THE PRINCIPLE OF LEGALITY OF CRIMES AND PUNISHMENT MIGRATES TO CYBERSPACE: AN APPRAISAL OF THE CAMEROONIAN EXPERIENCE

Written by ***Patricia Samkia Asongwe***

* Lecturer, Faculty of Laws, University of Yaounde, Cameroon

ABSTRACT

The general principle in criminal justice is that a conduct is criminal only when it is formally declared so by a particular substantive criminal law. This paper appraises how this principle is in Cameroon Cyberspace. The paper does so by reading of published records, academic document and internet search. The results reveals lack of effective criminalisation of cyber conducts would render Cameroon a safe haven for cyber criminals. The paper provides a blue print for judges, researchers and netizens. The paper equally provides a standard for fighting cyber criminality at cross- border level.

Keywords: Cameroon, Criminalisation, Cyber Offenses, Cyber Code

INTRODUCTION

Cyberspace invalidates the very basic tenets on which traditional law is built. Reliance on Cameroon's Penal Code to sanction some types of online illegal activities and the weakness of existing policies and laws, especially in the case of Cameroon provided opportunities for criminals to exploit e-security vulnerabilities, pose new challenges for criminal justice, criminal law, and law enforcement[1], thereby creating impunity and insecurity in the country. The manifestation of cybercrimes, its far reaching and potentially devastating capacity for harm caught the government of Cameroon off guards, and led to Cameroon being considered the world's riskiest zone for net users; as there was lack of protection for the state, individuals and property. It was therefore not surprising that in January 2010 the country was cited as the world's riskiest destination for Internet surfers with more than a third (36.7%) of websites hosted in Cameroon being suspicious. [2] In reaction to this accusation, the government was compelled to address the need for new legislation for the "information superhighway".[3]

Against this background, the country through its Ministry of Post and Telecommunications and the National Agency for Information and Communication Technologies advanced a bill to parliament that allowed them to set up a cyber-police force, define major crimes, and determine legal procedures to help fight cybercrime. Also, the Cameroonian Parliament passed for a bill to fight the alarming rate of cybercrime in the nation in and it was promulgated into law in December 2010[4]. However, such efforts have been largely ineffective at curbing cyber crimes.[5] Proof of this is that, in spite of the enactment of the Cyber Code, a World Bank report still points out that Cameroon is ranked as the riskiest nation in the world for online trade.[6]

---

[1]Longe, O. Longe, Ngwa; Wada & Mbarika, "Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives." Journal of Information Technology Impact 9(3),(2009) at 112-117

[2] Patricia Asongwe. "A Model Legislative And Regulatory Framework For Cybersecurity In Cameroon." First Commonwealth Telecommunication Organisation Cybersecurity Forum. (London ,2010)

[3] Many of the legal challenges facing prosecutors in their pursuit of cybercriminals can be illustrated by the destructive career of the ''Love Bug Virus''. See Leyden ,J " Love Bug Threatens Email Servers New York Times, June 2005, assessed 25th March, 2009 <http://www.vnunet.com/news/1100661.

[4] Solomon Tembang Mforgham "Youth use social networks such as Facebook, Hi5 to rip-off their victims with false profiles." Africa News Reporter (2010 Buea, Cameroon)

[5] Law n° 2010/021 of December 21st 2010 governing electronic commerce in Cameroon .

[6] 2013 World Bank Report

This concern is even more sickening when literature indicates that, Cameroon is one out of the top ten countries in the world with a high level of cybercrime prevalence.[7] This rate of cybercrime prevalence triggers a need for the birth of an effective means of fighting against cybercrimes in Cameroon.[8]

THE OBJECTIVE OF THE PRINCIPLE OF CRIMES AND PUNISMENT

The principal aim of criminal law in general and in particular the objective of legality of crimes and punishments is to recompense offenders by sanctioning with a given number of imprisonment terms to ensure the peaceful co-existence of the society and prevent other potential criminals from committing same.

A monumental principle in criminal justice is that a conduct is criminal only when it is formally declared so by a particular substantive criminal law.[9] This is a concept that has been profoundly embraced by Cameroon criminal law as provided by the Penal Code in its section 9 which spells out the legality of crimes and punishment. Accordingly, there can be no crime without a law for it. To use the famous Latin maxim: nullum crimen sine lege (no crime without law.) One of such concepts is the categorical legal identity that is the minimum identification necessary to react to an intruder with the widest possible range of lawful options.[10] An intruder's true identity may never be known, but his categorical legal identity which is the minimum information necessary to treat him as a terrorist, or a trespasser, or a thief may be defined in advance and uncovered rapidly in the course of an intrusion.[11] This will allow for an immediate, appropriate, and lawful response.[12] Accordingly, no one shall be convicted for acts, except such acts are prohibited in a written law in which a punishment is prescribed.

[7] Eric Akuta E , Ong'oa M and Chanika R.J ''Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice'' Journal of Research in Peace, Gender and Development Vol. 1(4) (2011) at 113

[8] Patricia Asongwe "Cybersecurity and Challenges of Cyber criminality: Response, Strengths and Weaknesses of Cameroonian Law" Ph .D Dissertation, University of Yaounde II, (Yaounde, 2017) at 433

[9] Longe.O et al . supra note I at 120-125, 137-139

[11] Ulrich Sieber Legal Aspects of Computer Related Crime (Wiley and Sons Ltd Great Britain,1998) at 25 -27

[12] F. Lawrence Street and Mark P. Grant, *Law of The Internet* Lexis. (Nexis New York NY. 2001) at 235-238.

JUSTIFICATION FOR THE MIGRATION OF THE CONCEPT OF LEGALITY OF CRIMES AND PUNISHMENT TO CAMEROON'S CYBER SPACE

The law on cybercrimes, while complex in detail, is based on general principles which should be familiar to technologies responsible for protecting systems of critical importance. The question as to whether a crime has been committed, who is involved and the general anonymity surrounding cybercrimes is a debilitating factor and must be provided by a law.[13]

The absence of express provisions in the Cameroon Penal Code is therefore a hindrance for punishment of online misconduct. Bill no 989/PJL/AN of 2016 amending certain section to the Penal Code seems to provide some hope by stating that significant developments have taken place in the country which have led to changing of the legislature's mind-set, and that behavioural changes inspired or amplified by new information and communication technologies have been noted among the people, including the fact that Cameroon has made some international commitments with regards to ICTs which it must honour. From this provision one would have expected the new version of Cameroon's Penal Code to include cyber offences. Unfortunately, the New Penal Code does not provide for crimes committed in Cyberspace.

The inability of the Penal Code to sanction cyber conducts renders the said law inadequate for the digital environment the country becomes a safe haven for cyber subverts who enjoy impunity, to the detriment of the state, individuals and businesses.[14] Accordingly, the utmost diversity of activities taking place over the net and their growing impact on a variety of national and international issues suggests that country's regulatory and legislative authorities should provide certain basic legislative and regulatory principles capable of orienting legal practice in the country. The conclusion that such a need exists will be made if the following conditions are found: firstly, that there is the need to understand the conventional concept of crime and comparing its incriminating elements with those of cybercrimes, the second task requires an understanding of the nature and problems of criminalising computer and Internet disallowable acts within the

[13] McConnell International Cyber Crime and Punishment? Archaic Law Threaten Global Information World Information Technology and Services (WITSA 2000) at 73

[14] Peter Grabosky, P. Virtual Criminality. Old Wine in New Bottles? (in Legal Studies, vol.10, n. 2, 2001), at 243-249.

national legal system.[15] Thirdly, that there is a need for making standard laws which are a prerequisite for international collaboration in the case of trans-national phenomenon which cannot be effectively dealt with under conventional law.[16]

Accordingly, Law n° 2010/012 and 2010/013 of Dec.2010 does not only serve as the pioneer legal framework outlawing illegal activities against electronic and network infrastructure and the main Legislation that criminalises unauthorised activities in Cameroon's cyberspace,[17] but still remains the only law that outlaws cyber misconduct. [18]

APPLICATION OF THE PRINCIPLE OF LEGALITY OF CRIMES AND PUNISHMENTS TO CAMEROON'S CYBERSPACE

The principle of Legality of Crimes and Punishments is provide in Chapter II of part 111 of the Cyber Code new offences on the misuse, disuse and unauthorised acts with the use of ICTs have been proscribed. Secondly, conventional unauthorised acts have been amended to encompass the use of computer technology. And thirdly, ancillary liability, corporate conduct and sanctions have been established.[19]

New Offences under the Cyber Code

This category never existed before the advent of ICTs and consists of offences committed against the confidentiality, integrity and availability of computer data and systems.[20] Thus, to address the most serious online misconduct, the Cameroonian legislator has proscribed: Illegal access, Illegal interception, Data interference, System interference, Misuse of devices. These offences are examined below;

[15]For the modi operandi, one can differentiate between methods causing physical damage and those causing logical damage. See Carlson Anyangwe. Criminal Law In Cameroon ;Specific Offences (Langaa RPCIG Cameroon 2011) at 125.See also section 278 of the Cameroon Penal Code.
[16] Seiber, U. (1998) supra note 14 at 28.
[17] Patricia Asongwe, "e-Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges" The African Journal of Information & Communication (2012) at 158- 160
[18] Nick Nykodym and Robert Taylor "The World's Current Legislative Efforts against Cyber Crime" Computer Law and Security Report, vol, 20(5) (2004), at 390-393
[19] Gordon, S. and Ford, R. "On the definition and classification of cybercrime" Journal in Computer Virology, n. 2, (2006) at 13-20.
[20] George Fletcher Rethinking Criminal Law. (1978 Boston: Little, Brown & Co.) at 199-202.

Unauthorised access offences

Section 68 of the Cyber Code criminalises intentionally accessing the whole or any part of a computer system, without the right to do so, or the unauthorised access to data.[21] This offence comprise of illegal access to computer system or/and data. Illegal access to computer systems and networks is "computer trespass", cracking or hacking offences.

Hacking threatens the integrity and confidentiality and availability of computer systems and, hence, strikes at the very heart of the modern information society which requires sustained public confidence and trust in the new information and communication technologies and systems. Section 68 of the Cyber Code will therefore allow organisations and individuals to operate their systems in an undisturbed and uninhibited manner[22] Hacking is often times than not a gateway offence to other offences, for instance, unauthorised access to data (as discussed above) or data manipulation. It is not surprising, therefore, that the Cyber Code and all leading international instruments on cybercrime have provisions on "illegal access" to computer systems and data. A distinction should however be drawn between hacking[23] and such other subsequent offences. The offence under discussion has its focus on hacking as an end in itself, and not the other offences that the hacker commits after gaining unauthorised access.

The second element of the offence is that the person must access "data." This also applies if he takes note of any data whilst aware that he is not authorised to access that data and still continues to access that data. Again the law does not supply any statutory definition of data. All that it does is to indicate the required mental element of the offence that is, that the person must be aware of the fact that he is not authorised to access the data and still continues to access it. But as to what activity actually amounts to access, the definition is not helpful. Considering the centrality of that term to this and other offences in the Cyber Code, it is imperative that the law should include a statutory definition of access. Such a definition will greatly improve on the clarity of the relevant provisions. It is equally recommended that the legislature must look at international instruments for a proper and instructive definition of what "access" means for

[21] Note section 68 (2) of the Cyber Code . See also Neal Kumar Katyal ''Criminal Law in Cyberspace ''149 U. Pa. L. Rev. (2001) at 1003, 1013
[22] Note section 68 (2) ibid
[23] Which is an unauthorised access to computers, and tampering with precious confidential data and information.

the purposes of the access offences under the law. Data may be defined as "electronic representations of information in any form."[24]

Also, in cybercrime terminology a distinction is often made between "computer data,[25]" "content data"[26] and "traffic data."[27] The Cyber Code does not specify what type of data should be accessed. This should be interpreted to mean that any of the three types of data are included and, hence, any access to either "computer data," "content data" or "traffic data" that meets the other requirements of the offences is punishable under the section 68.

Furthermore, not every access to data is punishable. To be so, the access must be either without authority or permission or by exceeding authorised access. Lack of authorisation to access data is a key requirement of all access offences. There is nothing to suggest that the words "authority" or permission are being used in any technical sense here. Hence in line with the ordinary principles of statutory interpretation, these terms must be given their ordinary grammatical meanings. And if given their ordinary grammatical meanings, the phrases "without authority" or "without authorisation" essentially mean doing something without the consent of the person legally entitled to give such consent, or without any lawful justification or entitlement. For instance, a technician permitted to access certain parts of a computer system will be held to have committed the offence if he decides to access other parts not authorised to. Even though the initial authorisation was lawful, but by exceeding that authorisation he commits an offence.[28]

It should be emphasised that where a person has authority to access data, therefore, the mere fact that he has put the data to some unauthorised use does not constitute an offence under the law. For instance, a technician is allowed to access data for its repair and he decides to copy it for his private use. In such cases, since the initial access was authorised, he cannot be held to have committed the offence by the mere fact that he decided to put it to an unauthorised

[24] Susan Brenner, Cybercrime And The Law: Challenges, Issues , And Outcome Northeastern University Press (2012) at 211

[25] Richard A. Spinello Regulating Cyberspace: The Policies and Technologies of Control (U.S.A, 2002) at 207-213, 325

[26] This refers to the communication content of the communication.

[27] means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

[28] Brenner, S. (2012) supra note 28 at 260

use.[29]Furthermore, section 68 of the Cyber Code may also be applied to any computer information, programme, access code and command.

Where he or she discloses that data and information to another person not entitled or authorised to disclose to the same he will be liable. It is not a requirement that the person to whom the data is communicated to must do anything with the data, or must have any use with it, all that is necessary is that he must be a person who is not entitled thereto. The disclosure need not be to an identifiable person, it suffices if it is to the general public. A person who leaks information obtained from computers to the general public commits an offence.

To avoid over criminalisation, it is proposed that the offence should be limited to certain categories of data, information, access codes or commands.

Section 68 may include receiving computer data not entitled to.[30] Accordingly a person who knowingly receives data not authorised to receive, commits an offence. At a look, one would say that the offence under section 68 (2) was intended to compliment the offence of unauthorised access or remains in all or part of an electronic communication network or an information system by transmitting, destroying, causing serious disturbance or disruption to the functioning of the said system or network in sub section 1. But the ambit of the two offences implicit in section 68 is surprisingly different: whilst section 68 (1) seeks to punish a person who communicates, discloses or transmits data, information, programme, access code or command without authorisation and to a person not entitled thereto, section 68 (2) is only limited to assess data. It does not punish the one who receives computer information, program, access code or programme.

[29] Street, L.& Grant, P, supra note 15 at 618
[30] Akuta E . et al supra note 10 at 129-137.
[30] Augustine Yanke ."The Policy, Legal, and Regulatory Framework For Cyber security And Cyber criminality In
Africa." Commonwealth International Cyber security Forum (Yaounde,2013)
[30] Philemon Tibad . "Fighting Cyber Criminality To Foster Economic Development In CEMAC Sub- Region ; The Case of Cameroon "A Dessertation Submitted In Partial Fulfillment of The Diplôme D'etude Approfondies (DEA) in Law. Unpublished, (University Of Yaounde II ,2013) at 56 .

The prohibited conduct under 68(1) has few elements: firstly, the person must "receive" data. The word receive must be given its ordinary grammatical meaning. In short, it covers all ways and manner how a person gets possession of something. Secondly, what is received must be data, which should be taken to mean computer data. Thirdly, the person must not be authorised to receive that data. In other words, he must not have the permission of the person entitled to the data to receive the data, and he must not be authorised at law to receive the data. The two are different: a person who is not authorised by the person entitled to the data to receive the data may receive the data without committing the offence if he is legally entitled to the data. For instance, an investigating officer who receives data revealing the commission of an offence from an informer does not commit an offence under the section even though he received the data without the consent or permission of the owner of that data. Lastly, the section requires that the person must "knowingly" receive the data.

Interception offences

The Cyber Code creates an offence for intentionally intercepting non-public transmissions of computer data, including electromagnetic emissions, to, from or within a computer system, by technical means.[31] Section 65 sanctions for from 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to10.000.000 (ten million) CFA francs or both such fine and imprisonment:

(1) Whoever, without any right or authorisation, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device (2) Any unauthorised access to all or part of an electronic communication network or an information system or a terminal device

According to subsection (3) the penalties provided for in Subsection 1 above, shall be doubled where unauthorised access violates the integrity, confidentiality, availability of the electronic communication network or the information system.

[31] See sections 41 to 45 of the Cyber Code. However, exception to this rule is provided in sections 49, 50, 51. See also sections 92 (3) and 245 of the Criminal procedure Code. See also Martin Wasik Crime and the Computer. Oxford: (Clarendon Press,1991) at 178.

Finally, subsection (4) states that whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished in accordance with Subsection 1 above[32].

The conduct proscribed by section 65 is equivalent to the traditional tapping and recording of oral telephone communications.[33] The offence covers all categories of electronic communication like telecommunication, e-mail or file transfer. Further, the offence must include monitoring, surveillance, listening to the content of communications and obtaining the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also include recording.[34] The offence requires technical means.[35] This includes all kinds of technical devices, namely, computer programmes, passwords and codes.[36] The offence covers "non-public" transmissions of computer data, qualifying the nature of the transmission process and not the nature of the data transmitted[37] Despite the data communicated being publicly available, if parties wish to communicate confidentially, the communication is "non-public."[38] This category of offences, involves unauthorised interception of data which is in transit. The data may be in transit within a computer system or between computers. Communication on the Internet, and other similar networks, is essentially through data exchange.[39] Data interception is a major challenge because, often times than not, the transferring of data involves more than one service provider and there are always different points where the data can be intercepted.[40] Illegal interception involves a serious assault on the privacy of computers or network users and erodes the confidentiality of computer communications.

The law offers no statutory definition of interception. However the word "intercept" means to access or acquire the contents of communication through an electronic, mechanical or other device.[41] This covers a wide range of activities including acquiring (or recording) the data,

[32]Unauthorised interception is punished under section 84 0f the Cyber Code.
[33] See the Telecommunications Authority Act 5 of 2000 Section 57. Investigations, intercepting, modifying or interfering with a message sent telephonically is an offence.
[34] See section 49 of the Cyber Code
[35]This on the other hand poses a challenge to law enforcement officers who are yet versed with the use of ICTs
[36] Wasik, M. supra note 37 at 203
[37] Therefore where data is transferred with consent and authority the act is lawful.
[38] Note section 41 of the Cyber Code
[39]Yvonne Jewkes and Majid Yar Handbook of Internet Crime (Routledge, 2010) at 123-125
[40]ibid
[41] Akuta E et al supra note 10 at 336

listening to it, viewing it, copying it or merely monitoring it.[42] Included here are several activities done in respect of data during its transmission.[43]

An interception can happen through an electronic, mechanical or other device. Device means an apparatus which can be used to intercept a wire, oral or electronic communication. A combination of the two definitions leaves us with quite a wide offence, something that borders on over-criminalisation.

The Cyber Code requires that the offence be "without right"[44] Thus, a systems administrator who intercepts data in order to check how the system is functioning would be acting lawfully.

Secondly, the law requires that the interception must be by technical means.[45]

Thirdly, the person must intercept the data during the transfer process. It should be emphasised that the offence does not extend to access to data which is not in transmission but is stored in a hard disk or other storage device.

Lastly, the defendant must act intentionally.

Interfering offences

Section 67 of the Cyber Code outlaws intentionally hindering the use of computer systems, including telecommunication facilities, by interfering with computer data.

Hindering refers to activities interfering with the proper functioning of the computer system, such as, imputing, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. Interfering with computer data, computer systems and computer networks is another major deviant behaviour affecting the integrity, confidentiality and availability of data,

[42]Olumide, O"E-Crime in Nigeria: Trends, Tricks, and Treatment." The Pacific Journal of Science and Technology, Volume 11. Number 1. . (2010) at 94
[43] Ibid
[44] The Cyber Code does not expressly states this, but it is advisable to read this in conjunction with Section 74 of the Cameroon Penal Code. See Anyangwe C. supra note 16 at 512
[45]ibid

computer systems and computer networks. This therefore protects the interest of operators and users of computer or telecommunications systems for their proper functioning.[46]

Also, Section 72, states that whoever without authorization and for financial gain, uses any means to introduce, erase or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in Section 66 .

Hindering the functioning of computer systems is critical; for instance, hindering the functioning of essential service computer systems may have grave implications for the nation.[47] For example, targeting critical infrastructure like energy, broadcasting, transportation and telecommunications may disturb and significantly threaten public administration and society.[48] Therefore offences of this nature are needed to protect Cameroon's critical infrastructure. However, since there are already existing rules and regulations on these infrastructure,[49] the new legislation will take care of attacks against infrastructure that are perpetrated by the use of ICTs.[50] These offences do not cover common activities for designing networks or common operating or commercial practices like testing or protecting the security of systems on the user's terminal if the user gave his consent.[51]

Likewise, modifying traffic data to facilitate anonymous communications (such as anonymous retailer systems activities) or modifying data to secure communications (such as encryption) are not "without right" and therefore are not data interference.[52]

The offences have several elements: firstly, a person must "interfere" with data. There is no statutory definition of the term "interfere" in the cyber code, suggesting that the word must be given its ordinary grammatical meaning. In that sense, to "interfere with" something essentially means to prevent a process, an activity or something from continuing, being carried out or functioning properly. Secondly, and most crucially, the act of interference must cause the data to be modified, destroyed or otherwise rendered ineffective or unfit for its purpose. This is the

[46] The Cyber Code in section 66 (1) punishes with an imprisonment of 2 to 5years or with a fine of one to two million CFA, or both whoever causes disturbance, disruption that renders data inaccessible.
[47] Martin Dodge , Mapping Cyberspace .(N.Y, Routeldge, 2001) at 51
[48] *ibid*
[49] See for example the COBAC Laws on banking,
[50] O. Goldman "New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine" Journal of Strategic Studies, vol.24 (2001) at 36-42.
[51] See section 66 (2) of the Cyber Code .
[52] Note sections 49 - 51 of the Cyber Code .

core of the offence. The words "modified", "destroyed" or "ineffective" must be accorded their literary meanings. It should be remembered that the interest sought to be protected by the offence is the integrity and the proper functioning or use of data. To modify something involves making changes to something, whether positive or negative. Here, therefore, any modification is prohibited.

The offences are equivalent to the real world offences involving malicious injury to property. Thirdly, what is interfered with must be data. All types of data (that is, computer data, content data and traffic data) are covered. Fourthly, the defendant must act 'without authority to do so.' He must lack authority to interfere with the data, that is, to cause data to be modified, destroyed or otherwise rendered ineffective. Lastly, the person must act intentionally.

Generally, interfering with data, a computer program, computer data storage medium or a computer system or cyber extortion which endangers the life, or violates the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons; causes serious risk to the health or safety of the public or any segment of the public; causes the destruction of or substantial damage to any property; causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service; causes any major economic loss; or creates a serious public emergency situation; or prejudices the security, the defence, law enforcement or international relations of the Republic.

Misuse of devices

Some of the cyber offences discussed above require some level of technical knowledge on the part of the cybercriminal on how computers, computer systems, networks and data function, or may require the use of certain technical tools. Not every Internet user can design and deploy a computer virus, hack into a computer system or send spam. Of course not all cybercrimes require any level of technical knowledge, for others all that may be needed is a computer and Internet connectivity. Child pornography, for instance, only requires a sick mind, a camera, a computer and Internet.

For those cyber crimes that require some sort of technical knowledge or tools, there is a black market for technical know-how and tools. Just as there are suppliers of instruments of real-world crime (for instance, a black market for guns or explosives to be used during robberies

and break-ins,) there, too, are individuals out there who supply or trade in the tools for the commission of cybercrimes. Hence, one can see here parallels between this kinds of conduct with what is already an established reality with regards to real-world criminality where there is an established market for criminal tools.

Also, as the technical know-how and the "hacker tools" have become readily available and accessible, cybercrime has spiralled out of control. Any person who wants to acquire them can get them easily. For instance, a person who wants to know how to construct a computer virus can find the necessary information as well as the tools readily available on the Internet. By the end of the day, cybercrimes are committed by persons who knowingly and illegally use those tools. Accordingly, section 84(1) of the Cyber Code states that whoever transmits, without authorization, signals or correspondence from one place to another, using electronic communication equipment's, or any other means defined in Section 82 of the law, shall be punished with imprisonment for from 1 (one) month to 1 (one) year or fine of from CFA 1 000 000 (one million) to 5 000 000 (five million).[53]

Accordingly, it is the conduct (that is, the using, the production, selling, or otherwise making available) of the tools for the commission of cybercrimes that is targeted by criminalisation.[54] The law does not provide the definition of device. However device can be defined as any apparatus or instrument which is capable of being used to intercept a wire, oral or electronic communication..[55] Criminalisation of computer misuse tools is in order to target acts preceding offences such as "hacking" and to prevent the creation of black markets in such items.[56] However, in order to prevent over criminalisation of unknowing possession, or possession with legitimate intent, of computer misuse tools, the law requires a specific intent of use for the purposes of an offence.

The offence does not cover devices designed or adapted for legitimate use (such as tools meant for testing and protecting the security of systems.[57] Thus, Cameroon prohibits intentionally and without right, producing, selling, obtaining, possessing, distributing or supplying such devices,

[53] See section 84(2) which provides for a confiscation of such a device by the court
[54] See sections 74(1) of the Cyber Code.
[55]Smith, R. Grabosky, P. and Urbas, G. Cyber Criminals on Trail (Cambridge: Cambridge University Press,(2004). at 123-130.
[56] Ibid p. 132
[57] Rogers Alunge, The Legal Response by Cameroon and Regional Communities to Cybercrime; . (Lambert Academic Publishing . 2015) at 252.

which are designed primarily for use in committing cybercrimes. The criminalisation of such conduct has obvious preventive advantage, just as is the case with the criminalisation of possession of housebreaking or forgery in real-world crimes.

It is a further requirement that the production, selling, offering for sale, procuring, designing, adapting for use, distribution and possession of the prohibited items must be done "unlawfully". Where, however, the law specifically allows a person to overcome security measures that protect data or access thereto, he cannot be said to have acted unlawfully. For instance, cyber inspectors acting within the legal powers conferred on them under section 49 which allows them to have access to data, cannot be said to be acting unlawfully.

It may be argued the offence is unnecessary because the targeted conduct is covered by the offence of unauthorised access to data under section of the law. Hence, a person who utilises any device or computer program in order to unlawfully overcome security measures designed to protect data or access to data, which is the proposed offence under section 65 commits the offence of unauthorised access to data or an attempt to commit the offence of unauthorised access to data. However, a possible justification for the offence would be that the use of a device or computer program to overcome security measures evinces a higher degree of criminal determination.

Traditional Offences Committed In New Ways Under The Cyber Code

This category addresses offences that have existed under the Penal Code but whose sanctions are now inadequate to prosecute because of the introduction of a new element (ICTs). Thus, the 2010 law proscribes: computer-related forgery, computer-related fraud, computer-related private indecency, computer-related extortion, child pornography, copyright infringement, and hate speech.

Online forgery

The Cyber code outlaws intentionally and without right inputting, altering, deleting, or suppressing computer data, resulting in unauthentic data that is intended to be considered or acted upon for legal purposes as if it were authentic, whether or not the data is directly readable

and intelligible.[58]This is in line with the provision of the Penal Code.[59] Computer-related forgery therefore involves unauthorised acts creating or altering of stored data to acquire a different evidentiary value for legal purposes, relying on the authenticity of information in the data to deceive.[60]

Computer-related fraud

The traditional sanction for fraud[61] has been amended by section 72 of the 2010 law. This section criminalises intentionally and without right causing loss of property to another, fraudulently or dishonestly intending to obtain an economic benefit for oneself or another, without right, by: inputting, altering, deleting or suppressing computer data; or interfering with the functioning of a computer system.[62] Traditional fraud offences which often require the direct deception of a "person" and may suffer challenges in their extension to acts committed through the manipulation of a computer system or computer data.[63]

Cameroon's traditional fraud provisions require deceiving a human being.[64] Since deceiving a computer is quite impossible within this meaning the new law has added the electronic element into traditional fraud provision.

A typical example of online fraud is stock fraud or online securities fraud. To constitute an offence, the defendant must use computer network as a medium for any illegal activity, trade or fraud.

The essence of sections 72 and 73 of the law is to eliminate the use of the ICT as a medium for illegal activities, illegal trade and fraud.

[58] According, section 73 (1) of the Cyber Code levies a fine of 25 to 50 million francs cfa or imprisonment of 2 to 10 years or both fine and imprisonment on anyone that uses an information system or a counterfeit communication network to falsify payment, credit or cash or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card.
[59] See articles 312-315
[60] See section 73 (2) of the Cyber Code
[61] See sections 160-168, 318 of the Penal Code
[62]See also article 8 of the Convention .
[63] Dodge supra note 51 at 184

[64] See sections 332, 333, 336 of the Penal Code

Online extortion

Online extortion involves transmitting a communication that threatens to damage a computer, in order to obtain unlawful proprietary advantage by undertaking to cease such action or to restore the damage caused. [65]The traditional elements for extortion still apply for computer-related extortion, namely: unlawfully applying pressure, inducing submitting to the demand; and, intending to obtain some advantage. Cyber criminals use extortion as a new threat by stating that they will crash computer systems if their demands are not met.

Online child pornography

The Cameroon Cyber Code has similarities with the legislation of other countries in dealing with online child pornography offences .[66] The section intends to criminalise the production of pornography for the purpose of its distribution through a computer system; the offering, distribution, transmission or procuring of pornography through a computer system; and the possession or storage of pornography in a computer system or computer data storage medium. The law targets both child as well as adult pornography. In effect, the sections will make it an offence for any person to produce, distribute, transmit, or make available pornography through a computer system and also possess any pornography in any computer data storage medium, including personal computers. It is important that the extent of the criminalisation of pornography under the law be properly understood and appreciated. The law does not only include the obvious explicit films that are made available on a commercial scale, but also any privately produced, distributed or possessed material that visually depicts images of a person engaged in an explicit sexual conduct. A video, drawing, painting, picture, or even presentation or depiction of people having sex or sexual organs will be deemed pornography. It qualifies as pornography whether it is held privately or displayed or communicated to the general public or a few people. A picture of oneself naked and stored in one's personal computer to which no other person has access is pornography for the purposes of the offence under the law. Such a person will be held liable under the section; so too is a couple who take their own pictures nude or having sex. It is this wide criminalisation of private possession of certain materials (most

[65] See section 90 of the Cyber Code

[66] The importance of protecting children in the digital environment was the concern of the Secretary General of UNICEF as stated that this is an era in which children must be given more online protection not only as a matter of law but as a matter of their right to self integrity.

importantly, which do not amount to child pornography) by fully grown up adults that is problematic here. The Cyber Code punishes the production, distribution or possession of pornographic materials.

One feature that has made the Internet so famous is that it allows users to create and share different kinds of media. It is also possible to access vast quantities of information stored in computers located all over the world, retrieve data and place it in one's own computers. All kinds of materials are uploaded, shared and accessible on the Internet today and some of that material is pornographic. Furthermore, Cameroon has not only criminalised procuring and possessing child pornography, but attached criminal consequences to each participant's conduct in the chain from producing to possessing. This is important in curtailing the production of child pornography.

The definitional elements of the offence are three: firstly, the defendant must either produce, offer, make available, distribute, transmit, procure, or possess pornography.[67] Those words must be given their ordinary grammatical meaning. Secondly, and crucially, the defendant must produce, offer, make available, distribute, transmit, procure, or possess "pornography." To amount to pornography, therefore, the material must visually depict images of a person engaged in a sexual activity.[68] Thirdly, the defendant must produce, offer, make available, distribute, transmit or procure the pornography through a computer system. For possession, the person must possess the pornography in a computer system or a computer data storage medium.

Intellectual property offences

According to section 4 (52) of the Cyber Code intrusion by intellectual challenge comprises of an intentional and unauthorised access to electronic networks or an information system. The Cyber Code criminalises intentionally committing offences related to infringements of copyright and related rights for commercial purposes through a computer networks.[69] According to section 65(4) whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished

[67] Melissa Hamilton "The Child Pornography Crusade and Its Net-widening Effect." Cardozo Law Rev, 33(4) (2012) at 167-
[68]Ibid at 168
[69]See Section 86 (1) and (2) and section 87 of the Cyber Code .

with 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to 10.000.000 (ten million) CFA francs or both such fine and imprisonment.[70]

Although traditional law punishes infringement of intellectual property rights,[71] reproducing and disseminating Intellectual property electronically is fairly easy and frequently occurs without the copyright holder's consent, hence the need for redefinition of criminalisation. Thus the law seeks to protect the unauthorised copying, reproducing and disseminating of copyright and related rights on computer networks.

Cyber harassment

Section 77. (1) of the Cyber Code sanctions cyber harassment with a penalty of from 2 (two) years to 5 (five) years or a fine of from 2 000 000 (two million) to 5 000 000 (five million) CFA francs or both of such fine and imprisonment." This deals with Offences which cover incitement to racial and religious hatred, as well as ethnic issues.[72] The provision applies to speech intended to create fear of future harm. Thus the law applies to a broad criminalisation covering "making insulting remarks" about a group of persons on the grounds of race, religion or belief, sex, sexual orientation or disability.

The increasing use of social media has resulted in a number of recent cases involving the Internet that raise hate speech issues, including video containing anti- Islamic content and Twitter messages inciting racism.[73] While ICCPR Article 20 imposes an obligation to combat such expression, it is important to recall that ICCPR Article 20 requires a high threshold. However restrictions must meet the three part test of legality, proportionality and necessity.

In assessing the severity of the hatred and hence the justification for restricting freedom of expression, a threshold assessment should include: (i) the context of the statement; (ii) the position or status of the speaker; (iii) the intent (negligence and recklessness should not

[70] See section 65 (1)
[71] See the OAPI (African Intellectual Property) Laws and the World Intellectual Property Organization(WIPO), See also section 3 of the 2000 Law on Copy Right in Cameroon
[72] See the United Nations Office of the High Commissioner for Human Rights, 2012. Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
[73]Stalin Halpin, ''Racial hate speech: A comparative analysis of the impact of international human rights law upon the law of the United Kingdom and the United States.'' Marquette Law Review (2010) at 463

suffice); (iv) the content or form of statement; (v) the extent of the statement; and (vi) the degree of risk of resulting harm.

Online defamation

In connection with defamatory offences, Section 78 provides that whoever uses electronic communications or an information system to design, publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true shall be punished with imprisonment for from 06(six) months to 02(two) years or a fine of from 5,000,000(five million) to 10,000,000(ten million) F CFA or both of such fine and imprisonment. The penalties provided for the above shall be doubled where the offence is committed with the aim of disturbing public peace.

Online infringement on personal data and privacy

Section 80 of the Cyber Code criminalises an unauthorised use of ICTs to receive the privacy and personal data of another person.

Also infringement on personal data and Privacy is outlawed by section 81 (new) (1) which states that whoever uses an electromagnetic, acoustic, mechanical or any other device wilfully to intercept a private message and divulge he shall be punished with the penalties provided for in Section 80 .

However section 81 (new) (2) states that the sanction shall not apply to is to ;

(a) persons who have obtained the express consent of either the sender of the private communication or its recipient;

(b) persons who intercept a private communications at the request of a judicial authority in accordance with the laws in force;

(c) persons who provide electronic communication services to the public and who intercept a private communication in any one of the following cases.

Section 83 of the Cyber Code provides the penalty for privacy and personal data infringement by stating that whosoever knowingly uses the services obtained through the offense referred to

in Section 82 (1) above shall be punished with imprisonment for from 6 (six) months to 2 (two) years or fine of from CFAF 1 000 000 (one million) to 5 000 000 (five million) or both such imprisonment and fine. And that such penalty shall be doubled in the event where such use is open to the public.

Online private indecency

This offence relates to the criminalisation of fully grown up adults for adult pornography for their own private consumption.[74] Whilst the Penal Code punishes some conduct merely because of its immoral nature[75] it is not every conduct that the society considers immoral that must be criminalised. One of the fundamental principles of criminal law is that of minimalism. The minimalist principle states that criminal law is not the only form of social control. Other forms of social control recognised by the principle include morality, social convention, culture, religion, peer pressure, and others. Now, the principle states that criminal law should be used to control or prevent conduct only when the other forms of social control have failed. Most importantly, criminal law should be reserved for the most serious of harms. The less serious harms should be left to other forms of social control or even civil law or administrative regulation. [76]

However, this sanction does not apply where such recording and publication fall under the normal exercise of profession aimed at informing the public on where they are carried out in order to be used as evidence in Court in accordance with the provisions of Criminal Procedure Code**.**

Online obstruction of justice

By virtue of section 61, Agency personnel and experts of corporate bodies in charge of security audits who without any authorization, disclose confidential information that they are privy to on the occasion of the security audit, shall be punished with imprisonment for from 03(three) months to 03 (three) years and a fine of from 20.000 CFA francs (twenty thousand) to 100.000

[74]Peter Grabosky Electronic Crime (New Jersey: Prentice Hall 2006) at 167

[75]See section 295 of the Penal Code
[76] See section 75 of the Cyber Code

(one hundred) CFA Francs. Refusal to comply with the summons of authorized officials shall be punished with imprisonment for from (three) 03 months to four years.

Emphasis should be made here that section 61 punishes one of the most common but most devastating offenses touching on a company. This offence constitute one of the most punishable as it does not only deprive the company of some profits but breaches her integrity and can eventually culminate in her winding up.

In the same vein, according to section 61(3) whoever, by any means whatsoever, obstructs, gives incitement to resist or prevent the conduct of investigation provided for in this section, or refuse to provide information or document there to, shall be punished with imprisonment for from 01(one) to 05 (five) years or a fine of from 100.000 (one hundred thousand) to 1000000 (one million) CFA France or both of such fine and imprisonment.

Reading into section 61(1,2, 3) leaves us with an impression that the law is confuse as it punishes to a greater extent the mere acts of inciting, obstructing or preventing the conduct of investigation on the offence contained there in more than even the punishment of the offence itself. Nevertheless, the legislators' intentions in this proviso is legally inferred to be logical in the sense that; most cyber offences have a complicated and complex nature and are rarely reported for investigations to be opened. Not only their nature, but as well, their investigation seems pretty technical and difficult to come by. It is for these reasons that the position adopted by the drafts men to punish the accessory more than the offender remains a lofty one and tenable in the eyes of the law. This hypothesis is further confirmed looking at the additional fresh impetus given by the Penal Code: "an accessory after the fact shall mean a person who after the commission of a felony or misdemeanor shelters an offender or his accessories from arrest or from investigation, or who has custody of or disposes of anything taken, misappropriated or otherwise obtained by means of the offence shall be punished under special provision of the law." The justice in this provision lies in the fact that not only perpetrators of cyber offences are to be punished but also, anybody who sympathies with them by complicating the procedure for prosecution. In so doing, not only would criminal cooperation be discouraged but as well, the cumbersome and herculean task of investigating cyber offences would be reduced, thereby facilitating prosecution of criminals.

Criminalisation of Inchoate Crimes under the Cyber Code [77]

Just like the Penal Code,[78]the Cyber Code provides for attempting, aiding and abetting cybercrimes.[79]

In attaching criminal liability for aiding and abetting, Cameroon by all implications also requires the intention to commit a crime, so that no liability attaches to a person acting without the requisite intent. For example, although transmitting harmful or malicious code through the Internet requires the service provider's assistance as a conduit, a service provider without the criminal intent cannot incur liability under this provision.[80]

Inchoate liability represents a middle ground in a criminal continuum: at one extreme , they are mere thoughts. And criminal law does not, as a matter of general principle, punish people for their thoughts alone, however heinous or immoral those thoughts might be. At the other extreme there is the completed crime which is the legitimate target of criminal law. Inchoate offences are in the middle: they represent a manifestation of the thoughts through some positive act (in the form of an agreement or an attempt) and yet a step from the completed offence.

There are several justifications for punishing inchoate offences, but the most prominent are two: firstly, it has been argued that in terms of moral culpability there is no difference between a person who successfully commits an offence and another who agreed with others to commit an offence or even attempted to commit that offence.[81] They are equally culpable or blameworthy. As Ashworth puts it, there is "no relevant moral difference between an attempter and a substantive offender and they all need to be subjected to the same punitive process."[82] Secondly, the punishment of inchoate offences is justifiable on preventive grounds. People who show a firm intent to cause a substantive harm by agreeing with others to commit a crime or attempt to commit that crime, or incite others to commit a crime pose the same danger to the society as those who succeed. They all engender genuine fear and concern amongst the

[77]This means "just began"
[78] Sections 94 and 95 0f the Penal Code
[79]Sections 74 (2) and 83 of the Cyber Code.
[80]See article 12 of the Convention. The term "person who has a leading position" refers to a natural person in a high position in the organisation, like a director.
[81]Andrew Ashworth "Criminal Attempts and the Role of Resulting Harm under the Code, and in the Common Law" 9 Rutgers Law Journal . (1988) at 725, 733
[82] ibid

citizenry and should be equally prevented or incapacitated. Moreover, the mere doing of the act that creates that fear is a sort of harm in itself that require prevention and punishment..[83]

Section 73.(1) of the Cyber Code expressly punishes inchoate liability with an imprisonment for from 02 (two) to 10 (ten) years and a fine of from 25,000,000 (twenty five million) to 50 000 000 (fifty million) CFA francs or both of such fine and Imprisonment."

Few observations can be made here: firstly, the provision spells out the punishment of only attempts. It does not include the other type of inchoate offences (for example conspiracies) recognised by the Penal Code. Secondly, the provision renders a person who attempts to commit any offence under the law liable to the same penalty applicable to the completed offence.

This shows that the Cyber Code has taken a similar approach, punishing inchoate offences to the same level as the Cameroon Penal Code

Corporate Liability under the Cyber Code

Legal persons are criminally liable under the Cyber Code. Having spelt out the obligations of legal persons in sections 26 to 32, the law goes on to impose sanctions on corporate bodies.[84] Specifically section 64 states that corporate bodies shall be criminally liable for offences committed on their account by their management structures, that the criminal liability of corporate bodies shall not preclude that of natural persons who commit such offences or are accomplices, the penalties to be meted out on defaulting corporate bodies shall be fines of from 5000000 (five million) to 50 000 000 (fifty million) CFA francs and that the penalties provided, notwithstanding one of the following other penalties may equally be meted out on corporate bodies.[85] Sanctions provided for corporate bodies include;

-dissolution in case of a crime or felony punishable with respect to natural persons with imprisonment of 03 (three) years and above and where the corporate body has departed from its declared object to aid and abet the incriminating acts;

[83]Actually, under the Cameroon criminal law, impossibility is not a defence to a charge of conspiracy or attempt.
[84] See sections 60 to 64 of the Cyber Code
[85] See also the principle of vicarious liability

-definitive prohibition or temporary prohibition for a period not less than 05 (five) years, from directly or indirectly carrying out one or more professional or corporate activities;

-temporary closure for a period of not less than 05 (five) years under the conditions laid down in Section 34 of the Penal Code of the establishments or one or more establishments of the company that was used to commit the incriminating acts;

-barring from bidding for public contracts either definitively or for a period of not less than 05 (five) years;

-barring from offering for public issues either definitively or for a period of not less than 05 (five) years;

-prohibition for a period of not less than 05 (five) years from issuing cheques other than those to be used by the drawer to withdraw money from the drawer or certified checks or from using payment cards;

-seizure of the device used or intended to be used in committing the offence or the proceeds of the offence;

-publication or dissemination of the decision taken either through the print media or through any electronic means of communication to the public.

Accordingly legal persons are liable for activities committed by physical persons acting for and with the authority of the legal persons. [86]However five conditions must be met:

-the offences described as cybercrimes must have committed;

-the offence must have been committed for the legal person's benefit;

-a person in a leading position must have been committed the offence (including aiding and abetting);

[86]See the Convention Art 12(1). These pre-conditions demonstrate that the person acted within the scope of authority to engage the legal person's liability.

-and the person in a leading person must have acted based on: the legal person's power of representation;

-have the authority to take decisions on behalf of the legal person; or an authority to exercise control within the legal person.[87]

Additionally, the law attaches liability to a person in a leading position failing to supervise an employee or the legal person's agent, with the failure facilitating the employee's or agent's committing a cybercrime. Failure to supervise must be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing an offence on the legal person's behalf. Such appropriate and reasonable measures could be based on factors like the business type, its size, the standards or the established business best practices, and others. [88]

Cameroon attaches criminal, civil or administrative liability to the legal person.[89] However, such liability must not prejudice the natural person's liability for committing the offence.[90]

APPRAISAL AND CONCLUSION

Generally, the Cyber Code has created a system of criminal offences and sanctions with regards unauthorised conduct in cyber space, but compatible with existing national legal system.[91]

Thus the law is still partly guided by some traditional concepts that exist under Cameroon's Penal Code[92]. Otherwise stated, cyber offences in the Cyber Code are not applied or interpreted by the criminal justice system in isolation, but rather with reference to rules that apply to all offences, such as rules on complicity, attempt, omission, state of mind, and legal defences. In this context, the Cyber Code limits criminalisation to acts committed with the intent to commit,

[87]See Art 12(2) of the Convention
[88] See the Explanatory Report para 125.
[89]See Tesco Supermarkets Ltd v. Nattrass [1972] AC 153.
[90]See, for example, United States v One Parcel of Land, 965 F.2d 316 (7th Cir 1992).
[91] See especially the sanctions on computer-related conventional acts like fraud, forgery, harassments.

[92]Hence, the conduct must be illegal (unauthorised) and intentional. See Anyangwe supra note16 at 125

or facilitate the commission of an offence.[93] Accordingly, the element of mens rea, also referred to as "guilty mind," "mental element" or "fault requirement," has migrated from offences provided in Cameroon's Penal Code to offences in the Cyber Code.

However, when it comes to "state of mind", exercise must be carried out with caution, because of the potential broad reach of some cybercrime offences, for example, illegal access to computer data. Further, although all the offences contained in the Cyber Code must be committed "intentionally", for criminal liability to apply in certain cases an additional specific intentional element forms part of the offence, for instance, with regards to computer-related fraud, the intent to procure an economic benefit is an additional constituent element.[94] Unfortunately, the law fails to provide the exact meaning of "intentionally."[95] It is therefore important that the mental element of cybercrimes be clearly defined by a text of application.

The Cyber Code provides special protection to such infrastructure by providing sanctions for illegal access, interception or interference to computers linked to the functioning of critical infrastructure. Many such offences overlap with other possible, separate, offences, such as illegal data interference or system damage. The most common aggravating circumstance is the involvement of computers to the functioning of critical infrastructure such as banking, telecommunications, health services, transport services.

Specifically, Legality of crimes and punishment under the Cyber Code has the following advantages:

- It defines and classifies behavior in Cameroons cyber space;
- It broadcasts the laws so that no-one may have the excuse of ignorance, and disposes of those who will not obey.
- It leads to an increase in criminal laws and their adaptation to the social structures of modern societies.
- The concept has become an important industry in crime control.

-The concept in very instrumental in the retribution, deterrence, incapacitation, rehabilitation and restoration in cyber space.

[93] The law does not provide for civil wrongs.
[94] Draft African Union Convention (Art. III-23); COMESA Draft Model Bill. See Longe supra note 1 at 124
[95] Wayne R. LaFave Criminal Law. (3rd ed. St. Paul: MN.(2000) at 224-234.

Lastly, by proscribing acts that were not formerly crimes, Cameroon has broken new ground for sanctioning crimes in an evolving and pervasive criminal ecosystem..

However, the concept is being challenged by the pervasive, borderless and evolving nature of crimes in cyber space not without challenges.[96]. Cybercrimes differ from real-world crimes in four respects:(1)they are easy to commit (2)they need few resources compared to the amount of damage potentially caused;(3) they can be committed in any jurisdiction without the perpetrator necessarily being at the scene of the crime; and (4)they are often not clearly defined as criminal.[97] Gelbstein drastically sums up the nature of cybercrime by stating that cyber crime is a separate and distinct phenomenon from traditional crime with material differences that require a new approach in the imposition of criminal liability and in the administration of criminal justice.[98] Underlying this belief is the perception that virtual crimes are actions in cyberspace, with its shared virtual community and virtual citizens, and consisting of a mixture of real identities, alter egos, clones and even virtual beings. Hence, it is fundamentally different from crimes committed in the physical world.

This new phenomenon challenges the Cameroonian law authorities are in a majority not versed with the various offences in cyber space. As a consequence, most cybercrimes go unpunished, and Cameroon becomes a safe haven for cybercriminals.

Also, criminalising online conducts without doing same offline may infringe the principle of offline/online consistency because, in effect, it will render an illegal activity criminal merely because it was committed through the medium of the Internet and yet the same illegality committed off-line will either not be criminal or will only be punished once. To say that we should punish the commission of an illegality merely because it is committed through one medium and not another is nonsensical because it does not in any way reduce the illegality in the first place. It will just be pushed from the medium it is criminalised to the other medium. It is like punishing the cutting of trees using an axe and not using a sword. People will just start cutting trees using swords. No one would take such a law seriously. This article therefore recommends that acts and omissions that are illegal in cyber space must also be illegal offline.

[96] See Section 79 which sanctions by virtue of section 295 of the Penal Code
[97]Boateng R. Longe O, and Mbarika V. "Cybercrime And Criminality In Ghana; Its Forms And Implication." Proceedings of The Sixteenth America's Conference On Information Technology (2010)
[98] Gelbstein, E. and Kamal, A. "Information insecurity" in Pauline C Reich. Ed 3 Cybercrime and security (2005) at 5.

Furthermore, the Cyber Code is fraught with difficult concepts and complex terminologies that may hinder effective implementation of the concept. This paper suggests the enactment of a text of application that would include following;

-An adequate definition of concepts and terminologies used in the law.

-Robust and flexible provisions that will ensure its applicability to changing technology and techniques used to perpetrate criminal offences as far as possible. If technologically neutral provisions are not possible for a particular subject matter, then fast and reactive amendments or updates to the law are the only other alternative.

Finally, since most cyber crimes have an international element, and with a view to obtaining effective migration of legality of crimes and punishment to cyber space the text of application of the Cyber Code must be standard in other to ensure harmonisation of cyber offences.