MUTUAL LEGAL ASSISTANCE IN CYBER CRIMES: ISSUES AND CHALLENGES FOR CAMEROON'S LAWS

Written by *Ngeminang Patricia Asongwe*

ABSTRACT

Cameroon's laws and their enforcement are formally bound to nationally defined borders, where a single transmission of computerised information over a network may passes through a dozen or more types of carriers, such as telephone companies, satellite networks, and Internet service providers, thereby crossing numerous territorial borders and legal systems. Consequently, it has become a vested interest of the Cameroon government to enact legal frameworks that offer a guideline on which the country can cooperate in the area of Mutual Legal Assistance with other countries and organisations on issues of cybercrimes. The reading of existing literature and consultation of experts on the subject reveal that the laws on digital trans border investigative methods in Cameroon are not sufficiently effectively enforced. The article suggests that there should be an review of the Cyber Code and also capacity building from law enforcement agents.

Keywords: Cyber Code , Cameroon, Mutual Legal Assistance

1 INTRODUCTION

Cybercrime is typically global in nature, with malicious cyber actors operating all over the world and transcending geographical boundaries. [1]

In order to effectively combat this threat, there is a need for increased international enforcement cooperation.

International cooperation in cyber criminality in Cameroon preceded by the creation of the National Information and Communication Infrastructure (NICI) in 2001 to wage a 10 year fight from 2004 to 2015 against cybercriminals in Cameroon.[2] By 2006, the decree

[1] Ashworth, A. (1995) *Principles of Criminal Law Oxford*: Clarendon Press: p.83

[2] This organ focused on the then prioty areas as e-government, e- commerce and ICTs services. These indicators are derived from the World Economic Forum's Executive Opinion Survey. http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf

ISSN 2581 3382

that created the NICI was revisited by the Presidency, partly due to the rapid diffusion of cybercrime, and also the inability of NICI to curb the increasing wave of cybercrimes. The issue of cyber criminality was therefore taken over by the Ministry of Post and Telecommunications.

Two things were amended in the 2006 decree; the name was changed to the National Agency for Information and Communication Technology, (ANTIC) and the agency was placed directly under the auspices of the Presidency in association with the Ministry of Post and Telecommunications, which had overseen the creation of NICI towards the fight against computer crime.[3] However, it should be noted that although international cooperation is not a new government policy, it is only in 2010 that Cameroon promulgated a law that befits the scope and nature of online security threat. Accordingly, the Cyber Code [4]provides Mutual Legal Assistance procedures as one of the mechanisms[5] for dealing with complex jurisdictional issues, and the development of new procedures to challenge cross border cyber criminality. Accordingly, the law provides the necessary mechanism to identify perpetrators across borders anywhere in the world, and to investigate and secure electronic evidence of their crimes so that they may be brought to justice in any jurisdiction with fairness and compliance with human rights standards.[6]This article states the justification for providing a legal framework on Mutual Legal Assistance , explores the procedures and enforcement under Cameroon's Cyber Code and evaluates the effectiveness of the highlighted mechanism**.**

II. THE CONCEPT AND RELEVANCE OF MUTUAL LEGAL ASSISTANCE

Mutual legal assistance in criminal matters (MLA) deals with the mechanisms of gathering assistance abroad, from foreign authorities. MLA is particularly important in investigations concerning cybercrime and cyber-enabled crime (meaning crime committed by means of ICT) because these type of offences are almost by definition transnational. On the one hand, cybercriminals can commit their offences from nearly any location, (mis)using globally available telecommunication technologies and networks systems. On the other, their acts often

[3] Asongwe, P. (2010) "*A Model Legislative And Regulatory Framework For Cybersecurity In Cameroon*." First Commowealth Telecommunication Organisation Cybersecurity Forum. London

[4] This is Law n°2010/012 of December 21st 2010 regarding Cybersecurity and Cybercriminality amended and supplemented by Law No 2015/006 of 20 April 2015

[5] The other being Convention

[6] See part IV of the Cyber Code

ISSN 2581 3382

affect individuals, companies and/or public entities in various countries across the world. In order to fight such crime, international cooperate on is thus, indispensable. Mutual legal assistance has the effect of providing common set of investigative powers which are important since those who commit cybercrime offences commonly seek to exploit this, undertaking their activities in one country but delivering the effect in another jurisdiction.[7] MLA activities include: extradition, voluntarily disclosing information, confidentiality and the limitations on using shared information, communications between central authorities, requests for preserving, accessing and disclosing stored data, interception of data trans-border access to stored computer data.[8] Such legal assistance is important since in the virtual world borders do not exist, and this is an attractive characteristic for criminal activity.[9]

However, in contrast with the rapidness of cyber(-enabled) criminal activity and the volatility of data needed for the prosecution of cybercrime, the existing mutual legal assistance framework in Cameroon is still quite slow and burdensome.

III JUSTIFICATION FOR MUTUAL LEGAL ASSISTANCE IN CYBER CRIMES

Generally, cybercrimes have an international dimension in two obvious respects. Firstly, cybercrimes generated from with a particular state often has serious impact upon states.

Secondly, it is now apparent that cybercrime cannot be resolved by states acting individually, cybercrime is not limited by so-called geographical boundaries. Hence, cooperation between should be a golden rule. However, the issue becomes more complicated when cybercrimes are committed anonymously and it is quite impossible to determine from which country, or cybercriminals, a particular form of cybercrime is committed. Given that no single country is immune to such cyber-threats, international collaboration is a necessity.

The global reach, speed, volatility of evidence, anonymity, and potential for deliberate exploitation of sovereignty and jurisdictional issues which are characteristics of cybercrimes pose challenges for the detection, investigation and prosecution of online misconduct.[10]

[7] This goes to reiterate the fact that appropriate responses must be standard and interoperable .
[8]Alunge, R. (2015) The Legal Response by Cameroon and Regional Communities to Cybercrime. Lambert Academic Publishing pp 654-658
[9] ibid. P.670

[10]Gibson, W. (1984) *Neuromancer New York*: Ace Books P.325

ISSN 2581 3382

Also, the menace of cybercrimes have collapsed and literarily paralysed the efficiency of Cameroon's Penal Code and Criminal Procedure Code. The limitations in national conventional legal frameworks impede efforts to enforce to curb crimes in cyberspace.[11] Importantly, Cameroon cannot shut down its borders to incoming cyber threats.[12] Cybercriminals are not and cannot be bound to geographical locations.[13] Laws and technological measures can no longer be limited to national boundaries.[14]

Further, cybercriminals are already exploiting vulnerabilities and loopholes in national and regional legislation.[15] There is evidence that they are shifting their operations to countries where appropriate and enforceable laws are not yet in place, so that they can launch attacks on victims with almost total impunity, even in those countries which do have effective laws in place.[16]

Further, Cameroon's laws are drawn up so as to be enforceable in well defined geographical boundaries that are either national or regional. Even if all countries introduce legislation, cybercriminals cannot be easily extradited between countries where the cybercrime unless these legal frameworks are interoperable.

To put in place a global solution to address those challenges, it is vital that Cameroon arrives at a collaborated fight.

There has been significant changes in the level of sophistication of cyber threats.[17] With the spread of networks of hijacked computers over different countries, criminals can launch cyber

---

[11] Sieber U. (1998). *Legal Aspects of Computer-Related Crime in information Society, The COMCRIME-Study for the European Commission.* See also .Sieber, U. (1996). "*Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society*." Statement for the Hearing on Security in Cyberspace of the United States' Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July

[12]Goldsmith, J. (2005). "*The Internet and the Legitimacy of Remote Cross-Border Searches*." Chicago Public Law and Legal Theory Working Paper, number 16, The Law School, The University of Chicago. p.221

[13]Ibid See also Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10

[14] See Goldsmith, J. op cit p. 225 . See also G8, Okinawa Charter on Global Information Society, Okinawa, 22 July 2000

[15] Calderoni, F. op cit p 220

[16] Ibid

[17] Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network,

ISSN 2581 3382

attacks using a decentralised model based on peer-to-peer arrangements, making it difficult for any single national or regional legal framework to deal adequately with this problem. Such far-reaching challenges can only be addressed at the global level.

This makes it very difficult to pinpoint one geographical location as the origin of these attacks, and consequently makes it difficult to identify them and shut them down. This shift strategy is not just aimed at delivering spam with more dangerous payloads but can also be used to disseminate inappropriate content, such as child pornography, without the knowledge of the hijacked computer owners that they are hosting and disseminating such content.

Furthermore, toolkits and applications for phishing, spam, malware, scareware and snoopware can today be acquired relatively easily from underground sites or even purchased legally, lowering the financial and intellectual entry barriers to acquiring tools to facilitate unauthorised access to information and communication systems to manipulate or destroy them.[18] Snoop ware is going mobile, threatening user privacy through the possibility of voice/data call monitoring, with devastating consequences, especially for the growing number of corporate users who rely on their smartphones for confidential discussions and data exchanges with their corporate IT systems.[19] With the phenomenal growth in mobile telephony (including smartphones),together with convergence, which is bringing down the walls between networks, cyber threats can now spread easily to all platforms and to all countries .

Finally, there is no existing convention with the particular state .The Cyber Code therefore provides new remedies to sanction complex jurisdictional issues and the development of new procedures through MLA mechanisms which provide solutions to the challenges of cross-border online crimes

Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10.

[18]Sieber, U. (1996). *"Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society*." Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs.

[19] WC Opello W.C. & Rosow J.S. (2004) The Nation-State and Global Order: A Historical Introduction to Contemporary Politics Boulder: Lynne Rienner. P.561

ISSN 2581 3382

Part IV of the Cyber Code provides the legal basis for Cameroon to fight cyber criminality from a global perspective.

IV PROCEDURES AND ENFORCEMENT OF MUTUAL LEGAL ASSISTANCE UNDER CAMEROON'S CYBER CODE

A) Procedures for MLA under the Cyber Code

The Cyber Code provides for procedures when Cameroon is requesting and when Cameroon is requested for MLA as outlined below:

1) Cameroon as the Requesting Country

Section 91 of the Cyber Code provides that unless otherwise provided for by an international convention to which Cameroon is a signatory, requests for judicial assistance from Cameroonian judicial officers to foreign judicial officers shall be sent through the Ministry in charge of External Relations. A request for mutual legal assistance should contain:

-the identity of the authority making the request,

-the subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;

-a summary of the relevant facts, except in relation to the requests for the purpose of service of judicial documents;

-a description of the assistance sought and details of any particular procedure that the requesting State wishes to be followed;

-where possible, the identity, location and nationality of any person concerned and

- the issuing authority with details of the central authority of the requested state, the channels of communication and other relevant information.

However, in case of emergency, requests for judicial assistance from Cameroonian authorities to foreign authorities may be sent directly to the authorities of the requested State for enforcement. The enforcement documents shall be dispatched to the relevant State authorities under the same conditions

ISSN 2581 3382

2*) Cameroon as the Requested Country*

Requests for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities must be presented through diplomatic channels by the foreign Government concerned and that enforcement documents shall be sent to the authorities of the requesting State through the same channel.

The law is to the effect that request for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities shall be subject to an opinion of foreign Government concerned. Such opinion shall be forwarded to the relevant Cameroonian judicial authorities through diplomatic channels.

In case of emergency, requests for mutual judicial assistance from foreign judicial authorities shall be forwarded to the State Counsel or Examining Magistrate with territorial jurisdiction.

B) Enforcement

According to Section 92. (1) Requests for mutual judicial assistance from foreign judicial officers shall be enforced by the State Counsel or Judicial Police Officers or Agents requested for this purpose by the said State Counsel.

The requests shall be enforced by the Examining Magistrate or Judicial Police officers acting on the rogatory commission of the Examining Magistrate where they require certain procedural measures which can be ordered or enforced only during a preliminary investigation.[20]

Request for mutual judicial assistance from foreign judicial officers shall be enforced in accordance with the procedure laid down by the Criminal Procedure Code.[21]

However, where the request for assistance so specifies, it shall be enforced in accordance

with the procedure explicitly indicated by the relevant authorities of the requesting State,

without such rules violating the rights of the parties or the procedural guarantees provided for by the Criminal Procedure Code.[22]

[20] See section 92(2) of Cyber Code
[21] ibid Section 93 (1)
[22] Ibid section 93(2)

ISSN 2581 3382

Where the request for mutual assistance cannot be enforced in accordance with the requirements of the requesting Sate, the relevant Cameroonian authorities shall immediately inform the authorities of the requesting State of such impossibility and specify under what conditions the request may be enforced.[23]

The Code further provide in section 93 (4) that the relevant Cameroonian authorities and those of the requesting State may subsequently agree on the onward processing of the request, where necessary, by subjecting it to compliance with such conditions.

Irregularity in the transmission of the request for judicial assistance shall not constitute grounds for nullity of actions undertaken in enforcing such a request.[24]

According to section 94 (new) where the infringements referred to Sections 92 and 93 above are committed in territorial waters or the continental shelf contiguous with the territory of Cameroon by a member of the crew of a Cameroonian or foreigner ship, they shall fall within the jurisdiction of Yaounde Courts or those of the ;

-port of registry of the ship boarded by the sender;

-first Cameroonian port where the ship anchors or whose territorial jurisdiction extends to the seawater extension of the place of the infringement"

V AN APPRAISAL OF MLA UNDER THE CYBER CODE

The general principle relating to MLA as provided in section 91 is to the effect that MLA can only be applied where there is no existing convention between Cameroon and the other country or organisation. Thus where there is a convention or any bilateral or multilateral agreement referring to cyber criminality, the terms of such an agreement shall prevail. . Thus, according section 91 mutual legal assistance does not substitute a convention. The Cyber Code emphasises that international cooperation should in general be carried out through the application of relevant treaties and similar arrangements. As a consequence, the Cyber Code does not intend to create a separate general regime on mutual assistance. Therefore, the law

[23] Ibid section 93(3)
[24] Ibid section 93(5)

ISSN 2581 3382

applies only in those cases where the existing treaties, laws and arrangements do not contain such provisions on cyber crimes

Section 91 contains a whole set of procedures pointing to the fact that Cameroon shall afford with other countries and organisation the widest possible measures leading to legal assistance in investigations, prosecutions and judicial proceedings in relation to cyber offences, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State . However reliance on the CPC inhibits adequacy of the Cyber Code in prosecuting cyber criminals. The necessary evidence of a case may be virtual, and may be located in the any part of the world making tracing difficult. The law also states that Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the States with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable. This fails to take into consideration cybercrimes perpetrated by corporate bodies. On the other hand, investigations may be refused where it compromises the right to privacy.

Another implication of section 91 is that Cameroon can co-operate with another state in accordance with the provisions of the Cyber Code , and through the application of other relevant international instruments in criminal matters, based on uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

In addition, section 91 notes that the general principles do not only apply in cybercrime investigations, but in any investigation where evidence in electronic form needs to be collected. This covers cybercrime investigations as well as investigations in traditional cases. For example, if the suspect in a murder case has used an e-mail service abroad, section 91 would be applicable with regard investigations that are necessary in regard to data stored by the host provider.

The Cyber Code contains a number of procedural instruments that are designed to improve investigations. However with regards to the principle of national sovereignty, these instruments can only be used for effective investigations at the national level. If investigators realise that evidence needs to be collected outside their territory, they need to request mutual legal

ISSN 2581 3382

assistance. Unlike any other user to access these websites, this could be a serious hindrance. Therefore, the first situation addressed by section 92 is widely accepted.

Accordingly, where other regulations are not applicable sections 92 and 93 provide a set of mechanisms that can be used to enforce Mutual Legal Assistance requests.

The second situation in which law-enforcement agencies are allowed to access stored computer data outside the territory is when the investigators have obtained a lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorisation is heavily criticised. One main concern is the fact that the provision in its current wording probably contradicts fundamental principles of international law. Based on international law, investigators have to respect national sovereignty during an investigation.

They are especially not allowed to carry out investigations in another state without the consent of the competent authorities in that state. The decision whether such permission should be granted is not in the hands of an individual, but of the state authorities, since interference with national sovereignty does not only affect the rights of the individual, but also state concerns.25 By signing a Convention or treaty, Cameroon partly dismisses the principle and allows other countries to carry out investigations affecting their territory.

Also, reliance on the Cameroon Criminal Procedure Code (CPC) makes enforcement inadequate for cross border crimes, just as such reliance on the CPC causes limitations in admissibility of evidence. This is because incriminating materials may not be physical, may be perishable and jurisdiction may not be limited to one territory.[26]

Section 92 provides conditions and limitations to request for assistance. Accordingly Cameroon can refuse cooperation, if it considers that the cooperation could prejudice its sovereignty, security, public order or other essential interests.

Again, the law seems to have relied on the jurisdiction of the requesting, and the receiving state. This presumption is inappropriate in a virtual environment in which these criminals can bypass prosecution by masking their undertakings and create difficulties for investigators in tracing them. In deliberately targeting their activities in or through jurisdictions where

[25] See section 2(7) of the U.N.Charter on Non Interference
[26] See more on this in chapter six on enforcement of cybercrimes. Grabosky P. (2004). Global Dimension of Cybercrime. Global Crime, 6(1)P.160

ISSN 2581 3382

regulation or legislation is not strong, or where investigative or other collaborative efforts are known to be poor, cyber criminals can minimise the risk of their activities being discovered or punishment being effected. International investigations require a time-critical response to help negate attacks as well as secure evidence.

Section 93 (2), seems to violate the dogmatic structure of a convention. If law-enforcement agencies were to be authorised to use this instrument in international investigations, by virtue of section 58 it would have been sufficient to include it in the catalogue of procedures in the context of mutual legal assistance.[27] Unfortunately , the instrument cannot be applied in international investigations because the corresponding provision in section 58 does not expressly provide for international cooperation. However, instead of relinquishing the dogmatic structure by allowing foreign investigators to contact directly the person who has control over the data and ask for the submission of the data, the law could have simply implemented a corresponding provision in section 58 of the Cyber Code to accessing publicly available data, regardless of where the data is geographically located.[28]

Furthermore the jurisdictional clause in the Cyber Code does not solve the problem of jurisdiction over cyber crimes. By referring to Jurisdiction as measures establishing jurisdiction over cybercrimes committed in territorial waters or the continental shelf contiguous with the territory of Cameroon by a member of the crew of a Cameroonian or foreigner ship, those of the port of registry of the ship boarded by the accused or the first Cameroonian port where the ship will anchor, whose territorial jurisdiction extends to the seawater extension of the place of the infringement within the territory, the virtual and the borderless nature of cyber crime seem to be disregarded.[29] The inadequacy of this provision is tied to its failure to consider the complex, virtual and borderless nature of cyber crimes [30]

Another uneasy challenge is the principle of dual criminality which requires the recognition of the particular cybercrime in question under national law. In fact, it poses difficulties, if the offence is not criminalized in one of the countries involved in the investigations. Owing to that

[27] Section 58 of the code provides for new mechanisms of preservation of stored computer data, preservation and partial disclosure of traffic data and production order
[28] See section 58 of the Cyber Code. See also Shinder, D.(2002) Scene of the Cybercrime: Computer Forensics Handbook Rockland: Syngress Media, P .235
[29] See section 94 of the Cyber Code
[30] August R. (2008)"International Cyber-Jurisdiction: A Comparative Analysis" 39 (4) *American Business Law Journal PP*. 531 and 533

ISSN 2581 3382

possible legal loophole, cybercriminals may take that advantage to choose targets outside their own country and act from countries with inadequate cybercrime legislation.

Since the nature of network technology creates opportunities for criminals to remotely victimize anyone on the planet, a response to computer crime needs to be international in nature.

Further, the investigators may follow the Mutual Legal Assistance Treaties (MLAT) mechanisms to request assistance and other evidences from a foreign country, which often proved to be time-consuming. Alarmingly, it has became very challenging for investigators and prosecutors to identify and locate the actual perpetrator since perpetrators now use modern technologies and methods to hide their identity and location.

Another issue which creates a serious problem for the prosecutor and the investigator is differences in the legality of the subject matter. This means what is illegal under the laws of Cameroon could be legal in other country. In today's world it became very easy for someone sitting in nation 'X' to commit a criminal act against a victim physically situated within the territory of nation 'Y' without ever leaving his own country.

Also,the recent intensification of the cybercrime is alarming. However, prosecutors and other investigator authorities face enormous problems in collecting evidences to prosecute the perpetrators operating criminal conduct extra-territorially. In an international context, it is often difficult and time-consuming to establish which jurisdiction regulates the preservation and collection of evidence from online service providers. This prosecution team do not receive enough evidence to overcome the evidential threshold to initiate the case against the perpetrator.

At times this negotiation process wholly depends on the political relationship between the States. It also shows that, Cameroon or the other state has different priorities and focus areas in terms of the importance of cybercrime investigations. As a consequence, the requests for assistance in cybercrime cases may simply be given a much lower priority, especially if they have come from a country with no history of cooperative action.

Securing extradition is one of the most challenging stages for the investigator and prosecution team. Extradition requires not only that an appropriate treaty exist between the two countries

ISSN 2581 3382

concerned, but also that the conduct in question be criminalised in both referring and receiving country that is "dual criminality". In the case of cyber related crime, this is often not the case.

The cyber code is indeed a significant step forward since it indicates a gradual shift from the mutual legal assistance mechanisms (where the requested Member State has a wide discretion to comply with the request of another Member State) into a mutual recognition mechanism (where each Member State must in principle recognize and execute a request coming from another Member State). However, in the context of transborder access, the Law does still not solve the need for time-critical access to transborder data during an investigation.

The Cyber Code does not require foreign authorities to carry out investigative measures that violate rights protected in domestic law. This therefore makes investigative powers territorial. Furthermore, very often, MLATs can only be used to coordinate an investigation and prosecution if the requirements of dual criminality are satisfied.[31] The case of Onel de Guzman is one of the commonly cited examples, where Guzman, the author of the Love Bug virus could not be prosecuted despite effective international cooperation between the law enforcement agencies of Philippines and other affected countries. The concept of dual criminality came to his rescue, when authoring and unleashing a computer virus was at the concerned time not an offense in Philippines. MLATs also fail with respect to the speedy and urgent preservation of evidence which is synonymous with cyber crime investigation. Investigators in Cameroon need to be able to contact their counterparts in other countries immediately in order to ensure that the necessary evidence should not be lost. [32]

International cooperation in cybercrime investigation in the form of MLA requires an international agreement or other similar arrangement such as reciprocal legislation. Such provisions, whether multilateral or bilateral, oblige the authorities of a contracting party to respond to a request for mutual legal assistance in the agreed case. Such assistance generally refers to specific coercive powers concerning the investigation of cyber crime[33]

[31] That is if the act constitutes a crime in both states. See Sussman S. (1999). The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium. Duke Journal of Comparative and International Law (9), p. 458. See also Nykodym, N and Taylor R (2004), ''The World's Current Legislative Efforts against Cyber Crime'', 20(5) Computer Law and Security Report p. 390.

[32] Part VI of the Cyber Code

[33] Akuta E. (2014)"Using the Cost Element Model to Explain Perceptions to Combat Cybercrime in *Cameroon: A Structural Equation Model Approach*" Journal of Research in Peace, Gender and Development (JRPGD) Vol. 4(2) pp. 167--170

ISSN 2581 3382

Apart from requests for traditional help, such as interviewing witnesses, the purpose is to obtain certain data stored in a computer system that is located in the territory of another state or being transferred electronically through a network and capable of being monitored or intercepted in the territory of that state.

Investigatory processes become difficult if Cameroon has no MLATs or extradition treaties the other country..

Another limitation is that a lower level of consensus has been reached. For example, unlike traditional offences in international criminal law, which have rarely been penalised in domestic law, cybercrime was initially devised in the legislation at the national level. The Cyber Code does not explicitly provide for offences over which mutual assistance can be reached. Standard substantive laws are therefore recommended for an effective enforcement of cyber crime laws since little time is used to apprehend the criminal and thereby a solution to impunity. [34]

Section 92 and 93 provide for formal, complex and often time-consuming procedures, and in addition are often not suitable for computer-specific investigations.

Also, the mechanisms of MLA in prosecuting cyber crime under the cyber code appears to be sluggish than domestic legislation; this is being exemplified by the fact that it requires the consent for enforcement to be given by the authorities of both countries. This exercise has a negative impact on effectively curbing cybercrimes at international level, as evidence may perish, or the perpetrator may not even be found either in Cameroon or the other country , but somewhere in the globe. This will make the measures less effective. Considering the characteristics of cybercrimes, the "safe haven for criminals" can only be eliminated when almost all the sovereign states have access to one agreement and almost all the online users are subject to the power of law enforcement.

The law seems to give too large a to the judges to cover a significantly large number of crimes in the cybercrime arena and to take a stand on crimes for which there may not be universal support. However authorities are free to issue reservations and declarations, allowing them to interpret offenses flexibly with due respect for national and cultural differences.

[34] Ojedokun, A (2005), ‘’*The Evolving Sophistication of Internet Abuses in Africa*’’ The International Information and Library Review No.37 P. 80

ISSN 2581 3382

The law requires a significant amount of involvement from the private industry. While the private industry is only required to assist in a manner consistent with their existing technical capability. 35The issue is complicated by the fact that the law does not provide a framework for funding government and international requirements for the private industry.

Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties that dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties.[36]

The cyber code further presents a number of limitations through a focus on "consent" and presumed knowledge of the "location" of data. In reality, "true" data location is rarely known at the outset of an investigation, or at the point at which data access may be required.

Setting up procedures for quick response to incidents, as well as requests for international cooperation, is of mutual assistance; it would generally be most efficient for the authority designated for such purpose under a Party's MLATs, or the 2010 law to also serve as the central authority when this article is applicable. However, a Party has the flexibility to designate more than one central authority where this is appropriate under its system of mutual assistance. Where more than one central authority is established, the Party that has done so should ensure that each authority interprets the provisions of the terms of the Convention in the same way, and that both incoming and outgoing requests are treated rapidly and efficiently, of the names and addresses (including e-mail and fax numbers) of the authority or authorities designated to receive and respond to mutual assistance requests .Parties are obliged to ensure that the designation is kept up-to-date. [37]

Further, all crime statistics are generally created at the national level and do not reflect the international scope of the issue. Even though it would theoretically be possible to combine the available data, such an approach would not yield reliable information because of variations in legislation and recording practices.[38] Combining and comparing national crime statistics requires a certain degree of compatibility that is missing when it comes to cybercrime. Even if

---

[36] De Vel G. (2002). "The Council of Europe in the New Information Era". Presented at the Agenda E-governance Agenda-setting Workshop, Strasbourg pp.79-85 .
[37] Tangham P. (2009) "Economic Crimes In Cameroon– Its Impact On The Sound Development Of The State." Resource Material Series . No.66 P.152
[38] Ibid p. 157

ISSN 2581 3382

cybercrimes data are recorded, they are not necessarily listed as a separate figure. Furthermore, statistics only list crimes that are detected and reported. Especially with regard to cybercrime, there are concerns that the number of unreported cases is significant. Businesses may fear that negative publicity could damage their reputation. If a company announces that hackers have accessed their server, customers may lose faith.[39] The full costs and consequences could be greater than the losses caused by the hacking attack. On the other hand, if offenders are not reported and prosecuted, they may go on to re-offend. Victims may not believe that law-enforcement agencies will be able to identify offenders. Comparing the large number of cybercrimes with the few successful investigations, they may see little point in reporting offences.

Even when a victimised nation does receive cooperation from a foreign nation under, for example, a Mutual Legal Assistance Treaty (MLAT), evidentiary requests often take several months to be honored, if at all. Since evidence of a cyber attack may be disposed of quickly, current international agreements like MLATs providing for law enforcement cooperation operate too slowly to be effective. Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialised investigative actions, such as preservation of computer data. Response times for formal mechanisms, that are used currently, are of the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence.

It is one thing to enact procedural laws , it is quite another to assert jurisdiction over conduct that may be located or originate anywhere in the world. Cyberspace is a distinct phenomenon, beyond traditional rules based on geographical location.

Furthermore, very often, MLATs can only be used to coordinate an investigation and prosecution if the requirements of dual criminality are satisfied. The case of Onel de Guzman is one of the commonly cited examples, where Guzman, the author of the Love Bug virus could not be prosecuted despite effective international cooperation between the law enforcement agencies of Philippines and other affected countries. The concept of dual criminality came to his rescue, when authoring and unleashing a computer virus was at the concerned time not an

[39] Goodman, S. et al.(2007) *" Towards a Safer and More Secure Cyberspace."* National academies Press p. 37
[39] Ibid

ISSN 2581 3382

offense in Philippines. MLATs also fail with respect to the speedy and urgent preservation of evidence which is synonymous with cyber crime investigation. Investigators need to be able to contact their counterparts in other countries immediately in order to ensure that the necessary evidence should not be lost. [40]

Investigations of computer crimes require specialized skills. Countries need to allocate resources to training individuals in these specialized skills. Additionally, developed countries need to coordinate with countries where investigators are less knowledgeable.

Although government computers are sometimes the targets of attack, the majority of attacks are targeted at private systems. Therefore, law enforcement agencies must effectively participate with and assist the private sector. This is critically important because the private sector has skills and resources that the public sector does not possess.

Computer crimes often transverse different countries where law enforcement officials speak different languages. This language barrier is problematic, especially because effective investigation requires speed in gathering electronic data from many parts of the world.

The evidence from a computer crime is extremely perishable. This makes it important that investigations are fast and efficient.

The provisions of the Cyber Code seems to be based on the principle of "dual criminality." Investigations on a global level are generally limited to those crimes that are criminalised in both countries. Although there are a number of offences, such as the distribution of child pornography – that can be prosecuted in most jurisdictions, regional differences play an important role.

One example is other types of illegal content, such as hate speech. The criminalisation of illegal content differs in various countries. Material that can lawfully be distributed in one country can easily be illegal in another country. Another important enforcement mechanism can be community or industry self-regulation such as code of conducts or practices which are in favor of "online-regulation" of Internet markets or "self-regulation" by industries themselves especially in the areas of privacy or personal data protection. Furthermore, close

[40] See Longe, O. et al (2009). "Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives." Journal of Information Technology Impact, 9(3), PP.155-165

ISSN 2581 3382

coordination is required among relevant agencies at not only national levels but also regional and global levels, since one of the most important challenge often faced by the enforcement agencies is that the cyber-criminals have the ability to commit the crime quickly and then disappear without revealing their true identity or location. Often these criminals are located in a foreign jurisdiction. Thus, tracking them requires law enforcement agencies to be created and act faster through cyber border cooperation from a spectrum of organisations representing governments, businesses and consumer groups in various countries.

REMOVING OBSTACLES TO MLA IN CYBER CRIMINALITY IN CAMEROON

- The country's law needs to empower law enforcement with necessary tools for carrying out modern investigations. In the case of more intrusive measures such as surveillance,3 conditions for further authorisation of a competent authority must be regulated in a clear and transparent manner and undertaken in accordance with law in order to be admissible in court. -The investigative measures relevant for the purposes of this article pertain to obtaining extraterritorially located evidence. Channels for obtaining data located extraterritorially may be built on formal or informal relationships but must at all counts be in line with international law as well as supported by domestic legislation and accepted procedures.

- Among other restrictions, these measures need to take into account the boundaries set by jurisdiction that reflect the extent of a State's right to regulate the conduct or the consequences of events.4 In the context of cyber crime, the interpretation and implementation of jurisdictional principles play a role in establishing jurisdiction for both prosecuting the offence (prescriptive jurisdiction, adjudicative jurisdiction) as well as for specific cross-border investigatory measures (jurisdiction to enforce). Although jurisdiction is primarily territorial, there may be grounds for its extraterritorial application. While over the years a lot of research has been undertaken regarding the limits of prescriptive jurisdiction, the territorial scope of jurisdiction to enforce has received undeservedly little attention. In fact, it is the interpretation of the latter that is especially relevant for outlining the rules for accessing and obtaining data in foreign jurisdictions. This is because, according to international law, the exercise of jurisdiction to enforce on the territory of another State is permitted only if the latter provides consent to such behaviour (such as a based on a bi- or multilateral agreement) or such a right would be deriving from international customary law.

ISSN 2581 3382

- As long as the existing MLA framework is not adjusted to the actual needs of law enforcement in the field of cyber(-enabled) crime, there is a real risk that law enforcement authorities will use alternative methods of obtaining digital evidence, without complying with the existing MLA framework and thus potentially resulting in overstepping the boundaries of national sovereignty and the principle of territoriality. Such MLA 'without assistance' or 'self-service' obviously puts at risk the suspect's fair trial rights.

Additionally ,in order to effectively carry on electronic MLA the following propositions are here below proffered :

- Enact a more flexible, robust and adequate procedural law for mutual legal assistance.
- ensure the timely gathering and exchange of evidence in cases involving transborder high-tech crimes.
- trained network personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
- appropriate steps must be to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other country .
- Strategies to ensure the possibility of establishing an online resource providing information on laws on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.
- encourage Judicial authorities to share information on good practices, training and improved procedures to encourage direct communication between judicial authorities. More comprehensive training and involvement of judges and prosecutors in matters related to cybercrime and electronic evidence.
- design and preserve a database of laws on electronic evidence and related criminal offences should be established. Accordingly, while these laws should address each Cameroon's unique challenges, they should also be harmonised with those of other countries.
- encourage private sectors like Orange Cameroon, MTN Cameroon and CAMTEL should be encouraged.

ISSN 2581 3382

- encourage effective Leadership of government and states organs like Telecom Regulatory Board and Agency for Information Communication should be sensitized on the need for effective transborder.
- ensure that requests for MLA must be in French to reflect the Bilingual nature of Cameroon
- focus with priority on dismantling criminal infrastructure, disrupting the key services that support or enable cybercrime and prosecuting those responsible for malware development, as the numbers of highly skilled cybercrimes are limited and their skills are hard to replace.
- invest more in capacity building, with a view of acquiring the necessary skills, expertise, knowledge and tools to perform cybercrime investigations, big data analysis and internet of everything related to digital forensics.
- ensure cooperation with third parties, including internet intermediaries, in running awareness campaigns about cyber-threats. This should involve measures highlighting the importance of digital hygiene and endpoint security, the importance of security by design, and providing more online resources for victims to report crime and seek help and support. However, it must be done in a manner that does not compromise with the right to privacy.
- train and equip law enforcement officers to address high-tech crimes.
- protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- ensure the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
- Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

ISSN 2581 3382

- Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
- Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
- Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
- Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.
- establishing a platform for all stakeholders of cyber crime investigation

ISSN 2581 3382