TALLINN UNIVERISTY OF TEHCNOLOGY
School of Business and Governance
Department of Law

Olufemi Abraham Johnson

# FIGHTING TRANSNATIONAL CYBERCRIME - PROSPECTS FOR THE APPLICATION OF EUROPEAN UNION CYBER STANDARDS TO THE AFRICAN UNION

Master's thesis
International Relations and European-Asian Studies

Supervisor: Holger Mölder, PhD

Tallinn 2020

I declare that I have compiled the paper independently
and all works, importantly standpoint and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 12112 words from the introduction to the ends of summary.

Olufemi Abraham Johnson.....
(signature, date)
Student code: 184531TASM
Student e-mail address: olufemijohnson12@yahoo.com

Supervisor: Holger Mölder, PhD:
The paper conforms to requirements in force

…….
(signature, date)

Co-supervisor: …….
The paper conforms to requirements in force
……
(signature, date)

Chairman of the Defence Commettee:
Permitted to the defence
……..
(name, signature,date)

**TABLE OF CONTENTS**

# ABSTRACT

Africa is one of the fastest growing regions on the globe in connection to incidences of cybercrime activities. The continent is also a launching ground for transnational cyber-attacks against various countries in various regions of the world. In the face of this, there is a need for certain measures to be put in place, geared towards addressing cyber threats while also improving the cybersecurity of the continent. To achieve this, the umbrella body of African countries, the African Union is saddled with the responsibility of establishing harmonized cyber norms that will be effective against the threat of cybercrime in Africa. It becomes appropriate to provide an argument for the adoption of the European Union's existing cyber norms by the African Union. The advantages of the adoption are two-fold, as it will allow the African Union to adopt a cyber-norm that is confirmed to be effective against incidences of cybercrimes, and also accord further harmonization of cyber norms and restraining cybercrimes. The conclusions and recommendations disclose that to solve the challenge of cybercrime effectively, the African Union needs to move towards a unified authority like the EU, so that there can be adequate coordination of every effort, nationally and regionally, aimed at eradicating cybercrime in Africa.



Keywords: Cybercrimes, African Union, European Union, Cyber Norms.

# INTRODUCTION

The increasing rate of cybercrimes in Africa is becoming an issue of general concern for the African Union and its constituent nations. The situation is alarming and calls for the examination of various reports that indicate that Africa plays host to four out of the top ten countries in the world with the highest prevalence of cybercrimes in the world. These countries are Nigeria, South Africa, Ghana, and Cameroon in no order (Fripp 2014). The emergence of information and communication technology (ICT) has resulted in Africa's significant leap from its perceived status as a backward continent. Various African countries are moving their data safekeeping from whiteboards to keyboards. The jumps recorded with the introduction of ICT have benefitted both the government and citizens in similar fashion. However, this giant leap has come with its accompanying problems, some of which are cyber bullying, online theft, and infiltration into national security data, data hacking and cybercrimes. It is important to note that for the purposes of this study is fighting against cybercrimes by using European Union Cyber Norms. For the purpose of this topic, European Union Cyber Norms was considered because it serves as model in creating European Union.

The fight against cybercrime has led to various stakeholders in the African continent coming together to fashion out ways to manage this phenomenon. Such stakeholders include the private citizens, business organizations that intend to deal with their contemporaries through the internet as well as government agencies who feel the need to tackle this unwholesome act. While various African governments have tried their best to lay down cybersecurity strategies to counter this issue, the perpetrators continue to explore new ways to engage in crimes.

Recently, the menace of cyber-crime is emerging as one of the paramount security challenges that are affecting African countries as a body. The growing incidences of cyber-crimes originating from Africa are becoming more frequent by the day, thus making it quite impossible for the global community to deal with Africans efficiently through the internet conveniently. For example, this unfortunate scenario of cybercrime spreading costs to the South Africa an estimated 5 billion Rand yearly (Fripp 2014).

As various countries continue to expand their respective digital coverage, improving the level of Internet connectivity for citizens and businesses, there is bound to be a corresponding increase in the rate of cyber activities. Some of these activities may be illegitimate, with some bordering on fraud and ultimately crime. Most of the time, cybercrimes in Africa are caused by the financial benefits that the culprits can acquire from engaging in them. As African countries continue to establish their cyberspace for civilians to enjoy, it is often exploited for illegitimate means.

With this increased cyber activity, there is a tendency for a potential security dilemma, in which a country could misinterpret the actions of another one. In addition, the risk attributed to cyber access cannot be overemphasized; from petty frauds to high-level cyber-arms race; it would be naïve for any country not to develop sound cybersecurity for its cyberspace. To embark on cybersecurity trends, it becomes essential for nations to evaluate the existing cybersecurity norms to assess the unique attributes of such norms. This would provide a framework for the development of Cybersecurity norms that will discourage cybercrimes while also limiting the incidences of cyber-attacks and cybercrimes in the continental cyberspace.

The objectives of this study is to discuss both the African Union’s and the European Union’s cyber norms and subsequently highlight the core discrepancies in both of the continent’s cyber norms, since there are certain speculations that the adoption of the European Union's methods of cyber norms could accord the African Union an efficient model that will safeguard and combat cybercrimes. Based on the objectives of this research as discussed above, the following research questions are designed to fulfil the objectives of this study: 1) what are the major shortages of the African Union’s normative regulation compared to European Union’s cyber acts; and 2) what are the main benefits the African Union might receive from the adoption of European Union’s cyber norms?

Therefore, this paper is based on desk research that analyses the challenges of cybersecurity among the AU member countries. The methodology adopted for this research follows the exploratory model, which is aimed at investigating and proffering solutions to a problem. The exploratory model has discussed extensively the cyber norms available in the European Union. This paper studies how effective it had been in the provision of cybersecurity for various

European countries. Qualitative data will be collected and discussed in detail in order to have informed knowledge of the prospective advantages of the adoption of European Union cyber norms for tackling cybercrime in Africa. The data analysed in the study are secondary, and they include articles, white papers and other relevant documents that support the argument. It details the various European Union cyber regulations, with a view to understanding how such norms can be effective if adopted by the African Union.

As an argumentative study, the methodology used for this paper, followed of the Toulmin Model, which identifies six major interdependent components of an argument. The Toulmin model is used to analyse texts in order to embark on supportive arguments. It was developed to help research students understand the process of evaluating claims made by others. It involves six steps, which include:

1) maintaining a position on an issue (claim);
2) providing evidence and information that validates the position maintained on the issue (grounds);
3) explaining how the evidence supports the position maintained (warrant);
4) giving more information to support the explanation on the evidence (backing);
5) brief introduction of one exception to the claim (counterclaim);
6) the argument against the counterclaim (rebuttal).

The researcher employed the Toulmin model to provide a valid argument on the reasons it is suggested for the African Union to adopt European Union cyber norms. While there may be in existence specific cyber norms being adopted by the African Union, there are verifiable articles that point to the inherent ineffectiveness of such cyber norms. As supportive arguments, the positive impact of European Union cyber norms in the South East Asian countries (ASEAN) was discussed. It is based on this discussion that the potential impact of the EU cyber norms on the African Union will be analysed. The Toulmin model is a reminder of the fact that argumentative researches are embarked upon in the form of qualifiers and rebuttals, as opposed to absolute assertions. It does not avoid the evaluation of a counterclaim if there is any. Rather, it includes the counter position in the discussion and further responds to it in the context of the maintained position.

This research is divided into three chapters apart from the introduction, which offers information about the reasons that necessitated the conduct of the research, the research questions in addition to these, the purpose of the research was started, without leaving out the study's methodology. Chapter one, on the other hand, contains the study's theoretical framework and a detailed discussion of relevant literatures that define cyber norms, cyber-crimes, various classifications of cybercrimes and other related concepts. Chapter two contains the empirical data and the analyses of these pieces of data, while chapter three discusses this research's data presentation and analysis. A conclusion of the study presents summary, findings and recommendations.

# 1. THEORETICAL FRAMEWORK: CYBER NORMS AND CULTURE

## 1.1. Cyber Norms Defined

Norms represent a standard of appropriate behaviour for a predefined set of individuals or groups sharing a given identity (Finnemore 1996, 325). This definition indicates that norms can differ with respect to scope, legitimacy, as well as in social characteristics and ethics. The definition above thus suggests that cyber norms are a set of standards designed to improve the security of cyberspace through the preservation of the utility of the globally connected society. They determine the level of acceptable and unacceptable cyber behaviours with the objective of limiting risks to encourage greater predictability while also limiting the potentials for criminal and problematic usage of cyberspace.

The first attempt to introduce cybersecurity norms was in 2003 when the United Nations General Assembly adopted Resolution 57/239, which noted that all operators and owners of internet technologies be made aware of relevant risks within the cyberspace and the expected roles every party should play (Finnemore, 1996 326). The resolution mandated member nations as well as other international organizations to establish a culture of cybersecurity in their respective enclaves.

## 1.2. Cybercrime Defined

The major problem with the literature on cybercrime is the absence of a unified definition that encapsulates the totality of what constitutes cybercrime. It is generally described as the criminal use of computer technology to perpetrate illegalities. The Council of Europe (2001) defines cybercrime as “an action intended against the integrity and availability of computer systems, networks, and data as well as the misuse of such systems and data”. Cybercrime is defined as “any conduct or action deemed unlawful, involving the use of a computer system or network irrespective of whether such a system or network is legal and legitimate” (Papadopoulos 2012, 336). Furthermore, the U.K National Cybersecurity strategy (2016), divided cybercrime into two distinct categories; cyber-enabled crimes and cyber-dependent crimes. This categorization points

to the fact that cybercrimes may either be aided through the cyberspace or may be perpetrated through the exploitation of the cyberspace.

The European Commission defined cybercrime as “criminal acts committed through the Internet with the use of electronic communication networks and information devices” (The European Commission 2017). This definition was further explained as criminal activities that may be traditional but are further aided and enabled by the exploitation of the internet. United Nations’ definition of cybercrime has two ingredients; an illegal behaviour channelled by means of electronic devices targeted at the security of computer systems and the subsequent processing of data gotten from such illegitimate means. By magnifying this definition, it is apt to say that cybercrime includes any unacceptable behaviour embarked upon through the use of a computer system or network aimed at accessing, possessing, and/or distributing information.

## 1.3. Classification of Cybercrime

Just as the definition eludes a unified perception, the classification of cybercrime is also perceived in diverse ways. However, the classification of cybercrime comes in two distinct forms: computer-focused and computer-assisted (Gordon & Ford 2006).

### 1.3.1. Computer-focused cybercrime

Cybercrimes under this class are dependent on installing and modifying malicious software into computer systems to facilitate the intended fraud or theft by granting the perpetrators unauthorized entry into the systems. The malware is most times designed; they are technological by nature because they involve the use of computer-related as well as computer-enabled technology for successful execution. Malware is programmed to engage in unauthorized online transactions through the personal details of the identities of unsuspecting victims (Nyamanga 2010). There are some inherent attributes of a computer-focused cybercrime, examples of such includes the following:

1) it is always a one-off activity;
2) it is made possible through the installation of malware;
3) the malware is introduced in the form of harmless yet discreet process

Some of the known examples of cybercrimes that fall under this category are phishing, virus installations, as well as manipulation of data through hacking. The forms of cybercrimes that fall under this category as those that are perpetrated as a direct result of computer technology.

### 1.3.2. Computer-assisted Cybercrimes

Computer-assisted crimes are not directed at computer systems but just used as a means of facilitating crimes against human beings. Such cybercrime while being made possible using technology is not directly aimed at technological devices, rather they are dependent on the exploitation of humans, in the hope that such humans make momentary errors and play into the perpetrator's hand. This form of cybercrime is always committed without necessarily infiltrating into computer systems. Rather, the perpetrators make use of legitimate and familiar computer programs to lure their victims. Many computer-assisted cybercrimes are perpetrated through acts of cyber stalking, cyber predation, cyber bullying, cyber harassment, and a host of others. It should also be noted that computer-assisted cybercrimes have an underlying precedent that indicates existence before the advent of computers. The fact is that such crimes are executed much easily with the existence and coming of computer systems.

A clear-cut attempt to distinguish between the two forms of cybercrime is not always so easy. This is because it is not all the cybercrimes that will easily be categorized under any of the two forms, as some cybercrimes may be a hybrid of the two forms (Gordon & Ford, 2006). Just as it is applicable in other continents, Cybercrime is an umbrella terminology of a wide range of illegal and illegitimate cyber activities engaged in electronically for various motives and can be divided into various smaller categories such as content-related activities, copyright and trademark infringements, computer-related, intrusive activities or a hybrid resulting from the combination of any of the aforementioned. It is as a result of the varying typologies and forms that make it a difficult task to effectively fight back against it or provide commensurate security against its occurrence. As noted by Symantec Corporation, there are quite several contributory factors that pull cybercriminals to specific regions around the globe. This includes broadband connections as well as unsecured internet connectivity (Castells 2001, 39). Cybercrimes, in general, have an endless list of possible manners of perpetration. However, with respect to Africa, the most common types of cybercrimes are card skimming and identity theft. These are briefly discussed below:

Card skimming is an illegal attempt to copy, capture, or retrieve the personal details from the magnetic stripe of transaction cards. Both the debit and credit cards offered by banking institutions do have a magnetic stripe wherein personal details of users are stored. Cybercriminals often capture unsuspecting individuals' cards, as well as the PIN details, which are subsequently encoded into a counterfeit or fake card, to be used fraudulently for transactions. While this form of cybercrime looks much like identity theft, it is limited to card use, unlike identity theft that is used in a variety of means that go beyond card usage.

The process of skimming cards is made possible through the uses of compromised POS terminals as certain bank(s). Not only that, some ATM is also manipulated for such process such as card skimming. This process of card skimming involves the perpetrator attaching false casing and PIN overlay devices on genuine ATMs. Sometimes, a skimming device is attached to the card reader, which records the PIN by sending the details through a concealed camera to a dedicated system. This has been used in African countries for quite some time now. The apex banking institution in Nigeria, CBN, recently proclaimed that the banking sector lost more than 20 billion Nigerian naira (over $57 million) to various card skimming acts, thereby hindering the promotion of a cashless economy (Essien 2018, 19). This problem is not peculiar to only one country among member States in the A.U, but it is happening in the African continent. For example, between 2013 and 2015, the continent experienced more than a 100% increase in card skimming activities (Essien 2018, 19).

The perpetrators of advanced cyber frauds in African consist of popular and respected individuals in various African countries who engage in business email compromise schemes as well as tax return frauds using malware and some other enabling software from the various underground fraud markets. These sets of individuals do operate in a consortium while maintaining very tight connections as well as maintaining overseas bank accounts to masquerade their illegitimate activities and hide from the watchful eyes of the security agencies. The cybercrimes committed by these individuals often result in the global search for them due to the magnitude of monies involved in such cybercrimes. The sophistication with which such cyber frauds are committed often leads to Interpol manhunt for the perpetrators (Longs et al., 2009). A recent example was a certain social media celebrity called Ismailia Mustapha, also known as,

Mompha who was arrested in Nigeria with his Lebanese cohorts with respect to internet-related fraud

While the above typologies do not outline whole range of cybercrime being perpetrated in Africa, they are perceived as the most prominent in terms of frequency of occurrence. The techniques used for some of these cyber frauds include email phishing, email bombing, card interception, as well as unauthorized access to computer systems and networks. Advanced level cyber frauds and card skimming remain the ubiquitous forms of cybercrimes perpetrated in Africa. While the incidence of card skimming and identity theft are targeted at individuals, advanced level cyber frauds are not limited to individuals only, but also include large corporations as well as countries sometimes. For instance, banks are among the major targets of cybercriminals that intend to embark on corporate cyber fraud.

## 1.4. Categorization of Cybercrimes

Based on the object of legal protection, some methods employed while committing the cybercrime, the 2001 Convention on Cybercrime stipulated four criteria for the classification of cybercrimes (Nyamanga 2010). These substantive classifications include the following:

1) computer-related crime;
2) content- related crime;
3) copyright infringements and crimes relating to confidentiality;
4) integrity of computer systems and data.

It is also important to note that the classification of cybercrimes as discussed above is also in mountain bike with the classification of cybercrimes that is adopted in the East Africa's draft of the East African Community (EAC) legal framework for cyber laws (Gumbi 2018). This legal framework adopted by the EAC is also the same with Article 29 of the African Union's Convention on Cybersecurity and Personal Data Protection, which clearly mentions four categories of cybercrime. These categories of cybercrimes are:

### 1.4.1. Person-targeted

This category of cybercrimes may be either assisted or enabled by computers, but the target of the attack is on an identifiable individual. Examples of such cybercrime include cyber defamation, cyber bullying, as well as cyber assault (Tamarkin, 2014, 37-38).

### 1.4.2. Property-targeted

This classification of cybercrimes includes cyber-attacks and crimes directed towards property that belongs to an individual and entails different levels of violation or tampering with an individual's property (Tamarkin, 2014, 37-38). These cybercrimes are capable of adversely affecting an economy and usually range from cyber-vandalism to cyber-squatting via computer related fraud.

### 1.4.3. Organization-targeted

Under this category of cybercrimes, the perpetrators indicate a desire to get critical or valuable information, either military or otherwise, of either a country or a private organization. Cybercrimes perpetrated against organizations are major to get classified information and are often indulged in illegally by competitors of private organizations or foes of a specific government. Examples include cyber-warfare, cyber espionage, and industrial espionage.

### 1.4.4. Society-targeted

The last category of cybercrimes is those perpetrated through cyberspace with the intention to cause harm to the society at large, which, if successful, often results in untold hardships. The main essence of society targeted cybercrime is to disrupt the balance of society by demoralizing the citizens with such attacks. Some examples of society-targeted cybercrimes include cyber terrorism as well as illegal auctions.

## 1.5. Theoretical Framework

Based on the exploitative tendencies of cybercrimes, the Routine Activity Theory (RAT) is adopted for this research. This theory emphasizes and highlights the environmental and societal "opportunities for crime". It explains that, when a potential criminal opportunity surfaces, the act occurs at a particular point in time and space between a motivated offender and an equally qualified target for victimization. This occurrence of crime occurs within an environment or space that is devoid of capable guardian to protect such target, which is deemed to either be a vulnerable individual or the person unguarded property.

Therefore, the unavailability of a part of these three situational factors, which are; an enabling environment to conduct crimes due to lack of a law; a qualified target for victimization; and a motivated offender, makes the carrying out of any crime theoretically impossible (Collins, Sainato & Khey 2011). This suggests that the Routine Activity Theory is seen as a macro-level theory that can be applied to many forms of crimes, because it predominantly attempts to shed more understanding to the process of criminal victimization and not merely the offender's particular motivations for engaging in crime (Akers & Sellers 2009 in Collins, Sainato & Khey 2011).

The theory discourses that crimes take place in instances where motivated offenders have the opportunity of coming into contact with targets that are considered to be qualified, in an environment or space that lacks a form of guardian, in terms of a law that is capable of curbing the offenders from carrying out crimes. This theory stipulates that differences in crime rates are explainable by the availability of qualified targets and the capable laws that are able to regulate or prevent the conduct of crimes on the targets (Ngo & Paternoster 2011).

There was a systematic theoretical reflection of this theory's ability to shed light on the patterns of cybercrime (Yar 2005). The theory began by firstly considering every of the three major elements of the theory that constitute the schema of any criminal situation, namely; motivated offenders, suitable targets, and the lack of a capable guardians, testing them in respect of their applicability in the digital environment or space. In terms of motivated offenders, it was discovered that there was ample existence of this in the digital space (Yar 2005). These motivated offenders include fraudsters, hackers, pirates, stalkers, cyber bullies and many others. In the same vein, there were also many available targets that were suitable for victimization. These include proprietary data, individual information, digital payment and purchasing services, computer systems that could be objects of compromise or disruption by unauthorized intrusion. Lastly, capable guardians could take different forms, such as network administrators, forum moderators, users, and peers or even laws that regulate digital or cybercrimes.

This theory's relevance to this study is that it breaks down into very succinct units, the various factors that lead into the carrying out of crimes and also explains the three units that are required for the conduct of crimes. In relation to the conduct of cybercrimes, this theory explains the rationale behind the conduct of cybercrimes, which are the availability of motivated offenders, such as fraudsters, hackers, pirates, stalkers, and cyber bullies, as well as the existence of suitable targets, such as proprietary data, individual information, digital payment, purchasing services, and computer systems, all of whom are victims of the African cyberspace that permits enormous conduct of cybercrime due to the unavailability of sufficient capable guardians. Capable guardians, such as network administrators, forum moderators, users, and peers or even laws to regulate the rate of the occurrence of cybercrime within member nations of the African Union.

## 1.6. Review of empirical literature

Cybercrime is a relatively new mode of criminal engagement in the global community. It is a phenomenon that has experienced a dramatic rise worldwide for some time now, and Africa is not immune to it. Cyber criminals are always on the lookout for enabling the environment and fertile regions in order to perpetuate their nefarious activities. These enabling environments are often regions with a relatively high level of technological vulnerability. For instance, African is positioned as the leading destination of mobile money transfers, with its e-commerce expected to rise to $75 billion by 2025 (Atta-Asamoah 2010, 105-114). Such a situation creates an appeal for potential cybercriminals to exploit as they are bound to prey on users' carefree attitude to engage in the cybercrimes. Another potential pull for cybercriminals into Africa is based on the fact that a larger portion of mobile phone users is still hooked to the Android OS platform, which is known to be a long way from being secured like its counterpart IOS.

According to several studies, (Ryle 2002; Schwab 2016 and Glance 2017), computer and ICT related crimes have been on the increase towards the end of the twentieth century. This trend, it is believed, would continue for the foreseeable future with a tendency to plunge the global community into conflict (Ojedokun 2005, 11-18). The challenges posed by cybercrimes have continued to rise as a result of the technological exposure of African that is accompanied by increased vulnerabilities and risks. The volume of cybercrime threat is so massive, with 286 million virus samples counted on a yearly basis (Olasenbaum 2005). These statistics present a

very dangerous scenario that can lead to cyber hackers invading strategic infrastructures like airport control towers, weather, and traffic signals to in-flight pilots. The emergence of computers and the Internet, which brought about the incidence of cybercrimes, have caught the African continent unawares. Reports have suggested that there are close to 400 million Internet users in Africa alone (Cassim 2012).

However, most of these users have their respective communication devices exposed to threats of various kinds, from viruses to malicious software (Kritzinger & Von Solms 2012, 37-51). It is also believed that Africa is also perceived in the global world as a permissive environment for the perpetration of cybercrimes, a situation that is aided by the lack of adequate Cybersecurity capabilities and measures (Sabillon 2016). Other issues that result in the high prevalence of cybercrimes in Africa can be attributed to the absence of requisite legislation across countries to prosecute the perpetrators of these crimes effectively. Throughout the nooks and crannies of Africa, cyber-crimes are perpetuated in business-like manners, with some of the perpetrators being professionals in the ICT world. This is because of the fact that there exist no blueprints or regulation that is in place to prosecute those who exploit its use for illegitimate motives (Kithi 2012). The pre-existing regulations that dealt with computers could only be applied to crimes that involve computer theft, computer sabotage, and other physical forms of criminal engagements; they do not expressly tackle the incidence of information theft and hacking. It has been affirmed that the spate of internet abuse has been on the increase in Africa as a result of the absence of national and transnational regulations to tackle occurrence (Kithi 2012).

This position can be said to be very true if we are to look at countries like Kenya that is experiencing increased cybercrime with no clear-cut laws to deal with the cybercrimes. Even in countries with existing laws, such as is applicable in member nations of the European Union, it has been observed that such laws had become inadequate; as such, laws do not clearly highlight predefined manners to prosecute cybercriminals. The cyber laws in South Africa as of 2006 were not equipped to handle cyber-related crimes in the country effectively (Makhanya 2010). This is because the criminal law in place at this time was the 1977 Criminal Procedure Act, which had little or nothing to do with the internet at the time of its designing and ratification.

The South African criminal law procedure never took into consideration thefts and abuse of data, which is the foundation upon which cybercrime is perpetrated. Kenya did pass its own Communication Act to address illegitimate acts, but the law never envisioned the spate of cybercrimes when it was being drafted. It did little to address the specifics of cybercrimes, culminating in its amendment twice before 2009 to meet with the demands of the time (Wanjiku 2009, 15-16). The first amendment incorporated criminalizing unauthorized access and interception of computer data as well as access to the internet for the aim of committing offences. It went on to stipulate a definite jail term for anyone caught.

The second amendment, within the same year, elaborated on what constitutes cybercrime and punishment for offenders. From that time up till now, there is yet to be any amendment, while the dynamics of cybercrime have shifted. The activities of cybercriminals make it quite a difficult task for legitimate businesses to benefit from the use of cyberspace for businesses because some dangers of cybercrimes had been ascribed to cyber activities in the region (Wanjiku 2009, 15-16). The generality of legitimate business professionals in Africa has lost a whole lot of opportunities to the fact that their respective regions have been tagged as cybercrime haven, thereby discouraging prospective clients from engaging these legitimate business owners.

As has been observed, many African countries have been awakened to the reality of cybercrimes, and its sharp increase in occurrence in the last two decades. This renaissance is thus acting as a fuel for the continent's search for a lasting solution to the hydra-headed phenomenon. Governments in Africa are beginning to understand the need for cross-continent law, legislation, and reforms that not only deal with specific crimes but also incorporate cybercrimes as well (Kioni 2008). Nigeria, the most populous African country, has been in the spotlight of the global community for its high involvement in cybercrimes around the globe. It is ranked as the number one African country with the highest prevalence of cybercrimes (Boateng 2010, 4). Although Nigeria had established the Economic and Financial Crime Commission (EFCC) as far back as 2003 through Presidential decree, the main jurisdiction of the agency was for the prosecution of all economic and financial crime that includes money laundering, drug trafficking, and advanced fee fraud while it was not established to investigate incidences of cybercrime, the agency is known to partner other law enforcement agencies in the war against cybercrimes in the country.

Cybercrime poses a serious challenge to Africa in its resolve to exploit the advantages that the digital age has to offer while also managing the associated risks. A particularly intriguing thing about cybercrime is the manner in which they are carried out. Cybercrimes are not limited by air, sea, or land jurisdiction, making it possible for the perpetrators to remain anonymous, ubiquitous, and very dangerous. There was particular incident that happened in 2012 when the terrorist organization, Boko Haram reportedly hacked into the personnel records of the Directorate of State Security (DSS), thereby compromising the safety of various personnel (Essien 2015 55-66). The insurgency group alleged that the hack was necessitated to get back at the Nigerian government with the manner it was handling the insurgency, especially the non-release of members detained by the government. This occurrence is further proof that African nations are hugely vulnerable to cyber-attacks.

Cyber-security culture has been a subject of intense evaluation for quite some time now (Burt et al 2014). The concept of cybersecurity norms follows two distinct forms (Burt et al., 2014):

1) norms relating to the improvement of defences to reduce risk through the provision of foundations for national cybersecurity capability as well as cross-national structures and processes that improve better understanding among countries;
2) norms relating to the limitation of offensive activities that serve as means of resolving conflicts, avoidance of conflict escalations, and also managing the catastrophic impact.

Within the highlighted norms, progress often requires dialogues and collaborations amongst various governments, not leaving behind the input of the other stakeholders such as the private sector, the academia and the civil societies.

## 1.7. Perpetrators of Cybercrimes

The term hacker has existed since the 1960s, and was formerly used to refer to well-meaning, disciplined and respected software and hardware experts. However, recently, the word “hacker is now used as a negative name to refer to a skillful computer savvy individual that illicitly or illegally interferes and accesses databases or computers without the appropriate permission (Gumbi 2018).

Hacking can also be defined as an unauthorized access to computers. This suggests that the hacker gains access into a computer network, without possessing the required authority to do so (Gordon 2017). In South African law for instance, hacking and other related computer-enabled criminal activities carried out to acquire unauthorized access to a computer, network, or data, are clearly prohibited and banned by Articles 86 and 87 of the ECT Act (Gumbi 2018). Till date, there exists no generally accepted definition for the term 'hackers' and the definitions that are adopted and used in most instances are inconsistent. However, with the knowledge of the major elements of hacking, some of which include the innovative employment of technology, the intention to exploit systems vulnerabilities and weaknesses, and programming, the description of hacking below is recommended. An activity which encompasses computer programming, circumventing security systems designed to protect computer networks and digital data stores, designing, and executing solutions to solve problems by combining software and hardware in unconventional ways, and modifying and re-purposing digital products of all kinds (Madarie 2017).

# 2. EUROPEAN UNION AND ITS DISPOSITION TO CYBERSECURITY PARTNERSHIPS

The European Union has constantly indicated its positive stance on partnering with the global community in achieving effective cybersecurity across the globe. Much of this is evident in its foreign policy documents, which are contained in the 2013 Cybersecurity Strategy as well as the 2015 Council of Europe conclusion on cyber diplomacy. The motive for the European Union's cybersecurity partnership is not only for bilateral cooperation but also for strengthening the multilateral fabric of global internet governance. Advocating for uniformity of norms relating to cybersecurity is not new to the European Union. The Council of Europe has always been at the forefront in the area of negotiating and interacting with regional and continental organizations with the objective of implementing uniform norms in the fight against cybercrime (Segal 2016, 7-8). These international relations have broadened its cope, resulting in various partnerships between allies and like-minded countries such as Japan and China.

The EU's cyber partnership agenda was as a result of the organization being the first continental organization to implement effective cyber norms that indicate uniformity across a continent. This is not the first time that the EU would be taking the lead in establishing blueprints for other continental organizations to follow suit. To get a better understanding of the purpose of the EU's agenda on strategic cyber partnerships Smith, Keukeleire, and Vanhoonacker (2016, 1-8) identified three levels of purposes; structural, reflexive, and positional.

The structural level explains how the EU makes use of bilateral cyber partnerships to promote a more effective multilateral system, as stated in the 2008 revision of the ESS by the Council of Europe, which was labelled 'partnership for effective multilateralism.′ The global multilateral setting is hindered by a series of problems relating to legitimacy and effectiveness. This is also true of the global fight against cybercrime. As Acharya (2014, 12-13) noted, most countries exploit multilateralism selectively. And, given the EU’s objective of a strong global response to cybercrime, bilateral engagements with other continental organizations can be perceived as an instrument to strengthen the multilateral fabric (Renard 2016, 18-35).

On the reflexive level, the successes of Cybersecurity norms in the EU member countries have positioned the EU as a regional cyber power with a cyber-security blueprint that reflects total cooperation among member nations. Although, there are various cyber powers (such as the U.S, China, Russia), who can individually shape or effective establishes Cybersecurity strategies that can be adopted. However, it should be noted that there are also cyber powers within the EU (UK, France, and Germany), who also can develop effective Cybersecurity measures but choose to go one step further by adopting a uniform Cybersecurity norm with their respective European neighbours to improve continental Cybersecurity effectiveness. The establishment of the NIS Directive (Network and Information Security Systems) has strengthened the EU member states' cyber resilience through the capacity building effort put in place by the European Network and Information Security Agency (ENISA). The cyber power of the E.U is not global, the cohesion and resulting effectiveness of uniform cyber norms in the continent will accord it a soft power with respect to global cybersecurity (Nye 2011, 23-31).

At the relational level, cyber partnerships can be seen as a means of cementing relationships with various international organizations on cyber issues with a view to solving the problems of cybercrime globally. Since it is not possible for the AU to solve this problem on its own, there is a need for cooperation on the base of mutual benefits and interests. These partnerships are meant to tackle strategic issues, and they go beyond just diplomatic and economic ties. More salient, it is for the fact that the relationship level focuses on concrete outcomes rather than mere socialization processes.

The contents of Article 28 of the AU Cybersecurity Convention established the provision for international cooperation on Cybersecurity. Among the details here is that AU countries are expected to evaluate existing models of Cybersecurity with the objective of developing international cooperation for the promotion of Cybersecurity on a global level (Orji 2015, 108). With the trusted EU Cybersecurity cyber norms, the AU will be equipped to deal with cybercrime on a global perspective.

## 2.1 The European Union Cyber-security Acts adopted

Since the commencement and adoption of the EU Cybersecurity Strategy in 2013, the European commission has ramped up its efforts to further protect European online. In the course of the adoption of this strategy, the commission has adopted a set of proposals, especially in relation to network and information security, budgeting over 600 million Euros of the EU investment specifically for research and innovation in cybersecurity projects within 2014 to 2020 (European Cybersecurity Initiative, 2017). This development has facilitated cooperation within the E.U and with other partners across the world.

The European Union also solidified its approach within the last couple of years through the inclusion of Cybersecurity into the center of its political priorities. Therefore, trust and security has become the core of the Digital Single Market Strategy presented in May 2015, while the battle against cybercrime is a part of the three pillars of the EU's Agenda on Security that was adopted in April 2015. Similarly, in July of 2016, delivering on the strategies, the EU presented more measures aimed at boosting the Cybersecurity industry and tackling cyber-threats. Thus, the adoption of the Directive on Security of Network and Information Systems (NIS Directive) by the European Parliament in July of 2016 represents yet another significant milestone towards attaining a more secured digital space (European Cybersecurity Initiative 2017). The subsequent paragraphs present some of the strategies that the EU adopted in order to strengthen its cybersecurity.

### 2.1.1. E.U Cybersecurity Strategy (2013)

As contained in European Cybersecurity Initiative, (2017), the European Union in conjunction with the European External Action Service adopted the E.U Cybersecurity Strategy in 2013. The strategy stipulated the principles that guide the Union's action within this domain. For instance, there is much significance of access to Internet and of the safeguarding of fundamental rights online. It made provision for these five priorities:

1) increasing cyber resilience;
2) immensely decreasing cybercrime;
3) developing EU's cyber defense policy and abilities in connection to the Common Security and Defense Policy;
4) developing the industrial and technological resources for cybersecurity ;

5) creating a coherent international cyberspace policy for the E.U and promoting important.

### 2.1.2 European Agenda on Security (2015)

According to European Cybersecurity Initiative, (2017), tackling cybercrime very effectively was a part of the three priorities as contained in the new European Agenda on Security 2015-2020 that became adopted by the Commission in 2015. As revealed in the (Factsheet on cybersecurity , (2017), The European Agenda on Security stipulated the actions below:

- focusing increased attention to the implementation of existing policies on cybersecurity , attacks on information systems, and battling child sexual exploitation;
- the review and potential extension of legislation on battling fraud and counterfeiting of non-cash payment mechanisms in order to recognize newer types of crime and counterfeiting of monetary instruments;
- the review of hindrances to criminal investigations of cybercrime, especially issues about adequate jurisdiction and rules about access to evidence or information;
- the enhancement of cyber capacity creation action within external assistance instruments.

### 2.1.3. Digital Single Market Strategy (2015)

Trust and security are cogent features required for receiving the benefits of the digital economy. This is the rationale behind the Digital Single Market Strategy that was presented in 2015 and comprises a public-private partnership on Cybersecurity. This partnership was adopted and signed on the 5 of July 2016 by the EU and the European Cybersecurity Organization (ECSO), which is an industry-led association, which is made up of different stakeholders, namely large companies, SMEs, start-up firms, research centers, universities, end-users, operators, association and public authorities. The aim of this partnership is the stimulation of European's competitiveness and helping in the achieving success against cyber insecurity, while simultaneously preventing market fragmentation via innovation, maintaining trust among member nations and industrial actors, and also aiding the alignment of demand and supply sectors for products and solutions that are cybersecurity-oriented (European Cybersecurity Initiative 2017).

The partnership has been helpful and instrumental to the structuring and coordination of digital security of industrial resources within Europe. This partnership also entails many actors that range from innovative SMEs, manufacturers of components and equipment, essential infrastructure personnel and research agencies. The partnership takes advantage of the EU's, national, regional and private efforts and resources that also involves research, innovation and finance, all directed towards increasing investments in cybersecurity. This Digital Single Market Strategy partnership essentially helps to:

- pool industrial and public resources, so as to deliver innovation to achieve a consensually agreed research and innovation plan;
- place emphasis on selected technical priorities jointly selected with industry;
- maximize the effectiveness of available financial resources;
- create increased visibility to European research and innovative perfection in cybersecurity .

This partnership is aided by EU funds emanating from the Horizon 2020 Research and Innovation Framework Program (H2020), which possesses a total investment of about €450 million and lasts till 2020.

## 2.2. ASEAN countries' Adoption of E.U Cyber Norm and how it relates to the African Union case

For one, it can be affirmed that Southeast Asia as sub-continent has benefitted immensely from the adoption of the EU cyber norms through the development of Confidence Building Measures (CBMs) by the Organization for Security Cooperation in Europe (OSCE), (Access Partnership 2017). The adoption of EU cyber norms by countries in Southeast Asia came at a time when the region was experiencing serious cybersecurity threats brought as a result of rapid technology adoption (Access Partnership 2017). The regional collaboration with the EU has helped to build a cyber-resilience, as well as a shared understanding and mutual trust. The African Union is also in the same situation that the South-East found itself before the adoption of European Union cyber norms. For the African Union to achieve success in its cybersecurity, there is a need for an effective blueprint such as the European Union cyber norms that have been put into use in other regions like South East Asia.

The initial work in the adoption of E.U cyber norms began in 2017 through series of bilateral interactions between the E.U and the member states of the Association of Southeast Asian Nations (ASEAN), rapid progress has been made to ensure that the region takes its place in the global community as a technological cyber power bloc. It should be noted at this juncture that the major reason of discussing the adoption of European Union cyber norms by ASEAN nations is to ascertain the rebuttal as highlighted by the Toulmin model, which is needed to ascertain another valid perspective for the argument. The major step achieved in 2017 was the adoption of the ASEAN Declaration to Prevent and Combat Cybercrime at the 31st ASEAN Summit in the Philippines. This document was the first of such a formal declaration that focuses on issues of cybercrime in ASEAN countries. Amongst the measures adopted by the summit include:

1) the harmonization of laws relating to cybercrime;
2) exploring any feasible measures to fuse the existing regional norms with that of the E.U in the fight against cybercrime;
3) the establishment of nation-wide plans aimed at addressing cybercrimes;
4) strengthening of international cooperation as well as collaboration amongst member nations and other relevant agencies such as EUROPOL and ASEANPOL to enhance security in cyberspace while also preventing cyber-related attacks (Access Partnership 2017).

The declaration also addressed the review and monitoring of the subsequent implementation as well as looking at providing assistance to each other in the area of training and research. Furthermore, the declaration also puts emphasis on the development of ASEAN capabilities and enhancement in combating cybercrime through a close working relationship with the INTERPOL Global Complex for Innovation (IGCI).

However, it should be noted that in comparison with the ASEAN countries, the cybersecurity regulatory framework adopted by the African Union still lags behind. A major reason for this is the fact that public awareness of cyber risks and cybercrime is lower in relation to the ASEAN countries who have witnessed an improvement since the adoption of European Union cyber norms. This lack of awareness has served to influence the approach and pace of reaction to the proposed adoption of European Union cyber norms. African countries, too, are presently faced with increased cybersecurity threats through various acts of cybercrime, and there is a need for a continental effort to introduce uniform cyber norms that would provide uniform solutions to the threat of cybercrime.

# 3. EFFORTS AGAINST CYBERCRIMES IN AFRICA

## 3.1. African Union fighting against cybercrimes

The African Union did not begin the enforcement of concrete regulatory initiatives in cybersecurity until after 2008 (Schjolberg, 2008). An important variable could have prevented the development of a regional cybersecurity initiative in the Au is traceable to the slow penetration of ICT in Africa before the widespread availability of wireless technologies in the first ten years of the 21st century. One of the AU's initial statements on the requirement for the promotion of cybersecurity is contained in AU's Draft Report on a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation (2008). This report highlighted the need for the creation of a unified regional policy and regulatory framework for cybersecurity (Ibid). Therefore, by November 2009, the AU Ministers that headed the Communication and Information Technologies convened an Extraordinary Session in South Africa where they decided and adopted several called the Oliver Tambo Declaration (AU 2009). This declaration required the AU to:

> *Jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection (AU 2009).*

In the same vein, in 2011, the attempts of the A.U resulted into the establishment of the Draft Convention for the creation of an authoritative Legal Framework for Cybersecurity in Africa (AU 2011). This Draft Convention was intended to unify the laws of African States in connection to electronic commerce, data protection, cybersecurity governance and cybercrime control. Subsequently, in 2012, the AU Expert Group on Cybersecurity that constituted of experts from member nations and Regional Economic Communities in Eastern, Southern and Northern Africa gathered in Addis Ababa, Ethiopia, to deliberate the Draft Convention (ECA 2012). This Draft Convention was later adopted in 2012, by the AU Expert Group on Cybersecurity (UNECA 2012).

In the same vein, the Convention called the AU Convention on Cyber Security and Personal Data Protection (AU Convention 2014) essentially attempts to:

1) harmonize the laws of African nations in electronic commerce;
2) data protection;
3) cybersecurity;
4) governance and cybercrime control.

This Convention also clarified the goals for the information society in Africa and attempts to empower already available ICT laws in member countries and the Regional Economic Communities (RECs). In connection to cybersecurity governance and cybercrime regulation, the Convention stipulates that:

> *"The current state of cybercrime constitutes a real threat to the security of computer networks and the development of the information society in Africa"*

This status quo therefore demanded the following;

> *"Defining broad guidelines of the strategy for the repression of cybercrime in Member States of the AU, taking into account their existing commitments at the sub-regional, regional and international levels".*

Therefore, according to Sharpe (2009), the Convention adopted a *"technology neutral"* language to create substantive and process driven criminal law provisions that tackled cybersecurity governance and cybercrime regulation in AU Member States.

## 3.2. Efforts of East African Community in fighting against cybercrime

In the past decade, East African Community countries, such as Burundi, Kenya, Rwanda, South Sudan, Tanzania and Uganda have scaled up their respective efforts in combating incidences of cybercrimes. This has been made possible through an approach that includes various stakeholders such as the government, the civil societies as well as other economic industries. In the East African region, there has been a cyber-security management task force led by Kenya that coordinates various activities that are channelled at bringing c=incidences of cybercrime to the barest minimum among the five countries that make up the region. The cybersecurity

management taskforce plans to set up a Computer Emergency Response Team (CERT) to fight cybercrime aggressively across the five countries.

While envisaging that the CERT may not effectively handle this mission, it was agreed by the five countries that the International Telecommunications Union's assistance should be sought (Gashumba 2012). It was also agreed that the five countries should set up a collaborative framework that will strengthen the CERT at country and regional and international levels. Since each country had its own set of internet laws, there was a need for the member countries to establish uniform laws across the five countries with very minor differences.

The fight against cybercrime in the East African region follows a similar model that is being promoted by the International Cybersecurity Norms which include:

1) the need for bilateral consultations on issues relating to cyberspace;
2) the adoption of uniform national cyber laws;
3) the establishment of a cooperative body to regulate the activities of the cyberspace of the member nations that make up the body;
4) enhancing cooperation with other international bodies in the fight against cybercrime.

The adoption of harmonized cyber norms in East Africa has been made possible as a result of the numbers of the country involved; five countries. It was quite easy to agree to common modalities in the fight against cybercrime, unlike other regions with a greater number of member nations.

## 3.2 The Effort of ECOWAS against Cybercrime

West Africa remains the most populous region in sub-Saharan Africa. It also is home to the highest number of countries; sixteen countries formed the Economic Community of West African States (ECOWAS). The first West African summit that relates to the issues of cybercrime was convened towards the end of 2011 in the Federal Capital Territory of Nigeria, Abuja. This summit was organized by the Nigerian government under the aegis of the Economic and Financial Crime Commission (EFCC) and supported by the United Nations on Drugs and Crime (UNODC), as well as Microsoft. The summit titled 'Fight Against Crime: Towards Innovation and Sustenance of Economic Development,' with participants cutting across the global community. The aim was to evaluate cybersecurity strategies that would strengthen international cooperation as well as improve regional coordination in the areas of tackling cybercrime, while also fostering economic growth (ECUNNI 2011).

The summit was attended by more than 500 people with countries such as France, the USA, Turkey as well as UAE sending representatives, while security agencies such as the INTERPOL, US FBI, Council of Europe (COE), and the European Union (EU) sending observers.
The major core of the discussion during the summit included the following:

1) positioning the fight against cybercrime in the region as a regional priority that would result in economic development for member nations;
2) strengthening mutual trusts through the establishment of effective security partnership among member nations of ECOWAS;
3) getting input from other stakeholders such as civil societies, academics, industry experts as well as the international organizations;
4) showcasing best practices and evaluating case studies of existing cybersecurity strategies that are deemed effective in the fight against cybercrime (www.waccs.net 2011).

The reasons for such deliberations are not far-fetched; West Africa is home to one of the most notorious forms of cybercrime, which is in the form of advance fee fraud, and credit card scams. The region is also a hotbed for perpetrators of various fraudulent schemes such as counterfeit inheritance scams, romance scams, fake lotteries, fake investment opportunities, and a fake promise of a fortune in return for advanced payments. In Nigeria, which has the reputation of having the highest perpetrators of such scams, the government, while trying its best to fight cybercrime through various security agencies, does not have the requisite legislation to embark on such fight efficiently. This necessitated the country's National Assembly to be persuaded by the World Bank to pass the Cyber Crime Bill, which was aimed at reducing the rate of internet fraud emanating from the country since it is a known fact that cybercrime is having damaging effects on the reputation of the country.

In response to this persuasion, the Nigerian government established the Nigerian Cybercrime Working Group (NCWG) as an autonomous body within the office of the National Security Adviser. Nigeria also inaugurated the Computer Crime Protection Unit (CCPU) under the office of the Attorney General of the Federation in order to curb incidences of cybercrime. The office is charged with the responsibility of establishing working paper for relevant laws aimed at protecting against computer crime in the country, which would subsequently be passed by the

National Assembly. Ghana, the second-largest economy in West Africa, also passed the electronic Transactions, Bill, in 2012 in order to protect the privacy rights of internet Users as well as websites from unethical hacking (Ghana News Agency 2012).

The establishment of the Economic and Financial Crimes Commission (EFCC) in Nigeria was a bold step towards the fight against cybercrime. There are specialized units within the commission that are focused on tackling the incidence of cybercrimes. Amongst these is the general and asset unit, training unit as well as prosecution unit. In order to fast track cybercrime investigations, the EFCC launched an operation codenamed 'Eagle Claw' which was aimed at tracing fraudulent emails through special software (Oates 2009). This was followed up with public education of the ills of cybercrime and how it affects the profile of the country globally.

From the foregoing, it is perfect for asserting that there have been various moves by African nations to tackle the growing incidences of cybercrime in the region. From East Africa's cooperative acts to West Africa nations' disposition to regional alliances to tackle cybercrime, it is safe to assume some parts of the continent are trying its best to come up with ways and means of minimizing cybercrime. However, there is an absence of a truly joint effort to tackle cybercrime on a continent-wide basis.

It is not enough for cybersecurity norms to be put in place; the important thing is for such norms to be effective in the fight against cybercrime. Despite the regional efforts aimed at fighting cybercrime in Africa, the complexity of cybercrime continues to affect the continent as a whole. The absence of uniformity in the strategies put in place serves as a hindrance to the effectiveness of the cyber strategies. It was based on the ineffectiveness of the national and regional strategies against cybercrime that necessitated an African Union Convention on Cyber Security and Personal Data (AccessNow 2016).

In the communiqué titled *"Room for Improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa,"* Ephraim (2018) noted that the various national cybercrime legislation existing in Africa are vague and involved semantics which often come to be interpreted as regulations to criminalize the works of journalists, whistle-blowers as well as digital security researchers. For instance, Article 10 of the Ethiopian Computer Crime Proclamation of 2016 is focused on computer-related fraud, but some clauses contained therein can be detrimental to journalists due to its vagueness. The clause 'distributing misleading

computer data, concealing facts that should be revealed' is a vague language that has the potential to be misused in the course of prosecution by state authorities. Such semantics can be used to pressure journalists to reveal sources that should ordinarily not be disclosed.

In addition to this, Section 4 of the South African Cybercrime and Cybersecurity Bill of 2015 stipulate it as an offence for any individual to unlawfully and intentionally access in whole, or in part, any data from a computer system or network, critical government database, or any information from the National Critical Information Infrastructure (Ephraim, 2018). Within this regulation, 'access' is taken to mean making Use of, viewing, communicating with, or other actions as deemed so. However, it fails to elucidate on whether access to such systems exceeds a person's lawful authority.

With respect to data retention, Section 32(2) of the Kenya cyberspace regulation offers no clause regarding the maximum data retention period. This is not as good as every effective cyber law should have provisions for mandatory data retention. Not having this stated in cyber law regulations is very dangerous because data can remain stored forever, leading to data breaches and the creation of extra burden on those responsible for preserving the data, although the law not making provisions for that would favour the absence of data. It should also be noted that the contents of cyberspace regulations in Kenya and Ethiopia have some clauses that could be interpreted to mean the government is allowed to hack into private computer systems. As affirmed by AccessNow (2016), the draft of such regulations is vague and do not have any judicial oversight, with the language of the regulation further empowering law enforcement agencies to permanently withhold devices even after the completion of cybercrime investigations. It is common knowledge that government hacking interferes greatly with the fundamental human rights of citizens, while also serving as a threat to their respective personal properties.

The contents of the various cybercrime laws in East Africa lack adequate USer notification and transparency. Although, Section 29 the Kenyan Computer and Cybercrime Bill of 2016, made some provisions for appeal mechanisms for aggrieved individuals with respect to cyber offences, other countries that make up the East African region are yet to have such provisions put in place. This has handicapped the collective effort of a united fight against cybercrime. In some countries like Nigeria in West Africa, security agencies are not required by any law to apply for a court arrest warrant before embarking on the investigation of cybercrimes. In the course of bypassing

the judiciary, security agencies are prone to gross misuse of power in cybercrime cases. There are enough reported cases of innocent individuals in Nigeria being summarily killed by security agents for resisting arrest or not providing devices such as phones for cross-checking by trigger happy policemen.

The Nigerian government, through the EFCC, recognized the fact that the fight against cybercrime cannot be won by one country alone within a region, and subsequently resorted to partnering other countries within and outside the West African region in order to explore collective and viable ways of combating this monster called cybercrime. Among the organizations penned down to include the United Nations, the European Union, INTERPOL, as well as Microsoft and Google. It was believed that the establishment of a central regulatory body would come up with cybercrime laws that would adequately regulate cyberspace.

In the past, the European Union, in a bid to see African nations continue the fight against cybercrime, committed funds to the tune of thirty-two million dollars to drive the fight against cybercrime in West Africa to a reasonable level. Not stopping there, the region also signed an accord with the INTERPOL for the establishment of a sub-regional bureau in Central Africa to assist in the cyberwar. As INTERPOL reported in 2009, there have been great efforts by African countries such as Nigeria and Cameroon, whose respective governments have improved efforts to fight trans-border crimes. It should also be noted that Mukinda (2009) affirmed that while countries like Kenya and Nigeria had revamped their Cyber Crime units to be more trained in specialized cybercrime investigations in the USA, collective and uniformity remains a key to effectively tackling crimes in the cyberspace.

In 2009, the African Union extra-ordinary conference involving various ministers in charge of national communications and information technology departments discussed the need for the continent in conjunction with other global bodies; develop a legal framework that would address issues relating to cybersecurity, electronic transactions and data security (African Union Draft Convention, 2009). By 2011, the African Union presented a Draft Convention on the need for a legal framework for cybersecurity in Africa. This represents the warrant which implicitly stated the assumption that links the claims to the grounds according to the Toulmin Model. The motive behind this was to improve on the existing national legislation of member states with respect to cybersecurity and data protection. The draft document contained four parts, which include:

1) part one: to electronic commerce, treaty obligations in electronic form, security and electronic transactions, and contractual responsibility of member nations in no definite order;
2) part two: issues relating to data protection;
3) part three: strategies to fight cybercrime;
4) part four: issues relating to cyber racism, xenophobia in ICT, minor and child pornography.

Worthy of note is the fact that part three of the draft convention related to issues that go beyond national strategies to fight cybercrime, but a continental strategy that would foster cooperation among member nations in cybersecurity. This is comparable to the framework of the Council of Europe Convention on Cybercrime of 2001. However, a noticeable flaw which made it not effective was contained in Article 21, which state that:

> *" each member nation shall adopt such measure as such nation deem necessary to foster information exchange and the prompt sharing of expeditious and reciprocal data by member states' organizations as well as other similar organizations around the globe with the responsibility to cause the law to be applied in the territory on the bilateral or multilateral basis."*

as well as Article 25 which state that:

> *"Every Member nation shall adopt any such measure, as well as strategy as such nation deem necessary to take part in regional and international cooperation in the area cybersecurity."*

These two resolutions are focused on promoting participation among member nations with respect to cooperation with international bodies such as the United Nations and the European Union with respect to the establishment of frameworks for cybersecurity. Bearing this in mind, it is glaring that the African Union as a body felt the need for a continent-wide strategy to tackle cybercrime. The reason for this is not far-fetched; individual nations have already adopted measures to tackle cybercrime. Also, various regions have tried to make an impact within their respective regions in the establishment of cyber norms to tackle the incidence of cybercrime. However, there is a need for a uniform approach that would cut across all regions of the African continent.

There have been developments in the past by the African Union to develop an imported framework on cybersecurity. This was contained in the AU-UNECA Convention which was subsequently adopted in 2012. However, there were oppositions to its adoption in 2014 as civil organizations and the academic world frowned at its adoption; following concerns of the potential harm such draft had on privacy and freedom of expression (Orji 2015, 105).

There have been great efforts by African nations as well as regional blocs to adopt cyber norms that would effectively tackle cybercrime in Africa. However, unlike the European Union cyber norms, there is an absence of uniformity in the cyber norms adopted by the African Union. The adoption of cyber norms in Africa is still embarked upon on a regional level as there is yet a consensus of a continent-wide model that will limit the incidences of cybercrime. Bearing in mind that there are some countries existing in different regions, and who share borders, the possibility of experiencing a clash of cyber norms. For instance, while Nigeria exists under ECOWAS, it's neighbour to the east, Cameroon is aligned with the central African region, a region that is prone to wars and crisis. With no uniform cyber norms available, it becomes difficult for coordination between Nigeria and Cameroun. This is still a hindrance to the overall objective of uniform continent-wide cyber norm adoption; hence there is a need for collective measures to tackle cybercrime in the continent.

# SUMMARY

The main crux of this investigation is aimed at establishing uniform norms across Africa in the fight against cybercrime. In the East African sub-region, which is classified under the East African Community (EAC), there has been partial establishment of cross-country norms among the five East African nations to fight cybercrime – these countries are; Burundi, Kenya, Rwanda, South Sudan, Tanzania and Uganda. The Computer Emergency Response Team (CERT), in conjunction with the ITU and EACO, has ensured collaboration among nations to fight cybercrime collectively. However, the absence of sound legislation has limited the effectiveness of the measures put in place.

In the West African region, the ECOWAS, while being an effective organization, has not been able to initiate policies that would result in capacity building among member nations with respect to cybersecurity. This has led to an increase in the sophistication and frequency of cybercrime in the region. Cybercrime has continued to pose a serious threat to national security as government establishments, and private businesses are not immune to its reach. As a result of the absence of clearly defined legislation in various African sub-regions, cybercrime continues to thrive, and many nations are yet to grasp its destructive tendencies fully. The way forward is for Africa to learn from the EU by adopting the latter's cyber norms in the fight against cybercrime. The cyber norms to be adopted have to be a tested blueprint that has been adopted outside of the region where it was initially developed. This is important so as to affirm that such cyber norms have the capability to be effective outside the region where it was developed.

Therefore, given the magnitude and nature of cybercrime in Africa, there is a need for a concerted effort in tackling the phenomenon through the effective coordination and implementation of policies. For this to be possible, the major issues surrounding effective implementation need to be highlighted. The interactions between the various stakeholders will reinforce the need for a carefully laid out uniform cyber security strategy that would provide crime-free African cyberspace. In order to successfully tackle the growing rate of cybercrime in Africa, the following recommendations have been developed:

1) as existing in the EU, there is a need to develop a unified platform that would focus on addressing cybercrime in Africa since it has been factored that cybercrime operates not within the scope of borders, hence it is difficult for one nation to engage in a standalone strategy to fight it. As a continent, there is a need for African countries to collaborate,

cooperate, and coordinate themselves in order to deal effectively with cyber threats at the national and continental levels. This would lead to the establishment of agencies that would be tasked with monitoring and reporting cybercrimes across the continent. This recommendation is in tandem with the AU Convention, (2014), which determined that the African Union already needs to adopt cybersecurity strategies that are harmonized across Africa in order to be able to tackle
cyber insecurity and victimization within member nations of the African Union;

2) the role of various stakeholders such as the various national governments, African civil societies, industries, and security agencies is important in setting up a policy and regulatory framework that would improve the potential success of any adopted E.U cyber norm. This assertion agrees with Sharpe (2009), who claims that African societies are in dire need of establishing a policy or regulatory mechanism that can improve cybersecurity in their different domains. This should be done with the support and involvement of the various African political leaderships. While the existence of regional frameworks like the one in East Africa can be applauded, there should be deliberate attempts to establish strategies and policies that would unify the various regional and national cyber security policies to fit a common objective;

3) there is a need for coordination between African countries and the E.U for the establishment of cyber security partnerships as a means of fostering cooperation between the two continents in the fight against cybercrime. This would allow for the transfer of technical expertise and personnel training for African countries in the fight against cybercrime. This would also create jobs as personnel would be needed to fill up the various agencies set up across Africa to tackle the incidence of cybercrime. Since Africa is in need of strong information and computer technology institutions to train personnel in the area of cyber security, coordination with the E.U should be a top priority;

4) lastly, there should be a concerted effort among African countries to make available funds that would be dedicated to specialized and professional management in order to financially support cyber security innovations as may be deemed necessary.

In conclusion, cybercrime remains a serious threat to African nations as well as the rest of the world. It cannot be totally avoided, but by putting in place adequate measures through the establishment of norms, effective cyber resilience can be built. In order to build this, it is important to adopt strategies and norms that have proven to be effective around the world.
Over the years, the European Union has put in a great effort in establishing a set of cyber norms that are geared towards tackling cybercrime in the region. The impressive cybersecurity policies that have been produced by various E.U institutions, aimed at regulating activities on cyberspace have brought relative ease to cyber activities. The E.U has been able to employ a nascent strategy that has brought together a fragmented understanding of the need for reliable continent-wide cyber legislation aimed at ensuring intelligence exchange among member nations, to deal with cyber-attacks.

As part of its role in fighting against the increasing occurrence of cybercrime around the globe, the E.U has become more vigilant of global cyber threats since 2017. Prior to this time, commercial and governmental agencies across the globe had been subjected to threats of malware and high-risk cyber activities. While some of regional organizations were able to establish national policies to counter the growing cases of cybercrime, had become hotbeds for the perpetration of cybercrime. Since physical borders do not limit cybercrime, the increasing frequency of cybercrime in these countries has a spill over effect on other countries within the region.

This led to the promotion of sound cybersecurity infrastructural model for the regional organizations like the African union to inculcate so as to overcome limitations in the fight against cybercrime. The major development of this is to evaluate the possible establishment of an E.U-AU partnership to adopt standard E.U cyber norms for cybersecurity in the region. Just as the E.U cybersecurity boasts of cyber powers such as the UK, Germany, and France, the AU countries also take pride in countries like South Africa possessing one of the best national cybersecurity agencies in the globe with respect to efficiency, standards, and measures put in place to fight cybercrime. The only recognizable limiting factor to the AU-EU collaborative cyber efforts has to do with the lack of adequate funding needed to equip and train the AU security forces. Therefore, for the African Union to be able to tackle the growing incidences of cybercrime effectively there is a need for the African nations to establish a central authority just as is available in the E.U, to coordinate the existing efforts of various national and sub-regional efforts that have been put in place to fight cybercrime.

# LIST OF REFERENCES


African Union Cybercrime Convention, Article 29(3)(1)(g) Date of Adoption 27 June 2014. Date of last signature 29 January 2018.

African Union (2008) Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report. Addis Ababa, Ethiopia: African Union.

African Union Ministers in Charge of Communication and Information Technologies (2009) Oliver Tambo Declaration. Johannesburg, South Africa: African Union.

African Union Convention on the Establishment of a Credible Framework for Cybersecurity in Africa. (2011), AU Draft0 010111, Version 01/01.2011.

African Union (2017). A Global Approach on Cybersecurity and Cybercrime in Africa. Available at https://au.int/sites/default/files/newsevents/workingdocuments/31357-wda_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf

Atta-Asamoah, A. (2010). Understanding the West African Cyber-crime Process. African Security Review, 18(4), 105–114. DOI:10.1080/10246029.2009.9627562

Boateng R, Longe O, Mbarika V (2010). Cybercrime and Criminality in Ghana: Its Forms and Implications. Proceedings of the Sixteenth Americas Conference on Information Technology, August 12-15, Lima, Peru.

Burt, D., Kleiner, A., Nicholas, J. P., & Sullivan, K. (2014). Cyberspace-2025: today's decisions, tomorrow's terrain. Navigating the Future of Cybersecurity Policy, 6, 47.

Cassim, F. (2012). Addressing the Spectre of Cyber Terrorism: A Comparative Perspective. Potchefstroom Electronic Law Journal, 394.

Castells, M. (2001). The Internet galaxy: reflections on the Internet, business, and society. New York, NY: Oxford University Press. DOI:10.1007/978-3-322-89613-1.

Collins, J. D., Sainato, V. A., and Khey, D. N. (2011). Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. Vol 5, Issue 1, pp 794-810 available from http:// www.cybercrimejournal.com/collinsetal2011ijcc.pdf> assessed on 7 May 2020.

Council of Europe Convention on Cybercrime: CETS No. 185 (Budapest, 2001). http://conventions.coe.int/Treaty/Commun/QueVoulezVoUS.asp?NT=185&CL=ENG.

Cybercrime Convention, Article 29(3)(1)(g) Date of Adoption 27 June 2014. Date of last signature 29 January 2018.

Cybercrime' European Commission, (2017). available at, https://ec.E.Uropa.E.U/hom affairs/what we- do/policies/organized-crime-and-human-trafficking/cybercrime_en, accessed on 19 Nov 2019.

Cybercrime' European Commission, (2017). available at, https://ec.E.Uropa.E.U/home-affairs/whatwe-do/policies/organized-crime-and-human-trafficking/cybercrime_en, accessed on 19 April 2020.

Economic Commission for Africa (June 2012) Declaration of Addis on the Harmonization of Cyber Legislation in Africa. Addis Ababa: Economic Commission for Africa, paragraph 10, p. 2.

Essien, E. (2015). The Challenges of Public Administration, Good Governance, and Service delivery in the 21st Century. International Journal of Civic Engagement and Social Change, 2(2), 55–66.

Essien, E. (2018). Ethical Implications of the Techno-Social Dilemma in Contemporary Cyber-Security Phenomenon in Africa: Experience from Nigeria. International Journal of Information Communication Technologies and Human Development, 10(1), 17–30.

Essien, E. D. (2019). The Imperatives of Critical Thinking, Social Norms, and Values in Africa: Pathways to Sustainable Development. In M. Lytras, L. Daniela, & A. Visvizi (Eds.), Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth (pp. 44-62). Hershey, PA: IGI Global.

European Union Briefing Paper, (2019). Challenges to Effective E.U Cybersecurity Policy.

European Cybersecurity Initiative, (2017). Factsheet on Cybersecurity: Working Towards a more secure Online Environment. European Commission.

Europol (2019). Cybercrime is becoming bolder with data at the centre of the crime scene. Press Release. https://www.E.Uropol.E.Uropa.E.U/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene

Finnemore, M. (1996). Norms, Culture, and World Politics. Insights from Sociology's Institutionalism, in International Organization 50: 2, 325-347.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. An international organization, 52(4), 887-917.Ojedokun A (2005). The Evolving Sophistication of Internet Abuses in Africa, the International Information and Library Review, 37:11-17.

Glance, D. (2017). What is the Dark Web? available at http://theconversation.com/explainer-what-is-the- dark-web-46070, accessed on 7 May 2020.

Gordon, S and Ford, R. (2006). Definition and Classification of Cybercrime. Journal of Computer Virology, 2:13-20.

Gordon, B. (2017). Internet Criminal Law. Available at, http://www.legalnet.co.za/cyberlaw/cybertext/chapter15.htm, accessed on 7 May 2020, para 426.

Gumbi, D. (2018). Understanding the Threat of Cybercrime: A Comparative Study of Cybercrime and the ICT legislative Frameworks of South Africa, Kenya, India, the United States and the United Kingdom. A Master's Thesis in Law in the University of Cape Town, 40-50.

Interpol (2011). About INTERPOL; http//www.interpol.int/public/icpo/default.asp

James, G. (2012). East Africa region moves to curb cybercrime, Buddecomm Africa research, pp 12-13.

Joint Communication to the European Parliament and the Council. (2017).

Kioni (2008). Are cybercrime laws in Kenya adequate? Kenya –byte; the Kenyan ICT sector issues and opinions, Retrieved Feb., 7, 2011 from http://kenya byte.blogspot.com/2008/10/are-cyber-crime-lawsin- Kenya-adequate.html

Kritzinger, E., & von Solms, B. (2012). A framework for cybersecurity in Africa. Journal of Information Assurance and Cyber Security, 12(2), 37–51. DOI:10.1109/ AFRCON.2013.6757708

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527.

Longe, O., & Chiemeke, S. (2008). Cybercrime and Criminality in Nigeria – What Roles are Internet Access Points in Playing. European Journal of Soil Science, 6(4).

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. 11. International Journal of Cyber Criminology, 79.

Makhanya P (2001). Hackers are stealing millions from KZN firms. Computer/IT, Retrieved November 21, 2019, from http://www.iol.co.za/index.php?click_id=115&art_id=ct20010514212 507126C1626355

Mukinda, F., (2009). Kenya Police Retrain 18 Officers to Fight Cybercrime; the nation, Retrieved from www.nation.co.ke/News/-/1056/510···16uhn/-/

Ngo, F. T and Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. Vol 5, Issue 1 p 773–793. available at http://www.cybercrimejournal.com/ngo2011ijcc, accessed on 7 May 2020.

Nyamanga, M. (2010). A Layered Framework Approach to Mitigate Crimeware. Annual ADFSL Conference on Digital Forensics, Security and Law. Available at http://commons.erau.edu/adfsl/2010/thursday/7 accessed on 7 May 2020.

Nye, (2012). The future of power, Public Affairs Quarterly Journal, vol 15 (3) pp 23-31

Oates J (2009). Operation Eagle Claw Nets 18 Nigerian Spammers, the A Register Retrieved November 2019 from http://www.theregister.co.uk/2009/10/23/nigeria_police_success.

Ojedokun A (2005). The Evolving Sophistication of Internet Abuses in Africa, the International Information and Library Review, 37:11-17

Orji, J. U. (2015). Multi-lateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation, 7th International Conference on Cyber Conflict: Architectures in Cyberspace.

Papadopoulos, S., & Snail, S. (2012). Cyberlaw@ SA III: the law of the Internet in South Africa. Pretoria: Van Schaik.

Renard, T. (2016). Partnerships for effective multilateralism? Assessing the compatibility between E.U bilateralism, (inter-)regionalism and multilateralism. Cambridge Review of International Affairs, 29(1), pp. 18-35.

Ryle, G. (2002). The Concept of the Mind. Routledge, pp. 12.

Sabillon, R. (2016). Cybercriminals, Cyber-Attacks and Cybercrimes: Privacy, Security and Control. Institute of Electrical and Electronics Engineers, PP.3-10.

Schjolberg, S. (2008) The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, p. 2. [online] Available from: law.net/documents/cybercrime_history.pdf [Accessed 14 May 2020]. http://www.cybercrime

Schwab, K. (2016). 'The Fourth Industrial Revolution: What it means, how to respond' World Economic Fsorum, available at http://bit.ly/1pBfye4, accessed on 7 May 2020.

Segal, A. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, New York: Public Affairs, pp. 7-8.

Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) Telecommunications Law and Regulation. 3rd ed. New York: Oxford University Press, p. 53.

Smith, M.H., Keukeleire, S. and S. Vanhoonacker, (2016). Introduction, in M.H. Smith, S. Keukeleire and S. Vanhoonacker (eds), The diplomatic system of the European Union: Evolution, change and challenges, Abingdon: Routledge, pp. 1-8.

Tamarkin, E. (2014). Cybercrime: A complex problem requiring a multi-faceted response. ISS Policy Brief, 51.

United Nations Economic Commission for Africa (UNECA) Press Release, Draft African Union Convention on Cybersecurity Comes to its Final Stage. [online] Available from: http://www1.uneca.org/TabId/3018/Default. aspx?ArticleId=1931 [Accessed 14 May 2020].

United Nations Office on Drugs and Crime (UNODC) (2013). Comprehensive Study on Cybercrime. Retrieved from http://www.unodc.org/documents/ organized-crime/ UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_ STUDY_210213.pdf

Wanjiku, R (2009). Kenya Communication Amendment Act (2009); Progressive or Retrogressive? Association for Progressive Communications (APC). Pp 15-16.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology 2(4): 407–427.

# APPENDICES

## Appendix. Non-exclusive licence

**A non-exclusive licence for granting public access to and reproducing the graduation thesis[1]:**

I Olufemi Abraham Johnson

1. Give Tallinn University of Technology a free of charge permission (non-exclusive licence) to use my creation

Fighting transnational cybercrime - prospects for the application of EU cyber standards to the African Union.

Supervised by Holger Mölder, PhD,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TUT library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TUT library until the copyright expires.

2. I am aware that the author will also retain the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed of the third persons' intellectual property rights or the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*