department of Law, Bishop Stuart University, Mbarara, Uganda and Department of Law, Kampala International University, Kampala, Uganda, and
Emma Ssali
Department of Law, Kampala International University, Kampala, Uganda

Abstract

Purpose – The purpose of this paper is to decipher the law relating to cybercrimes regulation and benchmarking best practices that could be adopted to address regulatory weaknesses in some countries. In many countries, cybercrimes regulation is undermined by a lack of robust regulatory regimes. The few regimes that are available are fragmented with no coherent global strategy to deal with these offences across countries and regions. There is a lot of scholarly literature to corroborate the fact that lack of requisite laws on cyber and financial crimes has rendered states lame ducks when faced with well-organized and resourced criminal organizations.

Design/methodology/approach – This paper articulates intricacies of regulating money laundering and cybercrimes using data from selected African countries and beyond. Generic issues on financial crimes, cybercrimes, case law and policy documents drawn from different jurisdictions have been examined based on the objectives of the study. Cybercrime activities and anti-money laundering (AML) regulatory models have been evaluated drawing on experiences of selected countries in Africa and other countries. Questions whether suspicious activity reports are appropriate as a model to counter incidences of cybercrime activities or whether other options should be considered were also examined. Most notably, the risk-based assessment model such as profiling of high-risk clients rather than reporting every transaction will be compared and possibly suggested as a suitable alternative in financial crimes regulation. The authors have evaluated the data and AML regulatory approaches and other policy measures to curtail the foregoing threats. There is a possibility that AML tools used by financial institutions and banking activities could be used to prevent the growing threat of cybercrimes. The paper has also been enriched by case studies of tenuous legal systems and fragmentation of laws on cybercrimes and financial crimes and how these gaps have been exploited to fuel incidences of illicit criminal activities around the globe. The paper has also used empirical data including visits to banks and financial institutions on the nexus between the threat of cybercrimes and money laundering prevention. The authors have been selective, evaluating cases from 2000s to date. This timeline was particularly important because of the increased incidences of computers and money laundering threats globally. After analysing the data, the authors were able to delineate that there is a close connection between the foregoing two crimes, how they operate in practice, differences and similarities in the counter-measures used to mitigate their negative effect globally. Thus, in the authors' contention, this is a novel study that is likely to spur farther research on law and policy against cyber and AML crimes not only in Uganda but also in other jurisdictions. At the same time, the findings of the study could complement, and perhaps also complete, the work of scholars who have written papers on cybercrimes to advocate for regulatory changes fight against these offences. The study will also complement the work of other researchers who have challenged the segregation of cybercrimes and financial crimes in local and international regulatory discourses. This research aims to make a significant contribution to the study of cybercrimes and how they are regulated in international law.

Findings – The findings of the paper have confirmed that the high incidences of money laundering and cybercrimes today are partly fuelled by inherent weaknesses in the global regulatory system and partly fuelled by weaknesses at an individual state level. Many countries have enacted a raft of anti-cyber and AML legislation but this notwithstanding, these laws have not been used to stem cross-border crimes globally. This

Journal of Money Laundering Control
Vol. 24 No. 1, 2021
pp. 10-28

1368-5201
DOI 10.1108/JMLC-11-2019-0092

is partly explained by the fact that many enforcement institutions lack the requisite capacity to institute measures through which to implement engendered laws and policies easily. The regulatory capacity of many countries has been eviscerated by deficiencies in infrastructure and systems.

Keywords Cybercrimes, Money laundering regulation

Paper type Research paper

1. Introduction

The paper examines anti-money laundering (AML) and cybercrimes (which involve dealing with complex social and financial processes more or less similar to AML regulation) and some of the inherent challenges to forestall them globally[1]. While cybercrime and money laundering crimes are different in many ways, their differences have recently become blurred and are not easy to disentangle. Both cyber and money laundering crimes are characterized by multiple financiers with transactions that can be located across different countries. As a result, they are complex for institutions to regulate. This also implies in effect that each bank will only be presented with a small component of a much larger problem leaving them prone to criminal exploitation.

Cybercrimes are computer-related crimes that in the parlance of financial crimes regulation are relatively new and transnational in character. Cybercrimes include information warfare, phishing, spams, denial of service attacks, hacktivism, hate crime, identity thefts, and identity fraud, online gambling, unauthorized publication of pornographic materials online, etc. Electronic and online business transactions have created opportunities and challenges for development today. In 2011, at least 2.3bn people, the equivalent of more than one-third of the world's total population, had access to the internet. Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years (Murray, 2013). By 2017, it is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population. By 2020, the number of networked devices (the "internet of things") will outnumber people by six to one, transforming current conceptions of the internet. Beyond this, however, computer-related acts for personal or financial gain or harm including computer content-related acts (all of which fall within a wider meaning of the term "cybercrime") do not lend themselves easily to legal definitions of the aggregate term[2].

This paper is significant in addressing gaps in the global regulatory systems against cybercrimes and money laundering both within countries and beyond. Very few studies have been conducted on cybercrimes and how they are regulated in many countries. This has left countries vulnerable to the high possibility of cybercriminals. The purpose of the paper is two-fold – analysis of generic issues relating to cybercrimes regulation and benchmarking best practices that could be adopted to plus regulatory weaknesses in some countries. In many countries, cybercrimes regulation is derailed by the fact that regulatory regimes are fragmented with no coherent global strategy to deal with them across different countries and regions. Some criminals and their syndicates are good researchers; they would have identified lapses in the mainstream regulatory systems and exploited them to launch their attack on the regulatory system. There is a lot of scholarly literature to corroborate the thesis that lack of requisite laws and enforcement mechanisms against cyber and financial crimes has rendered states lame ducks when faced with well-organized and resourced criminal organizations. The authors contend that regional integration of economies creates synergies to foster interstate cooperation on transnational criminal activities, which individual states would not normally be able to deal with singlehandedly.

2. Different cybercrimes typologies

There are different typologies of cybercrimes and how they are regulated often differs from individual typologies and country to country (Braithwaite, 1992). The increased incidences of cybercrimes have been fuelled by the increased electronic and online transactions that expose businesses to security breaches. Companies are under constant competitive pressures to provide faster and more convenient ways to maximize electric and online sales outlets even though some of them might not be adequately equipped to deal with the technicalities involved. In spite of increased investment opportunities by businesses, internet service providers, software providers, law enforcement agencies and individual consumers to make online transactions more secure, private individuals and public companies continue to become victims of cybercrimes. Common cybercrimes typologies include cyber-extortion, cyber-fraud and identity theft, with each carried out in a myriad of ways[3]. A well-known strategy used to carry out all three of these cybercrimes is spamming. Spam emails can be used to obtain unauthorized access to accounts and can deploy massive amounts of malware in the form of computer viruses, worms, Trojan horses and other malicious software[4]. When a criminal gains information about an individual, he/she can take over that individual's identity to commit a wide range of crimes, such as false applications for loans and credit cards, fraudulent withdrawals from bank accounts and fraudulent use of telephone calling cards. One of the strategies used by criminals is to falsely access credit cards and bank statements to gain unauthorized access into the victims' accounts in a crafty to make sure victims are not aware of what is happening until the criminal has already moved stolen assets away in another jurisdiction often using pseudo-names[5].

Spam is increasingly used to target online investors and spread false information about a company. In this way, the fraud is simultaneously perpetrated against the individual investor and the unsuspecting company. To prevent becoming a victim of spam, an investor should never rely solely on an online newsletter or bulletin board posting about an unknown company and should always check that the company files regular reports with the Securities Exchange Commission. Similarly, a company should perform regular searches to uncover the fraudulent information circulated about it by spammers[6].

The widespread threat of identity theft coupled with cyber-extortion has created a high priority on the agenda of regulatory institutions to avail resources to curtail cybercrimes. Cyber-extortion is commonly perpetrated through denial of service attacks and ransomware, which is used to encrypt the victim's data[7]. The cyber-extortionist then demands money for the decryption key. As the use of the internet has become vital to the business operations of many companies, the opportunities for cyber-extortionist have increased. Cyber-extortionists tend to operate from countries other than those of their victims and use anonymous accounts and fake email addresses. This makes cyber-extortion particularly dangerous because the probability of identification, arrest and prosecution of cybercriminals is low. There is an adage that "prevention is better than cure" and thus prevention should be the focus of regulatory agencies against cyber-extortion. From a corporate governance perspective, a company whose data has been compromised may face legal and business consequences not least for revealing confidential information about customers. Stolen information can also be used to launch attacks on other companies and individuals and damaging the reputation of the company and so forth. The first step in preventing a cyber-attack is being cognizant of the risks. In light of the evolving dangers posed by cyber-threats, businesses must respond with equal force and flexibility. As a robust counter-measure, we argue that only employees who require access to confidential information should have it, and they should first be thoroughly screened, trained and

supervised. There is a need for a strict firewall policy to be instituted to block access to former employees, not to mention ensuring the availability of extensive monitoring systems and incident response teams to deal immediately with security breaches. The good news is that there are cost-free synergies available from internet service providers, such as free security updates and malware removal tools. Companies will need to familiarize themselves with state regulations affecting their businesses and institute cyber-security, principally the Computer Misuse (2011) and AML Act in Uganda and globally.

3. Cyber and financial crimes regulatory nexus

Within the financial crimes regulatory discourse, money laundering is recognized as the biggest threat to financial institutions and the economic development of countries on a wider level. It is currently estimated at approximately 3-5 per cent of the global GDP (Gicobi, 2017). Within the banking sector, money laundering is often presented as a legitimate business or enterprise and detecting cases can require advanced sophisticated technology and technical skills[8].

However, even though they are no studies on the magnitude of cybercrimes globally, there is evidence that they are also on the increase. Cybercrimes are sophisticated to deal with by some individual countries because of their propensity to be cross-border in character[9]. This implies that to regulate them effectively, businesses will need to be well-resourced both in terms of human resources, financially and discerning to identify which core areas of concern they need to focus their resources on. More often than not, financial crime regulation is not a top priority for many boards of management. The fact that different countries operate different laws in the prevention of crimes calls for the need for harmonization to minimize regulatory disparities between countries and curtail cybercrimes money laundering and corruption[10]. There is anecdotal evidence that criminals take advantage of weaknesses in the regulatory system of states to launder illicit proceeds of crime globally. This challenge coupled with the instrumentalities of globalization has simplified the ability of criminals to move illicit proceeds of crime around the globe. Criminals have thrived in an environment of regulatory discrepancies or weaknesses between countries to gain access to new markets. The emergence of new markets-oriented economies has enabled criminals to develop the capacity to operate on a worldwide scale[11]. The large volume of legitimate capital moving into the global financial system at any one particular point, coupled with reduced regulatory controls on capital movement, has made it easy for large amount of money to enter the world financial system unnoticed [Financial Action Task Force (FATF), 1996].

4. Effect of globalization

Globalization of markets has induced a dramatic increase in the number of jurisdictions offering financial services without appropriate controls, and it has also created an environment where it might not be easy to separate “the chaff from the wheat”. With increased online transactions, criminals have been able to increase their presence globally and to take advantage of the internet for their expediency. The growing complexity of crimes and their transnational nature explains why they cannot be overcome by national law enforcement measures alone[12]. It needs to be noted that the fight against crimes underpins national sovereignty of every country – which regarded as an exclusive domain of individual states and jealously protected[13]. Lack of robust enforcement measures of regulatory regimes in some jurisdictions has fuelled incidences of cybercrimes whose members may be well-trained than fledging countries or local institutions where these crimes occur[14]. In other words, the weak regulatory environment is exploited by criminals

to easily establish into those jurisdictions where financial crimes are prevalent. The absence of a comprehensive global framework on financial crimes has created regulatory gaps that prolific criminal syndicates can easily tap into. Lack of robust anti-cybercrimes regimes in many jurisdictions especially in least developed countries (LDCs) has exposed countries to high incidence and other forms of financial crimes. This study sought to identify weaknesses in the current regulatory regimes against financial crimes and offer recommendations for regulatory changes where necessary. It will articulate inherent weaknesses in financial crimes regulation not only in the UK and the USA but also in other jurisdictions in Asia and Africa.

In many countries, there has been an uptake in global connectivity, which has come at a time of economic and demographic transformations, causing a rise in income disparities, tightened private sector spending and reduced financial liquidity[15]. Some scholars have perceived an increase in levels of cybercrimes as a result of both individuals and organized criminal groups who exploit new opportunities for profit and personal gain. More than 80 per cent of cybercrimes are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale and "cashing out" of financial information has become lucrative[16].

5. The Methodology

This paper analyses intricacies of regulating money laundering and cybercrimes from selected African countries and beyond to decipher what needs to be done to curtail them internationally. Generic issues on financial crimes, cybercrimes, case law and policy documents drawn from different jurisdictions examined based on objectives of the study. Cybercrime activities and AML regulatory models have been evaluated drawing on experiences of selected countries in Africa and other countries. Questions whether suspicious activity reports (SARs) are appropriate as a model to counter incidences of cybercrime activities, or whether other options should be considered were also examined. Most notably, the risk-based assessment model such as profiling of high-risk clients rather than reporting every transaction will be compared and possibly suggested as a suitable alternative in financial crimes regulation. We have evaluated the data and AML regulatory approaches and other policy measures to gain insights into the possibility of harnessing these similar measures to fight cybercrimes. There is a possibility that AML tools used by financial institutions and banking activities could be used to prevent the growing threat of cybercrimes.

The paper has also been enriched by case studies of tenuous legal systems and fragmentation of laws on cybercrimes and financial crimes and how these gaps have been exploited to fuel incidences of illicit criminal activities around the globe. The paper has also used empirical data including visits to banks and financial institutions on the nexus between the threat of cybercrimes and money laundering prevention. The authors have been selective, evaluating cases from 2000s to date. This timeline was particularly important because of the increased incidences of computers and money laundering threats globally. After analysing the data, we were able to delineate that there is a close connection between the foregoing two crimes, how they operate in practice, differences and similarities in the counter-measures used to mitigate their negative effect globally. Thus, in our contention, this is a novel study that is likely to spur farther research on law and policy against cyber and AML crimes not only in Uganda but also in other jurisdictions. At the same time, the findings of the study could complement, and perhaps also complete, the work of scholars who have written papers on cybercrimes to advocate for regulatory changes fight against

these offences. The study will also complement the work of other researchers who have challenged the segregation of cybercrimes and financial crimes in local and international regulatory discourses. This research aims to make a significant contribution to the study of cybercrimes and how they are regulated in international law.

6. Risk assessment model

Risk assessment discourses are essential to indicate the nature of white-collar crime and theories explain how they are regulated by financial institutions. The inherent disadvantage, however, with the risk assessment model within banks, is that many international AML regulations need vast resources of investment for banks and other financial institutions to implement. The risk assessment model was introduced to facilitate banking compliance and to reduce the costs and time spent reviewing every single client. This was to be achieved not by placing equal level risks on all clients but to differentiate between high- and low-risk clients. One of the key areas of consideration in the data collection is researcher access to the number of banking staff required. This could be restricted because of several reasons including:

- Corporate governance priorities may not view cybercrimes and AML compliance as their top concern and something they should share with other stakeholders. This attitude will need to change sooner rather than later.
- There could be a perceived sensitivity and apprehension about sharing information with other regulatory agencies and countries for some self-interests.

These potential limitations will need to be addressed including outsourcing some functions such as the enforcement of regulatory requirements of banks and other financial institutions. In addition, supporting documentation and questionnaires completed by a cross-section of subject experts will ensure that gaps in general knowledge are thoroughly addressed.

The African Union (AU) Convention has made efforts to ensure that state parties foster cooperation with stakeholders to adopt robust national cybersecurity policy strategies that internalize information infrastructure[17]. Further, it provides for the efficient strategies needed to maintain a strong mechanism for an efficient cybersecurity policy especially in areas of "legislative reform and development, sensitization and capacity-building, public–private partnerships and international cooperation"[18]. Additionally, it is paramount that critical infrastructure is protected by state parties by adopting vital mechanisms to protect sectors that are sensitive for national security, economy and communication technology systems and adapt stringent sanctions for such crimes with the aim of promoting security [19].

The Ugandan Computer Misuse Act defines cybercrime as, "an information system, program or data that supports or performs a function with respect to a national critical information infrastructure"[20]. Whereas critical infrastructure is defined as "processes, systems, facilities, technologies, networks, assets and services essentials to the health, safety, security or economic wellbeing of Ugandans and the effective functioning of Government"[21]. The majority of African countries' cyber infrastructure is underdeveloped and creates challenges for the effective regulation of these crimes. Thus, the cases reported are not accurately recorded or they are not recorded at all because of underdeveloped infrastructure. Whereas others do not realize that they are actually hacked until it's too late. In many least developed countries Africa's banking and money-laundering infrastructure has numerous flaws that permit fraudsters to transfer monies anonymously in scrambled itineraries, especially the use of electronic transfers as gears for the intake and exit of money

(Olowu, 2009). For instance, African countries suffered hectic financial misfortune in 2016 because of cyberattacks, that is, they "lost $2 billion in cyber-attacks, Kenya made loses of $171 million, Tanzania $85 million and Uganda $35 million" (Gicobi, 2017). Gicobi supplemented that "96 per cent of African organizations including banks spend less than $5,000 on cybersecurity annually"[22]. He further added that on "1 August 2016 a Nigerian man was arrested in connection with a global scam worth over $60 million"[23]. In "July 2019, Police in Ghana arrested six Nigerians believed to belong to a group stealing money from an ATM"[24]. This endangers persons because the infrastructure is underdeveloped that would be used to curtail cybercrime.

The Table I below shows sector by sector costs to regulate cybercrimes in Uganda in 2016

In our contention, lack of robust infrastructure has posed many challenges for Least Developed Countries in the fight against cybercrimes and money laundering threats"[25]. It is because of this that numerous business entities, government institutions and personal emails are hacked every day because of porous infrastructural organization thus resulting in huge costs on Africa, such as losses occasioned from business email scams totalling to a tune of $2m in 2016[26]. Additionally, Cassim added that the majority of the resources in Africa are spent on:

> [. . .] poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes such as murder, rape and theft, with the result that the fight against cybercrime is lagging behind (Cassim, 2009).

It is further appalling that little or no resources are set aside in the fight towards cybercrime. In 2015, in Kenya 20 per cent of the respondents questioned lacked a satisfactory cybercrime budget (Kigen *et al.*, 2015). While in 2016, in Kenya 6 per cent organizations allocated zero budget towards cybersecurity products, Nigeria 41 per cent, Tanzania 42 per cent and Ghana 11 per cent[27].

7. Lack of robust laws

Cybercrimes are committed through the use of computer networks, virtual in character often defying limitations of physical land laws and policies (Lewis, 2006). Therefore, the application of the law, policies usually differs from country to country (Hare, 2009). Accordingly, disparities in the cybercrime regulation in different African countries become a challenge because cybercriminals can move their activities from country to country with ease to take advantage of loopholes in the regulatory frameworks of countries (Oluwabukola, 2018). This opens up the aperture for the criminals to exploit these loopholes to hide in a country that has not adopted robust laws on cybercrimes making it hard to curb these crimes. Also, the AU Convention rather than serving as a cornerstone for the AU Member States in confining cybercrime, instead only 10 countries are signatories out of the

Table I.
A grimpse of cybercrimes sector by sector in East Africa

Institutions	Cost	Reported (%)
Banking and financial services	$206m	23
Government	$170m	19
E-commerce	$143m	16
Mobile-based transactions	$116m	13
Telecommunications	$98m	11
Cost of cybercrime to other sectors	$72m	8

55 Member States, 2 ratifications and deposits (African Union, 2018). A few of the Member States have numerous national laws instead of one major law to combat cybercrime, for example, Uganda has three laws on cybercrimes, that is, Computer Misuse Act, Electronic Signature Act and Electronic Transactions Act[28]. This is a major challenge because Africa and its regional groupings need a potent harmonized law on cybercrime that must be signed, domesticated and workable for Africa, especially with an effective legal enforcement mechanism. Similarly, it is noted that "digital evidence is fragile and transitory, and old techniques for wiretapping no longer work"[29]. In Uganda, the Electronic Signature Act, Computer Misuse Act and Electronic Transaction Act were enacted to safeguard the security of online transactions and to spur a healthy environment for the government and businesses to harness e-commerce without the fear of criminal exploitation[30]. Besides prescribing different offences-related misuse of computers, these acts also create penal sanctions to be imposed on any artificial or natural person who is caught using their computer for wrong purposes to perpetuate criminality[31].

At a wider African level, in sub-Saharan Africa, reports from victims of cybercrime are patchy that mostly come to limelight when foreigners are defrauded by cybercriminals (Boateng *et al.*, 2010). A case in point is highlighted by Ghana police service commercial crime unit of the criminal investigation department from 2006 to 2008 that include:

- Number of cases reported was 257 in 2006, 88 in 2007 and 241 in 2008[32].
- Number of cases prosecuted was 121 in 2006, 40 in 2007 and 125 in 2008[33].
- Number of cases convicted was 9 in 2006, 5 in 2007 and 27 in 2008[34].
- Number of cases acquitted was 9 in 2006 while none were acquitted in 2007 and 2008[35].
- Number of cases pending was 127 in 2006, 43 in 2007 and 89 in 2008[36].

Similarly, a survey indicates the inability of countries to arraign culprits to court because of inadequate legal framework:

- In Kenya, 71 per cent people experienced cybercrime with 3 per cent successful prosecution[37].
- In Nigeria, 37 per cent people experienced cybercrime with 7 per cent successful prosecution[38].
- In Tanzania, 20 per cent people experienced cybercrime with 1 per cent successful prosecution[39].
- In Ghana, 64 per cent people experienced cybercrime with 9 per cent successful prosecution[40].

In 2003, South Africa faced enormous challenges as a result of hackers' activities on various websites[41]. Such incidences occur purposely because of poor security, lack of potent regulations and enforcement agencies. Further, because of poor regulation of the social network sites commonly used by the African countries, Madowo dotted, that is why they are prone to fake news, for example, the 2017 presidential elections in Kenya was characterized by fake news causing disarray among the voters (Madowo, 2018). He further noted that it is why terrorist groups spread their extremist messages because of the lack of efficient regulations and regulators as compared to the USA and European countries[42]. Madowo provided two kinds of terrorists prone to the use of sites especially in Africa, "the Somalia-based militant group Al Shabaab militant that took credit of the Westgate mall attack in Nairobi in 2013 and the West Africa-focused Boko Haram"[43]. This kind of cybercrime

dubbed as cyber terrorism is a danger to the economy because peace is breached thereby affecting cross-border trade and a challenge in combatting cybercrime in Africa. To effectively curb cybercrime, a potent legal enforcement team is necessary. In Africa, there are limited resources allocated to cybersecurity because funds are spent on issues considered eminent such as poverty, AIDs and conflicts (Chetty and Goodman, 2008). A case in point in West Africa, Nigeria's institutional framework that curbs cybercrime is as follows:

> Economic and Financial Crime commission (EFCC), the National Security Adviser (NSA), Nigeria Police Force, Nigerian Communications Commission (NCC), Department of State Service (NSS), National Intelligence Agency (NIA) and Nigeria Computer Society (NCS) (Quarshie and Martin-Odoom, 2012).

Nevertheless, in 2016 Africa suffered an estimate of $2bn arising from cybercrime with Nigeria topping the list at a cost of "$550 million, Kenya $175 million, Tanzania $85 million, Ghana $50 million and Uganda $35 million"[44]. This shows that even though institutions are in place, still transnational crimes are eminent in Africa because of the limited resources given to them. Whereas in Eastern Africa in 1998, the East Africa Police Chiefs Cooperation Organization (EAPCCO) was established with its headquarters and Bureau Regional INTERPOL that serves as the secretariat in Nairobi, Kenya (EAPCCO, 2012). It has 14 Member States including Burundi, Comoros, Djibouti, Eritrea, Ethiopia, Kenya, Uganda, Tanzania, Rwanda, Seychelles, Somalia, Sudan, South Sudan and Democratic Republic of Congo (EAPCCO, 2018*)*. EAPCCO is majorly meant to curtail "transnational and organized crime" (xinhuanet, 2016*)*. Hence, during the workshop for Usalama V at Imperial Botanical Hotel in Entebbe, the current chairperson of EAPCCO Inspector General of Police Ochola condemned the rise of technology as the reason for the emergency of new kinds of refined crimes (Luwemba, 2018). Nonetheless, the increase of cybercrime in Eastern Africa is dreadful because it costs the government and private sector billions of dollars, loss of trust and disarray in the country.

The Ugandan Police said that the problems faced by institutions in curbing cybercrimes include lack of sensitization of the masses on issues of cybercrime, the fear by the victims to report the crime and the slackness in executing the Computer Misuse Act (Ocaido, 2018). According to the Serianu report of 2017, Uganda incurred costs to a tune of $42m because of cybercrime while 95.6 per cent of the occurrences were neither reported nor solved[45]. In 2017, a Rwandan company Broadband System Corporation (BSC) that provides government with video conferencing technology was hacked by anonymous that disclosed its private data to the public (Sabiiti, 2018). Further, it was surveyed by Serianu that organizations under the government in Africa 42 per cent provided a budget on cybersecurity while 45 per cent provided zero USD budget on cybersecurity (Kaimba *et al.*, 2016). Hence, to fully implement the laws on cybercrime, the government should first provide resources to the legal enforcers and train them because one of the major impediments is the lack of resources needed to enforce the cybercrime law.

In a nutshell, a society or continent without effective laws is doomed to find various hurdles along the way. Therefore, the majority of African countries' problems are stemmed from having a lot of laws on a single subject. Remarkably, though the laws exist there are limited resources that may be used to fight this vice.

8. Lack of adequate capacity on cybercrimes in Africa

In this contemporary internet era, cybersecurity is vital for all persons whether in business, politics, military, media or ordinary citizens, while Isaacson stressed that it is essential that

all person are knowledgeable and involved in cybersecurity issues (Singer and Friedman, 2014). According to a survey carried out in Kenya in 2015, the rate of ignorance of businesses and the public about cybercrimes was overwhelming as shown below:

- 21 per cent organizations were not concerned about cybercrime[46].
- 13 per cent of the organizations did not consider cybercrime a real issue[47].
- 64 per cent of the respondents had not enforced regular employee awareness and training[48].
- 20 per cent hardly review news about cybersecurity news[49].

The survey showed that developing countries such as Kenya, which may seem exemplary to LDCs in the East African Community, still have a lot to fix to curb cybercrime. Yet, it is a cumbersome crime whereby if the criminal starts their initial stage of hacking, it shall cost the organization more than it bargained for; for example, its data, trade secrets, loyalty of customer and profits. According to Macharia, a survey was conducted in 10 African countries in 2017 and it illustrated that governments "lost $204 million while banks and financial institutions lost $248 million" (Macharia, 2017) because of cybersecurity issues. He further penned that "fraud in e-commerce costs companies and individuals $173 million"[50]. Therefore, even though ignorance is bliss, it's about time Africa and Africans as a whole learn that knowledge supersedes all because ignorance is a bottleneck to curbing cybercrime.

Furthermore, even though there is a high degree of ignorance on cybercrimes, the majority of African persons rely on the internet without devising any safeguards for their electronic gadgets and hence are prone to cybercrime attacks. For instance, as of January 2018, Western Africa accounted for 147m internet users, Eastern Africa 118m, Northern Africa 116m, Southern Africa 34m and Middle Africa 20m (statista, 2018). But their awareness about the kinds of cybercrime is appalling as some get to realize that they are victims after the act has occurred or may never realize that they are victims. Thus, Boateng *et al.* (2011) adorned that cybercriminals exploit the "vulnerabilities, ignorance and gullibility on the part of users to perpetrate their heinous crimes". Therefore, although globalization is at its peak worldwide, Africa has enjoyed its fair share at a cost. Numerous African persons have been victims of this paradigm shift as a result of ignorance on how to secure their information safe from the public eye of the criminal. Atta-Asamoah wrote:

> [. . .] many internet users expose themselves to scam e-mails by responding to calls to complete forms, by circulating e-mails, or by subscribing to e-mail alerts from untrustworthy websites, purely as result of ignorance (Atta-Asamoah, 2009).

In July 2004, Muwanguzi lost her passport and $500 to a fake company arranging the visa, free transport and accommodation in Canada (Mulalira, 2018). This company disguised itself to be under "an HIV/Acquired Immune Deficiency Syndrome project of Trainer of Trainers course (TOT) by the Ministry of Health where officials were to travel to Toronto"[51]. Muwanguzi substantiated the website and supplied her details over the internet which were at par with the needed requirements[52]. However, upon the day nearing for the return of her passport and visa the criminals had vanished[53]. The summation of Muwanguzi's detriment occurs on a large scale and most victimized persons do not notice until it is quite late with no way of tracing the criminals because of the underdeveloped infrastructure as explained above. Lack of awareness and ignorance of cybercrimes by the public has acted as a deterrence in the fight against cybercrimes not only in Uganda but across Africa[54] act as a strong impediment to curbing cybercrime[55]. For

instance, in January 2005, Kasagga and two Congolese were wanted by the Kenyan Interpol for their participation in a multi-million scam[56]. This transpired as follows: the accused masterminded the "fraudulent intranet bank transfer of money between Standard Chartered Bank Nairobi (SCB) and Barclays Bank Kampala"[57]. The SCB staff "wired $5 million in three installments to separate bank accounts in Kampala"[58]. This is how the money was transferred:

- $1m was wired to Kasagga's Barclays Bank account in Kampala[59].
- It was alleged that $2m had been sent to Kalemera and intercepted at Crane Bank[60].
- During the investigations, "$3m from Kenya was detected before it was sent to a forex bureau via the DFCU Bank in Kampala"[61].

According to the South African "police and bank officials the hacker use spyware to obtain usernames and passwords, essentially engaging in identity theft in siphoning off funds from unsuspecting users"[62]. This illustrates how money is swindled and the lack of vigilance by the staff as money was transferred by them to foreign banks without the utmost precaution. Thus, this calls for the need to teach and then train the public and staff on issues of cybercrime. Many legal and natural persons are unaware of unscrupulous criminals, and their gullibility has been exploited to fuel the foregoing offences. Further, others do not know where to get redress after they have fallen victims of crimes and some are too embarrassed to accept that they have been victimized. A survey done in Kenya in 2015 showed that "73 per cent of cybercrimes victims do not report these crimes and 13 per cent do not know how to report these incidences"[63]. In addition, "19 per cent mainly concerned about their payment systems being attacked by the cybercriminals while 3 per cent were concerned of their mobile devices"[64]. Whereas Macharia wrote that "nearly 90 per cent of the crimes that hit banks went un reported"[65] in 2017.These call for redress of obliviousness among the masses because ignorance is a bottleneck towards curtailing cybercrime in Africa.

9. Limited number of experts

To prepare an efficient cybercrime-free government or private sector, it is vital that experts must be involved in the stages of preparing an impeccable firewall. Thenceforth, the AU Convention strives for transparency among the State Parties by "exchanging information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTSs)"[66]. However, according to Kigen *et al.*, in Kenya 50 per cent of the respondents questioned in the survey hardly knew what CERT is or whom to contact in case of any happening[67]. This creates a challenge in eradicating cybercrime because persons are not aware of the critical components needed in doing away with cybercrime.

During the Cloud and Security Summit of 29 March 2018 held in Kigali Rwanda, the Information and Communications Technology experts signalled on the need for expertise who can indulge in sophisticated cyberattacks because African economies are currently a major mark for such crime (Xinhuanet, 2018). While Michael Tumusiime said, because numerous persons are able to access internet in Africa, the increase in online usage is noticeable and yet few experts exist in Africa who may secure sensitive government and company data from cybercriminals[68]. African countries have become easy prey to cybercrimes largely because of the lack of enough experts to curb the crime. In a study carried out by AU in 2017, out of the 700 respondents in Africa, the governments had only

39 per cent security certificate holders, 33 per cent in the telecommunication sector, 28 per cent in other sector, banking, financial services and insurance[69]. As a result in 2017, customers suffered enormous fraud of more than $2.8m on their prepaid card services which the company then reimbursed (Signe and Signe, 2018). This fraud resulted from the cybercrime case of BGFI in Gabon the largest financial holding company[70]. Although in the ransomware case, the loss of productivity was vast to the extent of the companies paying a ransom to the attackers to attain their data[71]. In 2017, "at least 5 companies in Kenya were hit by the WannaCry virus attack that affected over 300,000 users after they had been warned by tech experts of imminent attack" (Dann Mwangi, 2017*)*. In this same year, Kenya lost about KES18bn to hackers who siphoned from or blackmailed businesses and individual[72]. Consequently, rather than entities and governments employing experts who can provide advisory opinions on how to curb cyberattacks, they either use passwords or install anti-viruses which according to experts is not enough protection (Businessdailyafrica, 2017).

Hence, the lack of enough experts per each private sector and government entity is a major challenge in curtailing cybercrime in Africa. Also, the act of waiting to get attacked and then look for experts is risky because it opens up businesses to any cyberattacks. Therefore, it is vital that resources are allocated for the purposes to use experts who can counter the cyberattacks.

10. Insider dealing effect on cybercrime regulation

Gottschalk penned that "employees of the organization commit most computer crimes, and the crime occurs inside company walls" (Gottschalk, 2010). Thus, far insiders entail employees and contractors. Such as in 2015 in Uganda:

> [. . .] nine former MTN staff were convicted of stealing 3b from mobile money platform while several MPS and individuals lost millions of shillings to hackers who duplicate SIM cards and gain access to their personal data[73].

These authors indicate that attack caused by this type of criminality was at 8 per cent in 2016 and it occasioned from online fraud and scams[74]. While insiders leak sensitive data or passwords to external parties aimed at attacking the system[75]. More often insiders "do not need a great deal of knowledge about their target computers, because their knowledge of the victim's system allows them unrestricted access to cause damage to the system or steal system data" with ease (Stovall, 2012). It implies that these insiders are the closest to the companies and organization because to gain access to information one needs to learn the workings of a particular place thus this makes insiders formidable in curtailing in curbing cybercrime (Pfleeger, 2008).

There is no doubt that insider dealing has become a major threat in curtailing cybercrime because they would be knowing where lapses in regulatory systems are and volunteer information to criminals. Most of the insiders would have been trusted with almost all the vital information they are entrusted to safeguard and this has posed threats in curbing cybercrime. Thirdly, insiders can easily save information on their devices which in the end are used to leak company secrets using malware and exposure of the data to the highest bidders or the public or criminals. This has created another layer of regulatory challenges in curtailing cybercrime because some companies at the stage of hiring do not carry robust due diligence because of time constraints creating problems to employers in the long run.

Insider dealing was identified as the growing challenge faced by businesses and organizations in many African countries to curtail threats related to financial crimes[76]. These threats have hampered efforts by the banking sector and e-commerce

businesses from growing in Africa[77]. Similarly, Musuva-Kigen *et al.* provided that a tune of $286m losses occasioned from insider threats at an estimate of $179m (50 per cent of direct costs) and $107m (20 per cent of indirect costs) per annum[78]. Whereas Dahir inscribed that in 2017 cybercrime cost Africa an estimate of $3.5bn with insider threats being the major cyberattack at $352m[79]. Therefore, it is necessary that the human resources needed for the sustainability of the company are censored at all times to ensure due diligence and as well as the other person monitored when using any company electronic products. Therefore, it is essential that businesses enact policy measures to follow-ups weekly or carry out surprise checks to test the robustness of computer security and financial systems.

Many financial crimes today are also fuelled by growing unemployment arising because of political instability, laziness, inefficient legal framework and poor planning. The World Bank recorded a high rate of unemployment in Africa in 2013 (Oppong, 2016). This figure was also confirmed by the International Labour Organisation (ILO) statistics on unemployment in Africa from 2000 to 2017. In the period 2000 to 2007, unemployment in Africa was estimated at a rate of 7.6 per cent per annum (Sow, 2017). Other scholars have opined that the high levels of poverty and unemployment coupled with the get-rich-quick attitude in many African countries (to accumulate wealth as fast as possible) has easily exposed them to criminal exploitation[80].

According to the National Bureau of Statistics, youth unemployment in Uganda is estimated at 45 per cent, whereby over 40 per cent of these are below the age of 14 years (Gbenga, 2017). In consequence, Yahoo boys merged in early 2000 (Timaya, 2018) because of the high levels of unemployment among the youth who are the majority in this group (Adeniran, 2011). Yahoo boys are responsible for cybercrime in Nigeria[81] particularly commission of online fraud dubbed as the "Nigerian 419 scam" (Maitanmi *et al.*, 2013). This group dubiously "sells fictitious goods or services and buy what they will not pay for (pay in no real value), money laundering, hacking and engaging in credit card scams"[82]. Nonetheless, what is disheartening is that this group is applauded highly in society among lecturers and friends who consider them to be geniuses (Ojedokun and Eraye, 2012). This creates a bottleneck in curbing cybercrime. Further, this group destroys the reputation of the country because it may seem to other nations that Nigerian partakes in cybercrime and is a sanctuary for such criminals instead of curtailing it[83] and sanctioning the criminals heavily. Because the conduct of Yahoo boys is greatly applauded in society, it encourages new unemployed youths to join and continue scamming people to make quick money thus making it a challenge to curb this crime:

- In London, three Nigerian internet fraudsters were arrested for running an internet scam and defrauding people of their money (dailypost, 2017).
- In 2007, the Nigerian letter fraud received in the USA, constituted 1.1 per cent and the individuals reporting fraud-type monetary loss put the letter fraud at 6.4 per cent amounting to $1,922.99m[84]. Although partakers in this group are apprehended, the damage caused on their victims is overwhelming because they cause both financial and psychological loss.

It is imperative that governments address the unemployment problem especially among the youth who can easily be recruited into the criminal underworld to easily make money. This will continue to fuel cybercrime, being recruited into terrorism ranks, money laundering, and drug trafficking and other forms of organized crimes.

11. Virtue currencies and offshoot regulatory challenges

The internet has created vast opportunities for socio-economic development in many countries but it has also regulatory challenges to financial institutions. The internet has, for instance, fuelled incidences of money laundering, tax evasion and other forms of financial crimes through the use of virtual currencies. The use of crypto-currencies as innovative financial products has raised challenges with respect to the consumer, investor protection, market integrity, tax evasion and money laundering. It uses internal measures such as checking the robustness of know your customer, SARs/ suspicious transaction reports, customer due diligence, enhanced customer due diligence and others. The irony with virtue platforms is that it is not easy to pindown specific countries in which they are regulated given that a transaction may be initiated in Uganda, involving ten other countries and effected in another set of countries. This is compounded by the fact that it might not be easy to identify the individuals involved in these transactions, which is why many countries including the UK have warned that businesses should go slow in the use of crypto-currency until robust mechanisms have been put in place to regulate it[85].

12. Conclusion

Money laundering and cybercrimes have become a challenge to many organizations and businesses and it is likely to get worse before it gets better. As we elucidated, there is still a lot of ignorance within organizations and business community about these offences, the precision with which they are planned and committed within countries and beyond. Thus, institutions will need to make sure that there is a deeper understanding of regulatory requirements and consider practical measures to achieve the following. They will need to incorporate process walk-throughs into the regular enterprise compliance-risk assessment models (e.g. facilitated workshops, regularly assess inherent risk exposures and advise business on how to deal with them). Businesses will need to implement a formal business-change-management process that flags any significant operational challenges they face. This should include, among others, developing a robust methodology for measuring risks (e.g. effective evaluation of inherent risks, money laundering counter-measures, etc.). Oversight institutions should work in tandem in developing and coordinating risk assessment and reporting methodologies to ensure that there is one set of assessments in cross-cutting topical areas. This will create consistence of compliance monitoring and testing activities, quality-control activities in operational risk of businesses in the regulated sector. Oversight institutions such as Bank of Uganda or any other central bank for that matter should define clear roles and responsibilities between risk and control functions at the individual risk banking level to ensure there are no gaps or overlaps, particularly in "grey areas" where disciplines converge (e.g. privacy risk, AML, fraud and corruption). Different regulatory agencies should develop mechanisms for jointly undertaking integrated training and communication programmes on the emerging trends of money laundering and other operational risks in the financial sector. This should include consistently involving and timely aligning senior compliance stakeholders to determine action plans, targeted training and prioritization of issues and matters requiring urgent attention. Governments will also need to establish a formal link and coordination processes between different AML/CFT oversight agencies. There is no organization or business today that can remain indifferent in the face of dynamic challenges if it is to survive the onslaught criminal attacks!

Notes

1. This paper has jointly been written by Ms Emma Ssali Namuli (LLB, LLM) and Dr Norman Mugarura (PhD). Ms Ssali has held many high-profile positions not least working as a Legal Officer with NGOs. She has also held senior academic positions as an Associate Dean at KIU and in many academic institutions in Uganda. Norman is currently employed as an Associate Professor and Dean of Faculty of Law at Bishop Stuart University in Uganda. Ms Ssali's research interest vary but largely are in human rights, computers and the law and family law, while Norman writes on international law, financial crimes, regional integration and international trade law and policy issues.
2. Murray (note 2).
3. Braithwaite (note 4)
4. Braithwaite (note 4)
5. Braithwaite (note 4)
6. Braithwaite (note 4)
7. Braithwaite (note 4)
8. Maryanne (note 10).
9. Maryanne (note 10).
10. Maryanne (note 10).
11. The recent global financial crisis (2008-2010) that started in the US subprime markets, spreading swiftly to other jurisdictions due to global interconnectedness is case in point.
12. FATF (note 15).
13. Some countries such as Bermuda, Cayman Islands, Cyprus, Malta, Mauritius and San Marino are very attractive to money launderers.
14. FATF (supra, note 15).
15. Murray (supra, note 2).
16. Murray (supra note 2).
17. African Union Convention on Cyber Security and Personal Data Protection. Date of Adoption: 27 June 2014. The AU convention objective is setting the essential rules for establishing a credible digital environment (cyberspace) and address the gaps affecting the regulation and legal recognition of electronic communications and electronic signature, as well as the absence of specific legal rules that protect consumers.
18. AU Convention (*n* 21) art 24 (2).
19. AU Convention (*n* 21) art 25 (4).
20. The Ugandan Computer Misuse Act 2011
21. The Computer Misuse (note 24).
22. Gicobi (*n* 27) accessed 27 August 2018.
23. Gicobi (*n* 27) accessed 27 August 2018.
24. Gicobi (*n* 27) accessed 27 August 2018.
25. Gicobi (*n* 27) accessed 27 August 2018.
26. Gicobi (*n* 27) accessed 27 August 2018.

27. Kigen *et al.* (*n* 33) accessed 17 August 2018.
28. Computer Misuse Act 2011, Electronic Signature Act 2011, Electronic Transactions Act 2011.
29. Lewis (*n* 36) 91.
30. Policy paper on cybercrimes in Uganda available at: www.forensicinstitute.org (accessed on 5 February 2019).
31. Ibid.
32. Boateng *et al.* (*n* 44) accessed 19 August 2018.
33. Boateng *et al.* (*n* 44) accessed 19 August 2018.
34. Boateng *et al.* (*n* 44) accessed 19 August 2018.
35. Boateng *et al.* (*n* 44) accessed 19 August 2018.
36. Boateng *et al.* (*n* 44) accessed 19 August 2018.
37. Kigen *et al.* (*n* 34) accessed 17 August 2018.
38. Kigen *et al.* (*n* 34) accessed 17 August 2018.
39. Kigen *et al.* (*n* 34) accessed 17 August 2018.
40. Kigen *et al.* (*n* 34) accessed 17 August 2018.
41. Ibid.
42. Madowo (*n* 55) accessed 19 August 2018.
43. Madowo (*n* 55) accessed 19 August 2018.
44. Kigen *et al.* (*n* 34) accessed 17 August 2018.
45. Ocaido (*n* 65) accessed 21 August 2018.
46. Kigen et al (*n* 34) accessed 20 August 2018.
47. Kigen et al (*n* 34) accessed 20 August 2018.
48. Kigen et al (*n* 34) accessed 20 August 2018.
49. Kigen et al (*n* 34) accessed August 2018.
50. Macharia (*n* 74) accessed 20 August 2018.
51. Mulalira (*n* 79) accessed 19 August 2018.
52. Mulalira (*n* 79) accessed 19 August 2018.
53. Mulalira (*n* 79) accessed 19 August 2018.
54. Mulalira (*n* 79) accessed 19 August 2018.
55. Mulalira (*n* 79) accessed 19 August 2018.
56. Mulalira (*n* 79) accessed 19 August 2018.
57. Mulalira (*n* 79) accessed 19 August 2018.
58. Mulalira (*n* 79) accessed 19 August 2018.
59. Mulalira (*n* 79) accessed 19 August 2018.
60. Mulalira (*n* 79) accessed 19 August 2018.

61. Mulalira (*n* 79) accessed 19 August 2018.
62. Herselman and Warren (*n* 46).
63. Kigen *et al.* (*n* 34) 20 August 2018.
64. Kigen *et al.* (*n* 34) 20 August 2018.
65. Macharia (*n* 79) accessed 20 August 2018.
66. AU Convention (*n* 3) art 28 (3).
67. Kigen *et al.* (*n* 34) 20 August 2018.
68. Ibid.
69. Kigen *et al.* (*n* 34) accessed 17 August 2018.
70. Signe and Signe (*n* 100) accessed 29 August 2018.
71. Signe and Signe (*n* 100) accessed 29 August 2018.
72. Mwangi (103) accessed 21 August 2018.
73. Gottschalk (note 106).
74. Gottschalk (note 106).
75. Gottschalk (note 106).
76. Gottschalk (note 106).
77. Gottschalk (note 106).
78. Kigen *et al.* (*n* 34) accessed 17 August 2018.
79. Dahir (*n* 18) accessed 17 August 2018.
80. Mwangi (supra note 103).
81. Adeniran (*n* 138) 3.
82. Mwangi (supra *n* 103).
83. Gbenga (*n* 136) accessed 22 August 2018.
84. Ibid.
85. The Times (UK Newspaper) 20th February 2019.

References

Adeniran, A.I. (2011), "'Café culture and heresy of Yahooboyism in Nigeria", in Jaishankar, K. (Ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC Press, p. 4.

African Union (2018), "African union convention on cyber security and personal data protection", available at: www.au.int>sites>files>treaties>African-union-co. . .> (accessed 17 August 2018).

Atta-Asamoah, A. (2009), "Understanding the West African cyber crime process", *African Security Review*, Vol. 18 No. 4, pp. 105-112.

Boateng, R., Olumide, L., Isabalija, R.S. and Budu, J. (2011), "Sakawa – cybercrime and criminality in Ghana", *Journal of Information Technology Impact*, Vol. 11 No. 2, pp. 85-87.

Boateng, R., Longe, O.B., Mbarika, V., Avevor, I. and Isabalija, S.R. (2010), "Cyber crime and criminality in Ghana: its forms and implications", *Americans Conference on Information Systems*, *Lima*, available at: www.pdfs.semanticscholar.org (accessed 19 August 2018).

Braithwaite, J. (1992), *Crime, Shame and Reintegration*, Cambridge University Press, Cambridge.

Businessdailyafrica (2017), "State agencies have weak security against cyber-crime: survey", available at: wwbusinessdailyafrica.com.> (accessed 21 August 2018).

Cassim, F. (2009), "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study", *Potchefstroom Electronic Law Journal*, Vol. 12 No. 4, pp. 36-65.

Chetty, M. and Goodman, S. (2008), "Cybersecurity in Africa: an assessment", available at: www.researchgate.net/publication/267971678 (accessed 21 August 2018).

dailypost (2017), "Three 'Yahoo boys' arrested in Cambodia", available at: www.dailypost.ng/2017/08/01/three-yahoo-boys-arrested-cambodia-photos/amp/ (accessed 22 August 2018).

Dann Mwangi (2017), "Kenyan firms hit by ransomware cyberattack, to get worse", available at: wwbusinessdailyafrica.com.> (accessed 21 August 2018).

EAPCCO (2012), "Small arms Survey-EAPCCO", available at: www.smallarmssurvey.org>tools>Africa> (accessed 21 August 2018).

EAPCCO (2018), "Archives – Uganda police force", available at: www.upf.go.ug>category>eapcco> (accessed 21 August 2018).

Financial Action Task Force (FATF) (1996), "Asia secretariat", Disposal of Proceeds of Crime Money Laundering Methods Workshop Report of the Expert Group in Hong Kong.

Gbenga, S. (2017), "Forget internet scams: Young Nigerians now use digital tech for good", available at: www.weforum.org>2017/04>ni. . .> (accessed 22 August 2018).

Gicobi, M. (2017), "Cyber criminals bleeding Africa's financial institutions dry", The East African, available at: www.theeastafrican.co.ke/business/Cyber-criminals-bleeding-Africa-financial-institutions-dry-/2560-3505564-24rp572/index.html (accessed 18 August 2018).

Gicobi, M. (2017), "Cyber criminals bleeding Africa's financial institutions dry", The East African, www.theeastafrican.co.ke/business/Cyber-criminals-bleeding-Africa-financial-institutions-dry-/2560-3505564-24rp572/index.html (accessed 18 August 2018).

Gottschalk, P. (2010), *Policing Cybercrime*, Bookboon.com and Ventus Publishing APS, Copenhagen, Denmark, p. 9.

Hare, F. (2009), "Borders in cyberspace: can sovereignty adapt to the challenges of cyber security", in Czosseck, C. and Geers, K. (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 93.

Kaimba, B., et al. (2016), 'Kenya Cyber Security Report 2016', Serianu Limited, Lavington, available at: www.serianu.com>downloads>Kenya. . .> (accessed 20 August 2018).

Kigen, P.M., Kisutsa, C., Muchai, C., Kimani, K., Shiyayo, B., Mwangi, M. (2015), "Kenya Cyber Security Report 2015", Serianu, Lavington, available at: www.serianu.com>downloads>KenyaCyber. . ..> (accessed 20 August 2018).

Lewis, J.A. (2006), "'Overcoming obstacles to cooperation: the council of Europe convention on cybercrime", ' in Lewis, J.A. (Ed.), *Cyber Security: Turning National Solutions into International Cooperation*, Centre for Strategic and International Studies, Washington, DC, D.C, 93.

Luwemba, J. (2018), "Technology has contributed to Cybercrime-IGP", available at: www.newvision.co.ug>te. . .> (accessed 21 August 2018).

Macharia, K. (2017), "Kenya lost Sh.21.2b through cyber security in 2017", available at: www.capitalfm.co.ke.> (accessed 20 August 2018).

Madowo, L. (2018), "How social media giants are failing African users", available at: www.weforum.org>2018/04>h. . .> (accessed 19 August 2018).

Maitanmi, O., Ogunlere, S., Ayinde, S. and Adekunle, Y. (2013), "Impact of cyber crimes on Nigerian economy", *The International Journal of Engineering and Science*, Vol. 2 No. 4, pp. 45-46.

Mulalira, F. (2018), "Uganda's legal and institutional framework in combatting cybercrime", A Critical Review of Uganda's ICT Laws New Opportunities, Old Challenges, available at: www.academia.edu>Uganda_Legal_a. . .> (accessed 19 August 2018).

Murray, G., (2013), "Comprehensive study on cyber crimes", UNODC paper.

Ocaido, M.P. (2018), "Uganda Loses Shs150bn to Cyber Criminals-New Report", available at: www.kampalapost.com (accessed 21 August 2018).

Ojedokun, U.A. and Eraye, M.C. (2012), "Socioeconomic lifestyles of the Yahoo-Boys: a study of perceptions of university students in Nigeria", *International Journal of Cyber Criminology*, Vol. 6 No. 2, pp. 1001-1003.

Olowu, D. (2009), "Cyber-Crimes and the boundaries of domestic legal responses: case for an inclusionary framework for Africa", *Journal of Information, Law and Technology*, Vol. 1available at: www.go.warwick.ac.uk/jilt/2009_1/olowu (accessed 18 August 2018).

Oluwabukola, A. (2018), "Catching up with the rest of the world: the legal framework of the cybercrime in Africa", available at: www.citeseerx.ist.psu.edu (accessed 18 August 2018).

Oppong, J.R. (2016), "Innovation, science and technology: regional networks for research and technology development in Africa", in Kobena T.H. (Ed.), *Contemporary Regional Development in Africa*, Routledge, New York, NY and London, p. 167.

Pfleeger, C.P., et al. (2008), "'Reflections on the insider threat" in Salvatore J.S. (Eds), *Insider Attack and Cyber Security: Beyond the Hacker*, Springer, New York, NY, pp. 6-7.

Quarshie, H.O. and Martin-Odoom, A. (2012), "Fighting cybercrime in Africa", *Computer Science and Engineering*, Vol. 2 No. 6, pp. 98-99.

Sabiiti, D. (2018), "How Rwanda stopped eight million cyber attackers", available at: www.ktpreass.rw>2018/01>how-rwanda-stop. . . (accessed 21 August 2018).

Signe, L. and Signe, K. (2018), "Cyber security in Africa: securing businesses with a local approach with global standards", available at: www.brookings.ed/blog/africa-in-focus.> (accessed 20 August 2018).

Singer, P.W. and Friedman, A. (2014), *Cyber Security and Cyber War: What Everyone Needs to Know*, Oxford University Press, Oxford, ii.

Sow, M. (2017), "Figures of the week: Sub-Saharan Africa's labor market in 2017", available at: www.brookings.edu>blog> (accessed 22 August 2018).

Statista (2018), "Number of worldwide internet users as of January 2018, by region (in millions)", available at: www.statista.com>statistics>num. . .> (accessed 20 August 2018).

Stovall, S.S. (2012), "The hazards among Us", in Michael J.F. (Ed.), *Principles of Emergency Management: Hazard Specific Issues and Mitigation Strategies*, CRP Press, Boca Raton, p. 123.

Timaya, A. (2018), "Top facts we should know about Yahoo boys in Nigeria", available at: www.naija.ng>1084198> (accessed 22 August 2018).

Xinhuanet (2016), "East African police chiefs seek smart ways to fight cyber crime", available at: www.xinhuanet.com>Home>Africa> (accessed 21 August 2018).

Xinhuanet (2018), "African economies most vulnerable to cyber attacks: experts", available at: www.xinhuanet.com>Home>Africa> (accessed 21 August 2018).

Further readings

Nankinga, M. (2018), "Gen Kayihura opens police chiefs summit", available at: www.upf.go.ug/gen-kayihura-opens-police-chiefs-summit/ (accessed 21 August 2018).

Corresponding author
Norman Mugarura can be contacted at: n2000mugarura@yahoo.co.uk