academicJournals

Vol. 6(1), pp. 1-12, August 2016
DOI 10.5897/JIIS2015.0089
Article Number: 930ADF960210
ISSN 2141-6478

http://www.academicjournals.org/JIIS

Journal of Internet and Information Systems

Review

Challenges to enforcement of cyber-crimes laws and policy

Ajayi, E. F. G.

School of Law, Kenyatta University, Nairobi, Kenya.

Received 4 August, 2015; Accepted 25 July, 2016

Cybercrime, a concept which to date has defied a globally accepted definition, appears to be the latest scourge plaguing man and same has occupied the cynosure. The word "cybercrime" is on the lips of almost everyone involved in the use of the computer and Internet, be it individual, corporate, organization, national, multinational or international. The attention accorded cybercrimes is not far-fetched; on one hand, it is partly rooted in its unavoidable nature as a result of the fact that telecommunications via the cyberspace, is the veritable means by which social interaction, global trade and commerce are transacted; and on the other, the economic losses to which all citizens are exposed whether now or in the nearest future. Aside economic losses, other consequences of cybercrimes includes but not limited to setback to the brand image and company reputation otherwise known as goodwill, loss of intellectual property and sensitive data, opportunity costs which includes but not limited to service and employment disruptions, penalties and compensatory payments to affected clienteles, contractual compensation for delays, cost of countermeasures and insurance, cost of mitigation strategies and recovery from cyber-attacks, the loss of trade and competitiveness, distortion of trade and job loss. This paper argues that it is not as if relevant laws and regulations are not in place because some advanced nations in the world have in one form or another, laws against cybercrimes, yet, the challenge of cybercrimes remains intractable and bewildering. As nations across the globe strives to curb cybercrimes through the instrumentality of the law, so are the cyber criminals devising new and sophisticated techniques to further their trade, thereby rendering impotent, the extant legal measures. This Article intends to bring to the fore, a comprehensive account of why cybercrimes remains an albatross in order showcase the enormity of the challenge faced by humanity, in the hope that, when the extent of the problem is known, may be, a global solution would timeously be fashioned out, to stem the tide of cybercrimes.

Key words: Cybercrimes, cyber criminals, challenges, enforcement, economic losses.

INTRODUCTION

Cyber-crimes are relatively a new phenomenon but same has occupied the cynosure of global attention simply because all citizens of the world, irrespective of whether private or public, are vulnerable to it, the said vulnerability

Email: ajayi.efg@gmail.com. Tel: +254 789192426.

is almost unavoidable for the fact that the world is in an information age (Encyclopedia of Library and Information Science, 1977), precisely; cyber-crimes emerged with the introduction of the Internet, thereby providing a conducive clime for crimes engendered by cyber criminals.

At the outset, it is necessary to briefly distinguish between a computer crime and a cyber-crime, the rationale being that more often times than not, the two concepts are regarded as one and same, when in fact they are only similar, but are definitely different.

Computer crimes, are those criminal acts perpetrated with the use of a computer; stated in other words, computer crimes includes crimes committed against the computer hardware, the materials contained or associated with the computer which includes the software and data; typical examples of computer crimes includes but not limited to embezzlement, fraud, financial scams and hacking etc.

Cyber-crime is an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes (McGuire and Dowling, 2013), the former are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT; this includes but not limited to fraud (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds); theft (including theft of personal information and identification-related data); and sexual offending against children (including grooming, and the possession, creation and / or distribution of sexual imagery).

Due to dichotomies in jurisdictions and yet addressing the same concept in legal literature, cybercrimes to date, has no globally accepted definition that could possibly encapsulate all the facets of this novel brand of crime, the definitional problem of cybercrime subsists, but one thing that is certain is that most definitions of cybercrime make reference to the Internet; for the sake overcoming the lacuna, cybercrime has been defined as crime committed over the Internet which might include hacking, defamation, copyright infringement and fraud. According to Oxford Dictionary of Law (2002), cybercrime also means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[1]

Having in the preceding paragraphs attempted the definition of cybercrime carried on through the cyberspace, it is necessary at this juncture to earmark the notorious fact that today, unlike in the past, there is unprecedented rise in the frequency and sophistication of cyber-crimes, unfortunately, the catastrophic effects of cybercrimes in turn, has engendered a barrier to trade and commerce and by so doing, a high cost in terms of losses incurred thereby affecting intercontinental business transactions across the globe.

At the global level, it is on record that cybercrime is a growth industry. The returns are great, and the risks are low. It is estimated that the likely annual cost to the global economy from cybercrime is more than USD 40 Billion, which reached USD 12 Trillion in 2012. A conservative estimate would be USD 375 Billion in losses, while the maximum could be as much as USD 575 Billion (CSIS, 2014).

The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen - incidents in the last year include more than 40 Million people in the US, 54 Million in Turkey, 20 Million in Korea, 16 Million in Germany, and more than 20 Million in China. One estimate puts the total at more than 800 Million individual records in 2013. This alone could cost as much as USD 160 Billion per year (Hawes, 2014). [2] All the foregoing figures as in number of victims and the staggering figures in term of economic losses, is a testimony to the almost insurmountable hurdle of cybercrime, to which mankind is faced and which challenge, must be addressed timeously.

MOTIVATIONS FOR CYBERCRIME

Aside from the global financial loss as summarized in the foregoing paragraphs with respect to impact of cybercrimes, other consequences of cybercrimes includes but not limited to loss of intellectual property and sensitive data, opportunity costs, including service and employment disruptions, damage to the brand image and company reputation, penalties and compensatory payments to customers (for inconvenience or consequential loss), or contractual compensation (for delays, etc.), cost of countermeasures and insurance, cost of mitigation strategies and recovery from cyber-attacks, the loss of trade and competitiveness, distortion of trade and job loss (Paganini, 2013).

Having previously brought to the fore, the impact of cybercrimes in terms of financial and economic effects as well as other consequences, the apposite question that would naturally agitate the mind of a discerning person is: what are the motivations of cybercriminals? This germane question is briefly addressed as hereunder:

The profit motive appears to be the first and major incentive that makes cybercriminals to persist in their

[1] Electronic Communications and Transactions Amendment Bill, 2012 South Africa

[2] See for detail account http://www.ponemon.org/news-2/23

nefarious activities of infiltration or unauthorized interference with computers and network systems; profits accruing to cybercriminals are indeed huge; from the account earlier on discussed before now regarding financial losses at the global level, these losses are profits to cyber criminals, hence, a serious motivation.

Closely related to the profit motive is the difficulty posed with respect to detection of cybercriminals; the Internet presents a wide range of freedom for all citizens of the world and the lack of prerequisite of identification as to who is doing what, in the use of the telecommunications via the cyberspace, continue to thwart global efforts targeted at tracking criminals and bringing them to book; stated in another way, the likelihood of identifying cybercriminals when they have perpetrated their illegal activities continue to be a motivation to them to persist in their criminal activities.

Competitors provides a boost to cybercriminal activities by sponsoring attacks on one another, either by way of espionage to steal critical information relating to trade secrets or paralysis of competitor's service through distributed denial of service (DDoS).

It should be added that some cybercriminals are motivated not for pecuniary advantage, but purely for satisfaction or pleasure they derive in gaining unauthorized access into computers and computer networks; the mere fact that cybercriminals are able to gain access into computer systems believed to be safe and secure by the owners and operators thereby revealing vulnerability gives the cybercriminals, under this head, the motivation.

Finally, another variant of motivation for cybercriminals is a challenge or protest against computer systems which is the outward manifestation of registration of disagreement or disapproval against owners or operators, this form or motivation is also more often than not aimed at getting profit out cybercriminal activities.

CYBERCRIME STATUTES

Cybercrimes seems to be well known to an average person who is Internet savvy wherever he is situate in the globe, unfortunately, the concept of cybercrime has no one definition that is world widely accepted. But the commonality of agreement is that cybercrime involves the use of computer having Internet connection to commit online crimes.

In view of the above, this paper adopts the succinct definition of cybercrime as illegal internet-mediated activities that often take place in global electronic networks (Chang et al., 2003).

There are many forms of cybercrimes and for ease of reference, it includes but not limited to 419 emails and letters, advance fee fraud, online auction fraud, online betting fraud, botnet-related fraud, child pornography and related offences, computer hacking, computer related forgery, computer related fraud, cracking, credit card fraud, cyber-laundering, cyber-smearing, cyber piracy, cybersquatting, cyber-stalking, cyber-terrorism, cyber-war, online dating fraud, denial of service attacks, domain name scams, identity theft, impersonation, intellectual property fraud, malware, viruses, misuse of devices, phishing, proxy servers, racist and xenophobic offences, smishing, spamming, spoofing, Trojan horse, spyware, system interference and vishing.

With respect to preventing, monitoring, criminalization, investigation and punishment of cybercrimes, many sovereign countries of the world have in place extant laws and those that do not, are striving to enact legislations, to tackle the challenge posed by cybercrime.

It is on record that the following countries have laws on computer or cybercrimes: Antigua and Barbuda, Argentina, Australia, Belgium, Bermuda, Cameroon, Chile, European Union, India, Ireland, Italy, Japan, Kenya, Malaysia, Mauritius, Pakistan, Portugal, Romania, Saint Vincent and the Grenadines, Singapore, South Africa, Spain, Sri Lanka, Thailand, Tonga, Turkey, United Arab Emirate, United Kingdom, United States, Uruguay, Venezuela and Zambia (Ajayi, 2015).

Hereunder is a summary of measures embarked upon at international and regional levels to address cybercrimes:

The G8 made public in 1997, a Ministers' Communiqué with action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment; it further mandated all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day and 7 days a week basis (Chang, 2003).

The United Nations (UN) General Assembly in 1990 the adopted a resolution dealing with computer crime legislation. In 2000 it also adopted a resolution on combating the criminal misuse of information technology while in 2002; it adopted a second resolution on the criminal misuse of information technology (Nicholas, 2008).

The International Telecommunication Union (ITU), saddled with telecommunications and cyber security issues in the United Nations released in 2003, Geneva Declaration of Principles and the Geneva Plan of Action highlighting the importance of measures in the fight against cybercrime and in 2005, adopted the Tunis Commitment and the Tunis Agenda for the Information Society.

The Council of Europe (CoE) comprising 47 European member states in 2001 took the lead by putting in place the first international Convention on Cybercrime, drafted in conjunction with USA, Canada, and Japan and signed by its 46 member states but ratified by only 25 countries (Ahamad et al., 2008). The Convention alternatively referred to as Budapest Convention is the first

transnational treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

The main objective of the European Convention, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation (Convention on Cybercrime, 2001).

With respect to regional efforts aimed at stemming the tide of cybercrimes, the Asia-Pacific Economic Cooperation (APEC) issued in August 2002 the Cyber security Strategy which is included in the Shanghai Declaration (Ajayi, 2016). The said Cyber security strategy deals principally with outlined six key areas for co-operation among member economies which are: legal developments, information sharing and co-operation initiative, security and technical guidelines, public awareness, training and education and wireless security.

The Organization for Economic Co-operation and Development (OECD) comprising of 34 countries published in 2002 "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."

The Commonwealth of Nations in 2002 presented a model law drafted in accordance with the Convention on Cybercrime (International Telecommunication Union, 2009), which provides a legal framework that harmonizes legislation within the Commonwealth and enable international cooperation.

The Economic Community of West African States (ECOWAS) comprising of fifteen member states adopted in 2009, the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law (Nicholas, 2008).

CHALLENGES TO ENFORCEMENT OF CYBERCRIMES

As earlier discussed, the efforts made through the instrumentality of legislations at national, international and regional levels were discussed; without prejudice to the effectiveness of the extant laws in place to combat cybercrimes, the scourge persists, nay, rather than the laws to curb, or better still, minimize cybercrimes, there is a rise in the frequency and sophistication and the reason for that development, is attributable to the fact that, as efforts are being made to stem the tide of cybercrimes, so are cybercriminals devising methods and means of thwarting global measures targeted at addressing the problem.

Here, the challenges faced by mankind which makes cybercrimes intractable are discussed as follows:

Identity of cybercriminals

This paper is of the view, that one of the greatest impediments against global efforts towards stemming the whirlwind of cybercrimes remains the anonymous nature of the identity of cybercriminals. There is no easy means of identifying who is doing what and where is a user of the Internet is situate at any point in time; the global information system is free and there is no perquisite that needs to be fulfilled, before a user can login to connect with anywhere and anyone across the globe. Thus, the unfettered freedom of information and communication enables the cybercriminals to hide their identity using different telecommunications gadgets so as to make it impossible to trace the online Internet Protocol (IP) address of any user. Further, if the IP address of a cybercriminal were traced to a particular location, the next hurdle cannot be scaled as the identity of a cybercriminal is undisclosed to the owner or operator of Internet service provider.

Several telecommunications gadgets such as Psiphon, The Onion Router (Tor) etc. are used to shield the identity of Internet users and communication are often routed via many servers which further compounds the possibility of cybercriminals being traced. In effect, if the identities of criminals are incapable of being traced, how can the laws enacted to address cybercrimes work? The dictum of law Lord Denning in a celebrated case [3] to the effect that, it is a cardinal principle of Law that "*You cannot put something on nothing and expect it to stand"* The point being emphasized here is that, in so far as the identities of cybercriminals remains elusive, no law, however well-crafted nor intended can work because the law does not work in vacuum; stated in another way, cybercrime laws were principally enacted to apprehend and prosecute cybercriminals, so, if the criminals are not identifiable, any law(s) put in place, is nothing but a nullity.

It should be quickly added that the campaign in some quarters to end anonymity in the use of the Internet by the mandatory introduction of identification as a perquisite has been ferociously opposed by human rights activists on the ground of violation of privacy rights, with that development, cybercriminals appears to have been offered latitude to continue to operate unhindered and by so doing, the challenge of anonymity continues to render cybercrime laws, nugatory.

Jurisdictional challenges

Aside from the germane issue of anonymity discussed before now, one other potent challenge to enforcement of cybercrime laws is jurisdiction. Taking into cognizance the time tested principles of state independence,

3Macfoy versus United Africa Company Limited (West Africa). 1962 AC 152

sovereignty and territorial integrity, each nation-state of the world, have the authority to make laws binding on things and all persons within its geographical entity, called a country.

For the above stated reason of nation-states making laws on the same matter from different jurisdictions, conflict of laws is unavoidable.

Jurisdiction may be defined as the power of a court or judge to entertain an action, petition or proceedings. See *Alade v Alemuloke.*[4] The issue of jurisdiction is so radical that if forms the basis of any adjudication, stated otherwise, it goes into the roots of any matter before the courts. If a court lacks jurisdiction, it also lacks necessary competence to try the case. A defect in competence is fatal, for the proceedings are null and void *ab initio*, however well conducted and well decided the case may be.

A defect in competence is extrinsic to adjudication. The court must first of all be competent, that is, possess jurisdiction before it can go ahead on any adjudication See *Oloba v. Akereja* [5] See also *Madukolu & Ors. V Mkemdilim* [6].

Given how fundamental the issue of jurisdiction is at law, and bearing in mind its radical nature, it has been asserted to the effect that, there is no technical word in the whole of conflict of laws that is more variously used and abused than jurisdiction. It is a word with too many meanings and all that can be done about it is to ascertain the sense in which it is being used at any given time. [7]

A distinction ought to be made between the use of the term jurisdiction in extra-territorial and intra-territorial situations. While intra-territorial competence of a court concerns the authority of a court to hear and determine an issue upon which its decision is sought, the significance of extra-territorial competence of a court comes into focus when its judgment is sought to be enforced outside the forum.

At this juncture, it is necessary to earmark that jurisdiction has many facets; however, the concern of jurisdiction with respect to enforcement of cybercrime laws basically revolves around two issues, namely, geographical jurisdiction and jurisdiction *in personam.*[8] Geographical jurisdiction addresses the fundamental issue as to if a court have the power beyond the territory where it is situate, while jurisdiction *in personam* deals with whether a court is empowered to hear and determine a case of a cybercriminal not within its jurisdiction.

Given the peculiar nature of cybercrime, it is in a class of its own, it is unique and distinct in character unlike traditional terrestrial crimes, which are committed in a particular locus and whereof, the effect(s) are felt by the victim(s); stated in another way, cybercrimes transcends states and jurisdictions; they are cross border or transitional crimes. Thus, a cybercriminal may sit in the comfort of his home, office, café or wherever he chooses, with a desktop, laptop, tablet or phone connected to the Internet and carry out his illegal activities that would be felt thousands of kilometers away, from where the act(s) took place.

The scenario depicted above, showcasing the pervasiveness of cybercrime has been aptly expressed as "the ubiquity of information in modern communication systems makes it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for the perpetrator or the victim of a crime to move or to meet in person. Unlawful actions such as computer manipulations in one country can have direct, immediate effects in the computer systems of another country...." (Sieber, 1997).

To sum up jurisdictional challenge to enforcement of cybercrime laws, it means if the hurdle of anonymity is scaled and a cybercriminal is clearly identified but he is situate in another country aside from where the victim is domiciled, the court of the forum cannot effectively try such a criminal as the court lacks jurisdiction geographically and also in rem; a discerning mind would immediately jump at extradition of the criminal as a solution, but this process, that is, extradition is fraught with its own challenges aside from double criminality requirement,[9] especially where there is not in existence extradition treaty or mutual legal assistance treaty between the requesting state and the state having custody of the criminal.

Extradition processes challenge

The word extradition is an amalgamation of two French words viz. *ex* - which means "out" and tradition - "deliverance." It is the process of returning somebody accused of a crime by a different legal authority for trial or punishment. [10] Extradition has also been defined as the surrender by one state to another of a person accused of committing an offence in the latter (Oxford Dictionary of Law, 2002).

A casual glance at the definition of extradition as above, would ordinarily raises the hope that, if a person is alleged to have committed a cybercrime in one jurisdiction and escapes to another country, all that needs to be done by the country where the cybercriminal is domiciled is expeditiously return the said criminal to the requesting country, to face trial, however, in practice, this is not so because of the principle of state independence and sovereignty earlier stated before now. Under

4 (1988) 1 N. W. L. R. (pt. 69) 207
5 (1988) 1 N. W. L. R. pt. 84 at 587
6 (1962) 1 All N. L. R. 587
7 Leflar: Jurisdiction and Conflict of Laws P. 223
8 Latin "against a person" opposite of *in rem* "against a thing" for example, property
9 Principle that the offence for which an accused is sought to be extradited must be a criminal offence at the state making a request and also at the state where the accused is domiciled.
10 Microsoft Encarta Dictionary 2009

international law, there is no instrument that imposes on sovereign nations an obligation to automatically return cybercriminals for trial. In effect, countries where cybercriminals are situate, for different reasons, more often than not, refuse to extradite cybercriminals and this development, present an insurmountable challenge to the enforcement of cybercrime laws across the globe.

To address the lacuna created as a result of lack of international law not making it mandatory to extradite criminals, extradition treaties fills the void, thus if there is a treaty between two states, criminals may be extradited and even at that, there are many exceptions to extradition processes.

One of the biggest hurdles to extradition of criminals to requesting states is the "unruly legal horse" called jurisdiction; jurisdiction is often invoked by countries to deny extradition especially if the requested state have jurisdiction to try criminals, who is a national of the requested state; as such, the requesting state have no choice than abide with that decision not to commence extradition. By this development, the object of criminal justice as in the enforcement of applicable cybercrime law is defeated by the legal hurdle placed in the part of justice by law. Quite a number countries having in their laws, jurisdiction to conduct trials over their nationals for offences committed abroad includes but not limited to: Austria,[11] Brazil,[12] The Czech Republic,[13] France,[14] Germany, [15] and Japan. [16] This paper is cognizant of the controversy surrounding the propriety of conducting trials by countries regarding their nationals for crimes committed abroad and feels that it is most unlikely that justice can hardly be done which of course compound the enforcement of cybercrime laws.

Under international law, a doctrine akin to the issue of jurisdiction discussed above and which imposes obligation on states is *aut dedere aut judicare*, a Latin expression which simply means "extradite or prosecute" persons alleged to have committed international crime. Notable international crimes to which the *aut dedere aut judicare* doctrine is applicable are: Acts of terrorism, taking of civilian hostages during armed conflicts, hijacking of civil aircrafts, torture, crimes against diplomats and other internationally protected persons, and financing of terrorism and other international crimes; unfortunately, cybercrimes is nor specifically mentioned in the list but same could be categorized under "other international crimes."

The *aut dedere aut judicare* principle is distinctly different from jurisdiction over nationals discussed as above in that it is a multilateral treaty and operates irrespective of whether a country has requested for the extradition of criminals or not and it does not matter whether the alleged criminal is a national or foreigner, the underlying issue is that in so far as the criminal is within the jurisdiction of any state, the obligation to extradite or prosecute operates. Some of the international treaties with *aut dedere aut judicare* clause are The Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Uniterd Nation Human Right, 2005). The Convention for the Protection of Cultural Property in the Event of an Armed Conflict (Uniterd nations educational scientific and cultural organization, 1954). The U.N. Convention Against Corruption (United Nations Office On Drugs And Crime, 2014), and Geneva Conventions. [17]

Other exceptions to extradition of cybercriminals which has made enforcement of cybercrime laws to be limping are hereunder briefly mentioned:

Dual criminality principle must be fulfilled which means that before a criminal can be validly extradited, the alleged offence must be a crime punishable at the jurisdiction seeking extradition, nay, same must also be a punishable offence where the criminal is domiciled; without satisfying this criterion, the criminal may not be extradited. Fear of inhuman treatment is a bar to extradition and this basically includes torture and degrading punishment which are likely to be meted out to the criminal. See the celebrated and protracted case of *Soering V. The United Kingdom* [18] dealing with extradition of a German national alleged to have committed murder in the US and who fled to UK; the court established in the case that states are indeed responsible for the wellbeing of individuals in their territory and held that implementation of the Secretary of States' decision to extradite Mr. Soering would represent a breach of Article 3 and not breach of Articles 6 and 13.

See also the extradition case of *Othman (Abu Qatada) v. United Kingdom,* [19] decided after the *locus classicus* case of *Soering V. The United Kingdom* (supra) on the ground of fair-hearing under Article 6 of ECHR.

In extreme cases, where death sentence is likely to be the faith of the criminal when extradited; extradition processes may be refused. In a bid to give credence to sanctity of human, a number of countries including but not limited to Australia,[20] Canada,[21] most European

11 Austrian Extradition and Legal Assistance Act Section 12 See http://www.ris.bka.gv.at/geltendefassung.wre

12 Brazilian constitution of 1988, Article 5 www.stf.jus.br/repositorio/cms/..en./constituicao_ingles

13 Charter of fundamental rights and freedoms, Article 14 (4) http://www.usoud.cz/en/charter of fundamental right

14 Code of criminal procedure (legislative part), Articles 696-1 to 696-7" (PDF) http://www.legifrance.goun.fr

15 Basic Law for the Federal Republic of Germany, Article 16 (2) http://www.bundesrecht.juris.de

16 Law of Extradition Japan Article 2 See http://www.moj.go.jp/english/information/loe.01.html

17 https://www.icrc.org/...law/ Accessed 18th May 2015

18 (1989) European Court of Human Rights; Extraterritorial responsibility under Article 3 EHRC establishes a legal barrier on deportation or extradition of persons if there are substantial grounds for believing that there is a real risk of treatment contrary to Article 3

19 8139/09 (2012) ECHR 56

20 EXTRADITION ACT 1988 www.austlii.edu.au/au/legis/cth/consol_act/ea1988149/ Accessed 18th May 2015

21 Justice Laws Website. laws-lois.justice.gc.ca/eng/acts/E-23.01/ Accessed 18th May 2015

nations aside Belarus,[22] and New Zealand[23] forbids death penalty as a punishment and thus, would not favour extradition of criminals for whatever offence, they might be alleged to have committed.

In addition to the exceptions to extradition stated in all the foregoing, where the alleged offence is classified as political, extradition of the criminal may be refused. The exceptions to extradition based on political motives are broadly classified as pure political offenses which are targeted at governments and includes treason, sedition, and espionage and the other is, relative political offenses committed for political motives or in a political context or in connection with a political act. Pure political offences are excluded from realm of extradition (Bassiouni, 1999), while relative political offences have many legal tests not particularly very relevant to the issue under discuss.See elucidation of political offences regarding the attitude of the courts, see generally the cases of *Quinn v Robinson* [24] *Cheng v Governor of Pentonville Prison* [25] *R v Governor of Brixton Prison, Ex Parte Schtraks* [26] *Re Ezeta*, [27] *Matter of Doherty*, [28] *Schtraks v Government of Israel* [29]

With reference to political offences, the concept is indeterminable and the category is never closed. This paper poses a question that: if an expert brings down a website used for propaganda of political falsehood about a particular government's activities and the said expert flees to another country, would his alleged offence be political or criminal?

From all that has been discussed here, it is manifestly clear that extradition of criminals whether for cybercrimes or other international crimes has been legally fettered by exceptions and aside from that limiting factor of legalese of extradition, the processes of returning criminals are overly cumbersome, time consuming and costly.

The challenge regarding the nature of evidence

One other impediment to the enforcement of cybercrime laws wherever attempts are made anywhere across the globe, is the nature of evidence available in the custody of prosecution and the admissibility of same, during the course trial of cybercriminals.

Evidence is that which tends to prove the existence of some fact. It may consist of testimony, documentary evidence, real evidence and when admissible. The law of evidence comprises all the rules governing the presentation of facts and proofs in proceedings before a court, including in particular the rules governing the admissibility of evidence and the exclusionary rules (Oxford Dictionary of Law, 2002). Evidence could take any form such as circumstantial, conclusive, direct, extrinsic, primary, secondary etc. but the purview of evidence with respect cybercrimes is application of science to decide questions arising from crime or litigation known as forensic. [30]

It is settled and far beyond controversy that in criminal prosecution, it is incumbent on the prosecution to prove his case beyond reasonable doubt before a conviction of the accused can be obtained; thus the nature of fact or documentary proof adduced as evidence in the prosecution of cybercriminals goes to the root of any trial; unfortunately, evidence available to prosecutors is at best described as tenuous, *ipso facto*, most attempts made at bringing cybercriminals to book are thwarted.

Unlike in terrestrial crimes where physical evidence could be presented to the court with the view of securing conviction of the accused, physical evidence is rare in cybercrime prosecution; this is an albatross, all what the investigators and prosecution can have and rely on, are mere footprints on the computers used by the criminals and traces left on the Internet; the nature of these proofs have little evidential value and same is hardly convincing to courts seized of criminal trials.

At this juncture, it is necessary to state in no uncertain terms; that the nature of evidence in cyber prosecution is basically digital, be that as it may, the digital era has brought with it so many advantages; however, the challenge of digital concoction that comes with advantages of electronics in cyberspace is overwhelming in view of evidential nature being a representation of sound or light waves as number by means discrete signals interpreted as numbers, usually in the binary system; this peculiar nature of evidence arising from digitalization is delicate in character and makes it vulnerable to damage whether intentional or otherwise, ditto manipulations, which naturally would render such evidence to be of little or no value and thus inadmissible by the courts.

What is being emphasized as to nature of digital evidence is that, generally, they are delicate so much that mere examination by inexperienced investigator(s) may contaminate or out rightly damage such evidence and of course if that happens, experts in data recovery would have to be called in to carry out repairs which is not cheap.

Added to above is the propensity of willful destruction of evidence by cybercriminals so as to escape justice, in other words, when evidence that could provide solving of a crime in the cyberspace is destroyed, investigators usually would have little or no clue to follow in the arrest and prosecution of such crime(s).

One other practice engaged by cybercriminals which compound evidence in cyberspace is impersonation or

42 Criminal procedure code of the Republic of Belarus; no specific legislation on extradition

23 Legislation Act 2012. www.legislation.govt.nz/pdflink.aspx?id Accessed 19th May 2015

24 783 F.2d 776 (9th Cir. 1971)

25 (1973) A.C. 931, 945 H.L

26 (1964) AC 556, at 583 HL

27 62 F. 972, at 978 (ND Cal)

28 599 F. Supp 270 (SDNY 1984)

29 (1964) AC 556, 582-584.

30 Microsoft Encarta Dictionary

identity theft; this is intentionally done to sway and steer off investigation as to the real identity of cybercriminals, more often than not, innocent persons are arrested and prosecuted for offences they know nothing about. In other words, digital technologies provide ample opportunities for impersonation by way of identity disguise so as make it difficult if not impossible to ascertain who the perpetrator of cybercrimes is.

Up to this point, the issue of challenges faced with respect to evidence in cybercrime enforcement has been discussed, it is necessary to sum it up by stating that the nature of such evidence is difficult to gather, nay, the said evidence is fragile and susceptible to manipulation and destruction besides being costly as same is forensic.

Lack of effective reporting and dearth of data

As elsewhere pointed out before now that many countries in the world have applicable law and policy against cybercrime but the enforcement of same is a challenge and part of the challenge is not unconnected with lack of effective reporting of incidences of cybercrimes to the appropriate authorities across the globe, in effect, this development has militated against bringing to global attention and appreciation of the extent of the menace of cybercrimes; closely related to reluctance to disclosure of cybercrimes is the lack of cooperation on the part of the victims, other stake holders and witnesses with police or other agencies saddled with investigation and prosecution of cybercriminals, it is immaterial whether private, corporate or institutional entities are the victims.

Several reasons have been advanced for reluctance to report cybercrimes and these includes but not limited to costs arising from follow up of cybercrimes which more often than not far outweigh the benefit derivable thereof, the damage to the reputation and goodwill of victims especially corporates which are going concerns, of course, the protracted investigation and prosecution which are generally considered as effort and time wasting exercises, more importantly, the difficulty of diligent investigation which is usually scuttled when a particular cybercrime investigation and prosecution traverses many jurisdictions thereby bringing to the fore issues in approach to cybercrimes.

In order to buttress apathy to the reporting of incidences of cybercrimes, for over a decade, an empirical evidence of a survey carried out by the consultancy firm of Ernst and Young (Ernst and Young, 2003), found that only one quarter (1/4) of frauds reported in the survey were referred to the police and further, that only 28% of those respondents were satisfied with the said investigation.

In a related survey, earlier on carried out and anchored by another globally renowned firm (KPMG, 2001) the reasons afore stated were replicated as accounting for unwillingness to reporting of cybercrime events, besides the priority accorded to the reinstatement of systems that were interfered with or intruded into, the rationale being to minimizing further business losses that would most likely occur while following up the cyber event as in investigation and prosecution of same.

For businesses that are in a competitive environment, reporting of cyber incursion is viewed as exposing the weakness or vulnerability of systems, this development erodes the clienteles' confidence and may engender consumer turn-away, thus the owners and operators would rather keep silent and try as much as possible to rectify the system than report to authorities in charge of cybercrimes.

Lack of effective reporting of cybercrime events and dearth of data go *pari passu*, the rationale being that, it is when cybercrimes are reported that data about same can be collated and published. The dearth of reliable data and information generally about cybercrimes has created lack of awareness; the said development has shrouded the extent of the problem to which mankind is presently faced with. This paper is of the view that the awareness and appreciation of any problem in human endeavors is the beginning of any problem solving; as things stands today, only a fragment of the elite are aware of the impact of cybercrimes on the society.

Cost, time and efforts incurred in investigation and prosecution

Given the nature of evidence, that is, forensic, needed in the prosecution of cybercrimes, the cost of same as a scientific crime solving approach as opposed to gathering of evidence in terrestrial crimes is not particularly cheap because of the high-tech equipment, materials and expertise involved to carry out such investigations.

With specific reference to business and social interaction, the advent of technology has two pronged outputs, one side represents the numerous advantages which are manifest in the speed and accuracy of information and communications to man wherever he is situate and which development has aptly described the world as one global village, [31] the other dark which has notoriously tagged the dark side, is the unsavory rise in cybercrimes; when the dark side rears its head, it presents herculean task for investigators and other law enforcement authorities to unravel, given the mass of information that needs scientific examination such as wading through numerous files and breaking encrypted codes, before clues that were intentionally hidden or destroyed, could be sieved out that would possibly lead to arrest and prosecution of cybercriminals at exorbitant costs aside time and efforts of experts which should have been usefully used in other ventures.

31 A term ascribed to McLuhan who described how the globe has been contracted into a village by electric technology and the instantaneous movement of information from every quarter to every point at the same time. See generally Marshall McLuhan, The Gutenberg Galaxy: The Making of Typographic Man (1962) and Understanding Media (1964).

At this juncture, it is necessary to remark that the first and foremost challenge in the enforcement of cybercrime laws as pointed out under section 4.1 of this paper, is the identification of the criminals. Be that as it may, it is relatively easier when the criminal is located within jurisdiction and a much more herculean task, if a cybercriminal is in another country different from where such criminal is wanted for the purposes of arrest and prosecution.

In cases where a criminal is wanted extraterritorially, many issues crops up which represents additional costs in the investigation of the cybercrime and these includes air travels where it is expedient that investigators have to be physically present in another jurisdiction, and where not, telephones and Tele-conferences, are not avoidable because investigators need to interact in other jurisdictions so as to effectively pool efforts together to unravel cybercrime; and such interactions between investigators, it must be noted, is not that easy due to time differences, for example, it could be that when some Americans are in bed, Ugandans may be at work. Additional costs associated with travels include accommodation, feeding, transportation, entertainments and other miscellaneous costs.

Further, with respect to different jurisdictions is the issue of language barrier, thus where Chinese investigators must work with English counterparts, language differences occasion problems which must be sorted out by translators at additional cost ditto where there is need for exchange of documents, same must be translated thus warranting extra cost.

Besides all the foregoing are other intangibles, yet, very important issues such as differences in culture, attitude and perception of countries to cybercrimes and cognizance must be taken of the double criminality principle; the cooperation of witnesses and other stake holders is not guaranteed as well and same cannot be taken for granted. It should be added that aside from cost of investigation, another variant of cost of cybercrime is the cost associated with prosecution, for this, lawyers have to be hired at very high cost in addition to filing fees and other incidental costs of litigation. From all what has been stated in this section, it is manifestly clear that cost of investigation and prosecution of cybercrimes is prohibitive which development sometimes occasion many cases to be jettison mind bearing that the benefits derivable from investigation and prosecution may not be worthy of the troubles, in effect, cybercrimes continue to flourish.

Lack of adequate legislation and ineffective ones where extant

The enforcement of cybercrime laws have largely been hampered due to inadequate legislations and the ineffectiveness of same where there are extant laws in place for cybercrimes.

According to the United Nations, [32] there are 193 Full UN Members, 2 Observer States and 6 States with partial recognition, making a total of 201 countries in the world. Out of this number, only about 79 countries (Ajayi, 2015), the majority being in Western Europe comprising 47 countries, have laws specifically enacted for cybercrimes; a simple inference that could be drawn from above data is that less than 40% of countries in the world have laws forbidding cybercrime.

Given the above scenario of lack of relevant legislations specifically in place for cybercrime, it goes without saying that the development tantamount to giving cybercriminals a license to operate freely without fear but rather with impunity. The absence of requisite laws is even more prevalent in Africa where out 54 countries [33] constituting the continent, only 4 namely Cameroun, Kenya, South Africa and Zambia (Ajayi, 2015), have laws criminalizing cybercrimes. It is hoped that when the newly enacted African Union Convention on Cyber Security and Personal Data Protection[34] comes into force, the lacuna in the law and policy with respect to cybercrimes and other acts incidental thereto, shall be frontally addressed.

It is instructive to note that even where there are legislations on cybercrimes, the provisions of the said extant laws are not severe enough to deter cybercriminals from their illegal acts. A few examples would suffice to buttress the assertion to the effect of non-deterrent laws; in Australia, there exist *Cybercrime Act 2001*, The *Criminal Code Act 1995: Computer and telecommunications services offences* and the *Telecommunications (Interception and Access) Act 1979*, all of these laws prescribed light sentences between one to three years jail terms except child phonograph. [35]

In the United Kingdom, United Kingdom Computer Misuse Act 1990 as amended by Police and Justice Act is in place but a conviction of the offences only attracts a jail term of between six months to five years except acts bothering on distributed denial of service attacks (DDoS) which prescribed a maximum sentence of ten years. [36]

The extant South African law on cybercrime is the Electronic Communications and Transactions (ECT) Act, 2002 is the applicable law which provides for imprisonment for a period not exceeding five years.[37]

32 As at 28th February 2015 See www.polgeonow.com/2011/.../how-many-countries-are-there-in-world. Accessed 29th May 2015

33 World Atlas

34 pages.au.int/.../en_AU%20Convention%20on%20CyberSe...Accessed 29th May 2015

35 Criminal Code Law of Australia section 474 prescribed a jail term of 15 years for child phonography and a term of 25 years where the offence is aggravated child phonography.

36 Section 3 of Computer Misuse Act 1990 Laws of United Kingdom amended by section 36 of Police and Justice Act 2006

37 The Act by virtue of section 89 prescribed penalties for contravention of the provisions of the Act whereof subsections provides as hereunder that: (1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months. (2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years

From all the foregoing, it is apparent that the state of the law is not punitive enough and by so doing, even if the extant laws are enforced, it would make little or no impact on the cybercriminals as the laws cannot possibly deter criminals from their illegal acts.

International law without enforcement mechanisms

It is often touted that international law is no law simply because of its lack of enforcement mechanisms; though this assertion is controversial, but the protagonists of this statement insist that, in so far as there are standing force to implement international laws, they are not persuaded by any argument(s) no matter how convincing, that international law is indeed law in practice.

This paper is of the view that the established principles of independence, sovereignty and territorial bounds in theory, preserves the equality of states but in reality, the George Orwell's sagacious statement that "all animals are equal, but some are more equal than others" is apposite to describe the strength of nations in their relation with one another.

Without dissipating so much energy and join a needless academic exercise, sanctions as may be imposed by Security Council under Chapter VII of the UN Charter is one of the means of enforcing international law and aside from that, reciprocity, collective action and shaming [38] have been documented as enforcement methods.

With specific reference to cybercrime, the Council of Europe Convention on Cybercrime (ETS No. 185) otherwise known as the Budapest Convention [39] is a well-known subsisting treaty that have a status of international application which entry into force on 1st July 2004.and the point that is being made is that, if a state is a party to the treaty, but refuses to enforce provisions of the same in its territory, what can other states in the comity do to ensure compliance of the erring state?

The non-binding nature and lack of strict enforcement mechanisms of international law is by and large, with respect to cybercrime laws appears to have stultified the enforcement of cybercrime laws. For elucidation, see generally Articles 15, 22, 23, 24, 28, 38, 39 (3), 40 and 42 of the Budapest Convention.

Domestication of international law and applicability to suit local conditions

Generally, it is a legal requirement to the effect that, when presidents or head of states as the case may be, might have signed international treaties, there is need to put in place legislations to make the signed treaties a binding legal instrument at the national level; but very often, the legislature saddled with law making authority neglect this obligation and by so doing, the international treaties or bilateral agreements cannot be enforced by the relevant countries who are parties to treaties.

The above rule also applies to putting in place, enabling legislations with the view to making international treaties and agreements to be applicable, so as to suit prevailing local conditions, largely due to differences in culture, language, religion, norms, values and other attributes associated with different nationalities. In other words, when treaties are made at the international level, the arrow heads of such treaties more often times than not, whether intentionally or otherwise, bring to the fore and reflect their ethnic nationalities attributes whereas the signatories of such treaties may or may not have influence over the terms of the treaties.

The inability or tardiness of legislatures across the globe to do the needful and timeously domesticate cybercrime laws has slowed down the enforcement of same. The provisions of The Budapest Convention in many of the Articles thereto, for instance, enjoins member-states who are signatories to domesticate and make applicable the Articles; a typical example of legal requirement of domestication of treaties is section 12 of the Nigeria Constitution [40] which *inter alia* provides that no treaty shall have a binding effect unless domesticated.

Ill trained, poorly paid and lack of protection for law enforcement agencies

This paper is of the opinion that cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or in rare cases wreak havoc to computer systems, they have been described as professional thieves and soldiers of fortunes, [41] above all, cybercriminals are experts in computer and cyberspace issues, thus, the expertise of cybercriminals cannot be juxtaposed with law enforcement agencies who are mere government officials that are ill-trained, poorly remunerated and who offer their services without proper security and protection.

The foregoing factors make efforts targeted at investigation and enforcement of cybercrime laws, puerile, because the cybercriminals are far ahead of law

38 The Levin Institute - The State University of New York, Globalization 101 Institute International Law: How is International Law Enforced

39 The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. See http://conventions.coe.int

40 (1) No treaty between the Federation and any other country shall have the force of law to the extent to which any such treaty has been enacted into law by the National Assembly.
(2) The National Assembly may make laws for the Federation or any part thereof with respect to matters not included in the Exclusive Legislative List for the purpose of implementing a treaty.
(3) A bill for an Act of the National Assembly passed pursuant to the provisions of subsection (2) of this section shall not be presented to the President for assent, and shall not be enacted unless it is ratified by a majority of all the House of Assembly in the Federation.

41 LegalBrief E Law & Management Cyberlaw & Technology Watch Issue No: 1581 29th 2015 p.1

enforcement agencies in terms of access to funds and necessary acquisition of skills in computers and cyberspace related issues.

Dearth of experts in prosecution of cybercrimes

Related to the above factors of poor training, remuneration and inadequate security and protection on the hazardous job for law enforcement agency officials is the dearth of experts in the prosecution of cybercrimes. It is a well-known fact that, if even if the law enforcement agencies had done a good job in the investigation of cybercrime, at the litigation stage, expertise of prosecution attorneys is still very important to secure the conviction of cybercriminal as it is incumbent on prosecution to proof his case beyond doubts; unfortunately, this is not the case as there is dearth of savvy prosecutors in government justice departments, however, cybercriminals have unfettered access to renown private attorneys who charge very high legal fees which is not a problem to the cybercriminals as they could readily afford to pay high professional fees to the best lawyers who specializes in cybercrime practice; further, anonymity issue of cybercriminals and the nature of evidence which more often than not tenuous, regarding the fact that investigators can only rely on traces and tracks left on computers and Internet, all goes to compound the case of prosecutors who are not as grounded in handling of cybercrime litigation compared with their counterparts in private practice; these identified gaps unfortunately are a plus for cybercriminal who in addition to technicalities in cybercrime cases have more than enough funds to hire first class attorneys.

Absence of one universal law governing cybercrimes

The absence of one universal law governing cybercrimes is the final point on which this paper anchors this discuss, and state as elsewhere before now emphasized, that cybercrimes respects no jurisdiction because it is possible for a criminal can sit in Cape Town and perpetrate his act that would have effects in Cairo, Honolulu or anywhere in the world.

Stated in other words is that, cybercrimes are borderless, transnational and international crimes and which said crimes, are committed in the cyberspace; but the majority of the laws and policies dealing with cybercrimes to date, are either national or regional; the only law specifically dealing with cybercrimes which is international in character, is the Budapest Convention which for all intents and purposes, is hampered by difficulties associated with international laws, an issue already copiously discussed.

Cybercrimes have only one jurisdiction, that is, the entire world; by so doing, the extant laws and policies which are fragmented, national, regional or quasi-international cannot possibly cope with the problems engendered by cybercrimes; *ipso facto,* cybercrime laws shall continue to suffer from enforcement challenges; the only law that can frontally address the menace of cybercrimes, is that law that would have only one jurisdiction, applicable globally, and not until the political will is mustered to enact that universal law, mankind shall continue to be plagued by challenges of enforcement posed to cybercrimes laws.

CONCLUSIONS

This paper states that there are relevant laws across the globe dealing with cybercrimes but the challenges of enforcement of the said laws, continues because of issues discussed in “Challenges to Enforcement of Cybercrimes”.

In addition to the foregoing, are the absence of a global consensus on the types of conduct that constitute a cybercrime; the absence of a global consensus on the legal definition of criminal conduct; the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to computerized data; the lack of uniformity between the different national procedural laws concerning the investigation of cybercrimes; the lack of extradition and mutual legal assistance treaties, synchronized law enforcement mechanisms that would permit international cooperation in cybercrime investigations, and existing treaties that take into account, the dynamics and special requirements of these investigations (Miquelon-Weismann, 2005).

RECOMMENDATIONS

This paper holds the view that the identification of any problem is a stepping stone to addressing the identified problem; this paper has thus strived to put into clearer focus the challenges faced by man with respect to cybercrime enforcement for a better understanding and appreciation of the issues.

The foremost recommendation proffered by this article, is the need to put in place a universal law, that would have universal applicability with only one jurisdiction, so much that, wherever a cybercrime is committed, the perpetrator can be brought to book, irrespective of where he is situate; other recommendations specifically addressing each of the sub-heads of challenges identified in this paper, are reserved for another paper, dedicated to solving the challenges of cybercrimes.

Conflict of Interests

The author has not declared any conflict of interests.

REFERENCES

Ahamad M, Amster D, Barrett M, Cross T, Heron G, Jackson D, King J, Lee W, Naraine R, Ollmann G, Ramsey J, Schmidt HA, Traynor P (2008). Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Centre. Georgia Inst. Technol. 9p.

Ajayi EFG (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015-issue-2-article-4/

Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2810782 or http://dx.doi.org/10.2139/ssrn.2810782

Bassiouni MC (1999). The Sources and Content of International Criminal Law: A Theoretical Framework, 1 International Criminal Law 3-126. 2:353-356

Centre for Strategic and International Studies (CSIS) (2014). Net Losses - Estimating the global cost of cybercrime. Economic impact of cybercrime II. June 2014. pp. 1-24. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Chang W, Chung W, Chen H, Chou S (2003). An International Perspective on Fighting Cybercrime, ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics. pp. 379-384.

Commonwealth, Litigation Practice (1962). Macfoy versus United Africa Company Limited (West Africa). PC 27 NOV 1961

Convention on Cybercrime (2001). Summary of the treaty, European Convention on cybercrime. Available at: ftp://ftp.freenet.at/privacy/gesetze/europarat-cybercrime-summary.pdf

Encyclopedia of Library and Information Science (1977). The modern age regarded as a time in which information has become a commodity that is quickly and widely disseminated and easily available especially through the use of computer technology. Available at: http://www.merriam-webster.com/dictionary/Information%20Age

Ernst, Young (2003). Fraud: Unmanaged risk. 8th global survey. Global investigations dispute advisory services, South Africa. Available at: https://www.whistleblowing.com.au/information/documents/EY8thGlobalSurvey2003.pdf

Hawes J (2014). “2013 An Epic Year for data breaches with over 800 Million records lost.” Naked Security, February 19, 2014. Available at: https://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

International Telecommunication Union (2009). Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Sector. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

KPMG (2001). Global efraud Survey, KPMG Forensic and Litigation Services. Available at: https://home.kpmg.com/xx/en/home/services/advisory/risk-consulting/forensic.html

McGuire M, Dowling S (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom, October. 30p.

Miquelon-Weismann MF (2005). The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?, 23 J. Marshall J. Comput. Info. L. 329.

Nicholas CAMQC (2008). Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities, International Association of Prosecutors, Singapore. Available at: http://www.odpp.nsw.gov.au/docs/default-source/speeches-by-nicholas-cowdery/emerging-trends-in-cyber-crime.pdf?sfvrsn=2

Oxford Dictionary of Law (2002). Oxford Dictionary of Law 5th Edition p. 132, 149. Available at: http://www.fd.unl.pt/docentes_docs/ma/wks_MA_21613.pdf

Paganini P (2013). InfoSec Institute 2013 Cost of cybercrimes http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/

Sieber U (1997). Memorandum on a European Model Penal Code. P. 2.

United Nations Office On Drugs And Crime (2014). United Nations Convention Against Corruption. Available at: https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

Uniterd Nation Human Right (2005). Ratification of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. Available at: http://www.ohchr.org/en/hrbodies/cat/pages/catindex.aspx

Uniterd nations educational scientific and cultural organization (1954). Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention 1954. The Hague, 14 May 1954. Available at: http://portal.unesco.org/en/ev.php-URL_ID=13637&URL_DO=DO_TOPIC&URL_SECTION=201.html