Global Scientific JOURNALS

GSJ: Volume 11, Issue 3, March 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

CYBERSECURITY ENHANCEMENT CAPABILITIES FOR LEGAL AND SECURITY OFFICERS IN CAMEROON

Rachael Eben,
Ph.D. MaritimeLaw,
Department of Law,
University of Buea, Cameroon
ebenrah@yaoo.com

KeyWords: cybercriminality, cybersecurity, judicial police officers, online space, digital education, digital evidence, computer systems

ABSTRACT

This work examines some of the complexities faced by judicial and security officers in the country in tackling the menace posed by cybercriminality which has permeated almost every facet of modern day society. With advancements in technology, the new arena for the commission of crimes is the cyber space, where criminals use the benefit of the internet to commit crimes from the comfort of their bedrooms, mobile phones, computers, and computer systems, while victims (companies, governments and individuals) suffer huge losses. Since this is a new pathway used by criminals, the law is slow to catch-up, and judicial police officers (police and gendarmes), lawyers (advocates), and magistrates in the country are still entrenched in solving traditional crimes. Indeed, it is not enough to understand the laws needed to investigate and prosecute; it is now critical that they also learn the craft of the cybercrime enterprise, by acquiring the fundamental technical skills necessary to help them match these online 'wizards'. Their new training curricular should incorporate a cybersecurity component which will equip them with the requisite technical skills needed to combat cybercriminality. Most especially, police and gendarmerie branches, and courts across the country should have cybercrime units that are dedicated to solving this menace. ENAM[1] recently revised its curriculum to incorporate a component on firearms deployment; a cybersecurity component should also be added to the academic curricular/programs of these investigating and prosecuting institutions in the country, as the damage caused to organizations and governments by burglary, even armed robbery, is now miniscule in comparison to that done by a compromised network security system.

[1]Ecole Nationale d'Aministration et de Magistrature (ENAM) -established in 1959, ENAM is an elite training institution for first grade magistrates and civil administrators in the country.

Cybersecurity Enhancement Capabilities For Legal And Security Officers In Cameroon

I. Introduction

The emergence of technology which has come to affect almost all facets of modern day life, including governments, corporate bodies and ordinary individuals, is both a blessing and a curse. The treacherous side of technology has led to the growth of cybercriminality, facilitated mostly by easy internet access. Sadly, cybercriminality is perpetrated not only by petty criminals from their bedrooms, governments and companies-even multinational corporations, have invested enormous amount of time and resources to both perpetrate and counter cybercriminality. This is corroborated by revelations that the United States of America (and indeed other governments around the world) had been involved in the perpetration of gross instances of unauthorized surveillance of fibre optics and phone communications of ordinary citizens and other foreign governments,[2] even friendly ones. Companies have even set-up dedicated cyberspace units in and out of their home countries to engage in Intellectual Property (IP) violations (trade secrets, copyrights, etc.) and other untoward activities that give them unfair advantage over competitors. In addition to persistent surveillance activities, big data, unauthorized access and the sale of information is now a flourishing business[3] which led to the US Congress summoning the founder of Facebook[4] and Google and Yahoo CEOs to provide clarifications on this new global problem in the peddling of big data;[5] a phenomenon which their platforms have become the conduit for their perpetration.

At a more familiar level, individuals and small businesses are suffering from email hacking, SIMBOX fraud,[6] phishing, spamming, Internet Access Denial (IAD), Denial of Service (DoS), pornography and revenge porn,[7] online stalking, cyberbullying, data espionage[8] and much more. But the reality of the true extent of the menace posed by cybercriminality is felt by most technology users only when either their mobile money account or bank account is emptied or tempered with. That is when they become alert and start asking questions about cybercriminality, whereas they could have suffered from email hacking, spamming, internet access denial,etc., without giving heed to these detrimental aspects of cybercriminality. By then, they must have lost personal data, which is now worth billions of dollars to technology companies and cybercriminals. Unfortunately, most judicial police officers and even judicial authorities in the country lack the requisite technical skills to combat this new type of crime which is slowing overshadowing the traditional crime scene.

II. Definition of cybercriminality

With the cyberspace being an agile and dynamic environment, definitions for cyber crimes/computer crimes are diverse and varied. Indeed, providing a definition which is legalistically incontrovertible has

[2]*BBC News*, "Edward Snowden:Leaks that exposed US Spy Programme"1 July, 2013 htttps://www.bbc.com/news/
[3]*Ibid* – The case of Cambridge Analytica on President Trump's 2016 election in the United States.
Facebook Founder Mark Zukerberg has even been summoned by the US Congress, together with Google and Yahoo CEOs, and have all been interrogated by the same House.
[5]*The Washington Post*, "Big Tech Hearing: Apple, Google, Facebook and Amazon CEOs testified before House" (2020)www.washingtonpost.com
[6]A SIMBOX is a device that enables people abroad to place calls at local tariffs, causing huge financial losses to companies as well as the treasury.
[7]A practice whereby intimate photos of former lovers are published online in the event of a breakup to embarrass them.
[8]Illegal acquisition and use of information.

been impractical since establishing the balance between a computer as a perpetrator and victim of crime is a challenge. To tackle this challenge, the United Nations Congress on the Prevention of Crime and Treatment of Offenders proposed two different definitions during its 10th congress. The first definition states that, "computer-crime covers any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them."[9]

The second definition of the UN Congress indicates that "computer-related crimes covers any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network." [10]

The network systems approach to defining cybercriminality is buttressed by The Stanford Draft in its article 1(1)[11] which points out that cybercrime "means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention" This definition ties in with the United States Computer Fraud and Abuse (CCFA) Act, 1986 which focuses on acts or conduct perpetrated by use of a computer. Indeed, The United Nations Office on Drugs and Crime[12] holds a similar view to the acts and conduct committed using computer systems rather provide a definitive definition of cyber crime itself.[13]

The Commonwealth of Independent States Agreement prefers to address cybercrime from cyber information perspective and views it as a 'criminal act of which the target is computer information.'[14] This definition limits itself only to information that can be gleaned from a computer, without venturing into the non-information exploits of cybercriminality. This information abuse attributed to cybercriminality is shared by the Shanghai Cooperation Organization Agreement which defines cybercrime as "using information resources and/or influencing them in the information space for illegal purposes."[15]

Cybercrime is also described as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks." It should be noted that this definition is outside the purview of the Commonwealth Model Law on Computer and Computer-related Crime; and the Council of Europe Convention on Cybercrime[16] which both recognize that computer hardware is capable of being used in committing regular crimes like fraud, forgery, child pornography, or other crimes like pod slurping, piggy backing or inserting a USB into a computer port and causing damage to the target data system.[17]

Instead of providing a definition, The Convention on Cybercrime[18] prefers to characterize cyber crimes in terms of their typology as; offences against the confidentiality, integrity and availability of computer data and systems; Computer related offenses; content-related offences; and offences related to infringements of copyright and related rights. In the same vein, The Council of Europe's Cybercrime Treaty prefers to characterize "cybercrime" as offences ranging from criminal activity against data to content and copyright in-

[9]United Nations, "10th Congress on the Prevention of Crime and the Treatment of Offenders," pp.86-87
[10] UN, *Supra.* 9
[11]The Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism
[12]United Nations Office on Drugs and Crime (UNODC, "Comprehensive Study on Drugs and Crime" Draft- February 2013
[13]*Ibid*, pp.12
[14]Commonwealth of Independent States, Annex 1(a) - Agreement on Cooperation in Combatting Offences related to Computer Information (Commonwealth of Independent States Agreement), 2001
[15]Shanghai Cooperation Organization, Annex 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization,2010
[16]Convention on Cybercrime,2001- Articles 7- 9 states - a person who produces USB 94 devices containing malicious software that destroys data on computers when the device is connected commits a crime
[17]Asian School of Laws, *A to Z of Cyber Crime" LEXCODE: Regulatory Compliance* Technologies PVT. Ltd.
[18]The Council of Europe Convention on Cybercrime, 2001 (Budapest Treaty) to address actions against confidentiality integrity, and availability of computer data and systems

fringement.[19] Even though these categories serve as a good starting point in understanding the variety of features that form the basis of cybercriminality, distinguishing between categories based on legal protection and the method used in the commission of a computer crime could be a hurdle that may become trying for legal and security officers in solving computer crimes.

From the above, it is evident that cyber crimes or computer crimes are used to either describe crimes that fall under the realm of traditional crimes or crimes that are network related. With this understanding, it is evident why huge amount of time and resources are now being invested by governments and businesses to counter this crime which is complex to define, but perceptible all the same.

III. The Outlook of Cybercriminality in Cameroon

To understand the extent of the proliferation of cybercriminality in Cameroon, it is necessary to indicate that in 2015, Edward Snowden's revelations of WIKILEAKS dumping of classified information on its website,[20] brought home to many ordinary users of technology the extent of governments' role in the furtherance of cybercriminality.[21] But government systems are also at peril from attacks being committed by cybercriminals.[22] In Cameroon, government websites have been defaced, critical systems attacked for vital documents, data compromised, viruses thrust into computer systems and government officials embarrassed from online hacking and posting of sensitive official correspondences. Between 2015 and 2017, 7 government websites suffered web defacement, 34 of 144 government sites were infected with malicious programs, and 182 government personalities suffered usurpation of their identities in Cameroon[23]

Although the US State Department states that it cannot independently ascertain that email accounts are being monitored by the government of Cameroon, ANTIC[24] admits to 'checkmating' or swooping email accounts, capturing personal information of mobile phone users.[25] The Director of ANTIC stated that:

"…ANTIC uses state-of the-art tools or cutting-edge tools to permanently watch social networks. This consists of browsing the various profiles on the social networks to detect illicit content representing a potential threat for the national security and the image of Cameroon, and to weed them out."[26]

According to the US State Department, the government of Cameroon has repeatedly used internet restriction to control the social media landscape –starting with a nationwide restriction in January 2017 for 93

[19] Ibid

[20] Arjun Kharpal, "Edward Snowden: US government 'reckless beyond words' after WikiLeaks doc show CIA hacking tools." Online *CBNC* March 2017

[21] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, "Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime" International Journal of Cyber Criminology Vol. 8 Issue 1 Jan- Jun pp.2 -3 2014

[22] Anthony Zurcher, "Hillary Clinton's emails- what's it all about?" Online *BBC* November 2016
Even government infrastructures are also vulnerable, as the US State Department's email system suffered the worst government compromise in November 2014, leading to a one week shut down of the e-mail system.

[23] ANTIC, – "Rapport Sur La Cybercriminalite Et La Cybersecurite Au Cameroun De 2015 A 2017" ANTIC%20CYBERCRIME%20STATISTICS%20statistiques_2015_2017.pdf

[24] Decree N°. 2002/092/PR of 8 April 2002 -creating the National Agency for Information and Communication Technologies (ANTIC). The agency was originally created to develop ICT in the country and foster growth.
Then, Decree N°. 2012/180/PR of 10 April 2012- assigned new missions to the ANTIC - including the regulation of electronic security activities and of internet in the country.

[24] Law no. 98/014 of July 14 2010 creating the Telecommunications Regulatory Agency (TRA) in Cameroon

[25] Cameroon Tribune, (2014, March 29). [Interview] Cameroun: Dr Ebot Ebot Enow Directeur Général de l'Agence Nationale des TIC. Afro Concept News. www.afroconceptnews.com/2014/03/29/ interview-cameroun-dr-ebot-ebot-enow-directeur-general-delagence-nationale-des-tic .

[26] *Supra.*24

days, followed by another targeted blockade in October 2017; disrupting educational, financial and healthcare institutions that depend on internet access to function.[27]

Financial institutions have also suffered enormously from this new crime endeavor, with the National Anti-Corruption Agency in Cameroon (CONAC),[28] reporting in 2014, that fraudulent card activities through acts of skimming[29]costs banks 3.7 billion CFA for the period between November and December 2013.[30] In 2015, mobile phone operators suffered losses of up to 18 billion CFA, while the state lost about 4 billion CFA in the same time period for the same activities. MTN reported that it had lost 60 million minutes of phone calls to SIMBOX fraud alone.[31]

Apart from these powerful entities being assaulted by cybercriminals, small business concerns and ordinary citizens are also at the receiving end of the cyber criminal enterprise. Indeed, individuals have suffered losses in both financial and personal terms. While scamming is prevalent in the university towns of Bamenda, Buea, Douala and Yaoundé; with large student populations according to ANTIC, pornography is also a common occurrence on the Cameroon cyberspace- with videos/nude photos of victims posted online, without permission. Acts like this have caused great anguish to victims. Unfortunately most of these crimes remain unreported and unresolved because most victims cannot obtain redress in a country which is still lagging behind as far as cybercriminality prosecution is concerned.

The problem is further compounded by the fact that over 90% of software and operating systems in the country are prone to hacking.[32] McAfee named Cameroon in 2009 as the world's riskiest destination for internet surfers; with more than a third (36.7%) of websites hosted with the Cameroon domain name (.cm) now more risky than Hong Kong (.hk), China (.ch) and Samoa (.ws).[33] In essence, the online crime world in the country is an enterprise that must be treated with the same amount of firm fervor that traditional crimes are being handled by judicial and security officials.

IV. The Cybersecurity Legal and Institutional Landscape in Cameroon

a) The 1996 Constitution of Cameroon

The preamble to the 1996 Constitution provides that "the privacy of all correspondence is inviolate. No interference may be allowed except by virtue of decisions emanating from the Judicial Power."[34] Privacy is therefore an essential component that is guaranteed by the constitution, for which sanctions may apply in the event of breach. This protection of private correspondence is also reinforced by section 300 (1) of the Penal Code which states: '*Whoever without permission from addressee destroys, conceals or opens another's correspondence shall be punished with imprisonment for 15(fifteen) days to 1 (one) year or with fine of from CFAF 5000 (five thousand) to CFAF 100,000 (one hundred thousand), or with both such imprisonment and fine.'*[35] So, with the advent of technology, privacy has become an essential component in the cybercrime paradigm, and personal data; which could include email addresses, phone numbers, house location (home address), bank account details, and other intangible details, are now more valuable than ever be-

[27] United States Department of State-Bureau of Democracy, Human Rights and Labor, "Country Reports on Human Rights Practices for 2018- Cameroon" pp.7-19
[28] The National Anti-Corruption Agency in Cameroon (CONAC) -investigates and reports high level misappropriation of public funds of more than 50,000,000frs, perpetrated by public officials - to the Special Criminal Court for Prosecution.
[29] Skimming consists of criminals hacking magnetic cards with special devices inserted in automated teller machines
[30] The National Anti-Corruption Agency in Cameroon (CONAC)
[31] A SIMBOX is a device that enables people abroad to place calls at local tariffs, causing huge financial losses to companies as well as the treasury.
[32] ANTIC - National Agency for Information and Communications Technologies
[33] IT News Africa, "Cameroon has the Web's riskiest Domain" 2010 www.itnewsafrica.com/2020 May 2021
[34] Law No. 96-6 of 18 January 1996 to amend the Constitution of 2 June, 1972
[35] Law no. 2016/007 of 12 July 2016 relating to the Penal Code, Section 300(1) on tampering with correspondence

fore. The premise of the constitution therefore sets the foundation for the protection of privacy, including personal data, which is inviolate, but which could be compromised by acts of cybercriminality.

b) Law on Cybersecurity and Cybercriminality

The 2010 law on Cybersecurity and Cybercriminality[36] is the most important law in the country in force against cybercriminality. The key focus is on the privacy of personal data[37] and the substantive components of the law relates to criminalization of unlawful interception, illegal access, system interference, misuse of device, data interference, and computer-related fraud,[38]and other offences related to child pornography and grooming.[39] The Procedural competence of this law rests with judicial and security officials to investigate and prosecute cybercrimes, in addition to search and seizure powers over computer data.[40] To attain its objective, the law provides for the use of electronic communications in hearings in criminal proceedings,[41] in line with the Commonwealth Model Law on Computer and Computer-related Crime, 2002.[42] Considering the broad spectrum covered by this law, it is essential to highlight the latitude that judicial police officers have in the retrieval and interception of information (data). It is therefore critical to emphasize the need for best evidence rule to reign in the search and seizure; and data capture powers that these officers have, which may be prone to abuse if some control is not enforced by judicial authorities with the requisite knowledge and skills in cybercrime forensics.

c) The 2010 law on electronic communication

The law on electronic communication[43] is another vital piece of legislation that is in place to uphold the privacy of all electronic communication running on providers' platforms. This law governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the misuse of information and communication technologies in the country. Once privacy of data or information is compromised, businesses and government entities may suffer the same amount of injury that individuals are exposed to, which could range from reputational to financial losses.

d) The 2010 law on E-commerce

The law on electronic commerce[44] is critical within the paradigm of cybercriminality since most internet activities that take place online have a financial base. In order to protect e-commerce users therefore, the

[36] Law no. 2010/012 of 21 December, 2010- relating to cybersecurity and cybercriminality
[37] Section 44: It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.
[38] Articles 65- 86
[39] Article 76 and 81-83
[40] Articles 53- 57
[41] Article 59
[42] Commonwealth Model Law on Computer and Computer-related Crime, 2002 -dealing with digital evidence
[43] Law no. 2010/013 of 21 December, 2010-to govern electronic communication
[44] Law n° 2010/021 of 21 December 2010 - on electronic commerce in Cameroon
Other legal instruments emanate from regional and international conventions that the country is signatory to, some of which are the 2009 Draft Directive on Fighting Cybercrime within ECOWAS (ECOWAS Draft Directive);[44] the African Union 2012 Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (Draft African Union Convention); the United Nations 2000 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (United Nations OP-CRC-SC), ratified by Cameroon in December 2019; the 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information (Commonwealth of Independent States Agreement); as well as the country's alliance with INTERPOL in the global efforts to fight cybercriminality (INTERPOL, 2009).

focus is on the commercial dimension, focusing on the privacy of personal data online,[45] the validity of electronic documents, the use of e-signature in online transactions, as well as sanctions that apply in the event of violations. It therefore aims to promote e-commerce in the country through assurances on the protection of data in online commercial transactions,[46] including e-signatures to wit; sanctions apply for violations.

e) National Agency for Information and Communication Technology (ANTIC)

Apart from these pieces of legislation, the government has also put in place some institutional mechanisms to counter this problem. The National Agency for Information and Communication Technology (ANTIC),[47] created in 2002, was charged with the duty to facilitate and accelerate the uptake of ICTs in the country in order to contribute to development. Its remit was expanded in 2012 to include the regulation of electronic communication and internet activities. Since its inception, ANTIC has been kept busy by men of the cyber world, whose enterprise has put the government, businesses and ordinary individuals in a persistent state of heightened alert.

f) The Telecommunications Regulatory Agency

The Telecommunications Regulatory Agency (TRA)[48] was created in 1998 to work in consort with ANTIC in keeping the country safe from cybercriminality. It monitors and controls the activities of telephone operators, regulates the market and grants licenses to all telephone operators. TRA has managed to set standards and order in the Cameroon mobile phone sector, but the deviance posed by cybercriminals using mobile communication platforms is still elusive for the regulator and even the mobile phone companies themselves. Despite the existence of a regulator which supervises and regulates the telecoms sector, the country still lacks full expertise in oversight and policing of the sector, thus easing the growth of cybercriminality. The United States Patent and Trade Office (USPTO) in 2011 even provided training on intellectual property rights protection to Cameroonian officials (including customs officers, magistrates, and civil servants) and set up a training centre at the University of Buea to counter cybercriminality. All these efforts attest to the prevalence of cybercriminality in the country which needs attention from the investigators and prosecutors of this new channel for the commission of crimes.

V. The Problematic

Cybercriminality is a fast growing crime which is underreported because victims do not often see the prospects of their crime being resolved in institutions that do not yet have dedicated cybercrime units and personnel. Legal practitioners and law enforcement officers in the country are not equipped with the requisite knowledge and technical skills to combat this new crime pathway. These practitioners are still stuck in the old mortar and bricks arena of crimes prosecution, whereas, hackers, scammers, data espionage agents, pedophiles have evolved to the online space as their new crime hub. In fact, the training of police officers in the country is still done in dedicated classrooms, with pens and paper, and no real access to sophisticated

[45] Section 44: It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally

[46] *Ibid,* Section 44

[47] Decree N°.2002/092/PR of 8 April 2002 creating the National Agency for Information and Communications Technologies (ANTIC) and Decree N° 2012/180/PR of 10 April 2012- assigning new missions to ANTIC, including the regulation of electronic security activities and of the internet in the country.

[48] Telecommunications Regulatory Agency (TRA) created by decree no. 98/014 of July 14, 1998

computer systems or even cyber security experts. The same difficulty is noticed even in the elite training institution of ENAM[49] which still has just incorporated courses on cybersecurity into its training program, in spite of the growing threat posed by these crimes. Even lawyers in the country who are well qualified and knowledgeable in legal skills, lack the training in fundamental technical skills needed to combat cybercriminality. This means that, these experts are pursuing criminals whose craft in trade they do not master.

These assertions stated above are corroborated by the United Nations Office on Drugs and Crimes which relate that 70% of specialized law enforcement agencies in less developed countries do not have adequate computer equipment and skills. In addition, more than half of the countries examined in its report highlighted lack of sufficient resources dedicated to tackling cybercrimes. It further asserts that all the countries in Africa indicated that they were in need of cybercrime investigative techniques, to which 60% of the technical assistance was needed to assist law enforcement agencies.[50]Therefore, this is a prevalent problem that needs dedicated attention in Cameroon from those involved in the prosecution of crimes.

VI. The Missing Piece in the Paradigm

1. Training of Judicial and Security Officers on ICT and fundamentals of cybersecurity

With ENAM training and graduating at least 30 First Grade Magistrates every year, and about 400 judicial police officers and gendarmes graduating at the same time from various law enforcement institutions across the country, there is a disconnect between the Ministry of Justice and the General Delegation for National Security- Delegation Nationale a la Surete Nationale (DGSN). In fact, there should be synergy in the training of these two corps; with investigatory and prosecutorial powers. In order to combat this new phenomenon which is permeating the Cameroonian society; with its ever growing youth population; which is adventurous and enterprising, the training of legal practitioners and security officers in this new weaponry in the hands of criminals must be intensified at police training schools, at ENAM as well as at university law departments. This must be incorporated into their training programs, not just left as an elective course, but given the same level of importance that has been accorded to the firearms training at ENAM. This will give room for these officials to be able to combat crimes from a multiplicity of angles. This is especially critical for the new crop of magistrates, lawyers, and judicial police officers who are entering the 21st century, with a new set of criminal challenge awaiting them.

Although the 2010 law provides for admissibility of best evidence of electronic data, digital evidence does not yet constitute a great part of the courtroom portfolio in most Cameroon courts, which is still largely dependent on traditional means of investigating and adjudicating crimes, mostly due to lack of expertise and equipment. Due to these challenges, cybercriminality is flourishing because criminals in this domain are one step ahead of those who should be keeping tab of their activities. Although ANTIC is already making efforts to address this problem through training seminars and workshops,[51] this is simply not enough as there is a great difference between this approach and traditional classroom instruction, which is what is ac-

[49] Principally trains the judicial officials of the public sector in the country
[50] United Nations Office on Drugs and Crime, "Comprehensive Study on Drugs and Crime" Draft – February 2013 pp.12
[51]*Journal Du Cameroun,* "Law enforcement officers trained on cyber prosecution adjudication"5Th July 2018-
A three-day seminar to enhance the capacities of magistrates and law enforcement officers in the West Region of Cameroon to prosecute and adjudicate cybercrime and make use of electronic evidence is underway in Bafoussam.

tually needed to equip the judiciary and the security forces with the requisite skills to combat the problem of cybercriminality that the country is already grappling with.

2. Better entry qualifications for security officers

ANTIC reports a high rate of scamming in university towns like Bamenda, Buea, Douala and Yaoundé with high students population. These university students are comfortable in the use of computers and computer systems, more sophisticated in their calculations, and even adventurous in the use of online media. Unfortunately they are being pursued by an aging judicial police corps, most of who are not quite computer savvy, got admitted into training institutions with 5th grade aptitude[52] and are still receiving training in paper and pens, with minimal access to sophisticated computer systems and internet at their training academies. Most of the top brass in the judicial police corps in the country came in as Police Constables and have moved through the ranks. They were molded in the paper and pen era, are yet to change from what they have been doing for the past thirty years. However, the new breed of trainees coming into the corps, who are young, highly educated, and some university graduates, should be targeted and given the requisite technical skills to accompany their training to counter those who are still entrenched in the traditional ways of doing things.

3. Digitize the Courts and judicial police branches

Courtrooms in the country still depend on paper and pens, with little or no form of technology being used. Courtrooms do not even have stenographs (Steno Machines) for court clerks (registrars) to take notes and judges still have registers (Ledgers) where proceedings are written by hand. Courts and law enforcement units need to be digitized, this way, the process of collection and admissibility of digital evidence in courtrooms can be facilitated. The requirement for the collection of digital evidence spelt out in article 56 of the 2010 Cybersecurity and Cybercriminality Law[53]gives law enforcement officers the power to intercept electronic data/conversations and search and seize any equipment suspected to be used for the commission of cybercrimes. This wide powers given to security officers, to intercept data content and conduct remote content search is not fully being utilized in courtrooms as they do not yet have the basic technology to admit digital evidence. Even the complex issue of storage or preservation of digital evidence is another troubling aspect that suspects have to grapple with, but which well-trained advocates and magistrates in the techniques of digital evidence (forensics) can easily address in courtrooms to facilitate prosecution.

4. Devolve ANTIC and establish a more defined role for the agency

ANTIC was created in 2002 with its main remit being to develop ICT in the country in order to promote growth. In 2012, the agency was accorded further functions in the regulation of electronic security and internet activities.[54]Although the agency has been working tirelessly to achieve this, it has invariably been given extremely broad competence. Cameroon and Cameroonians are much more aware of cybercriminality issues from the nearly 20 years since the agency was created through the sensitization efforts put in place by ANTIC. Yet ANTIC states that one of the measures that it employs to tackle cybercriminality in the county is by providing assistance to security officers and individuals through adjudicating cybercriminality complaints and cases.

[52]The basic entry qualification for Police Constables and Gendarmes is First School Leaving Certificate; which is equivalent to 6-7 years of primary school education (or 5th grade).
[53]Article 56
[54]Decree no. 2012/180/PR of 10 April 2012 - assigning ANTIC with new missions to regulate electronic security and internet activities.

> Dans le cadre du renforcement de la cybersécurité au Cameroun, l'ANTIC a mené plusieurs activités dans les domaines suivants:- l'assistance des Forces de Sécurité et des usagers dans le traitement des réquisitions et des plaintes liées à la cybercriminalité [55]
>
> [Personal Translation –In its effort to combat cybersecurity in the country, ANTIC provides assistance to security officials and individuals in adjudicating cybercrime cases and complaints]

This proposition by ANTIC indicates that the agency still has a stronghold in the country on the adjudication of cybercriminality, which should have been handled by security officers, as provided for by the 2010 law, who are properly trained in the investigation of crimes. Security officers are the ones charged by the 2010 law to intercept, search and seize, preserve and store data collected in the process of investigating cybercrimes, under the supervision of judicial authorities. In essence, ANTIC is performing outside its remit in adjudicating cases and complaints, so educating law enforcement officers to rightfully conduct this activity themselves will put order in this sector, as the agency has also taken over the prosecutorial functions of courts - acting parallel to the court system in the country.

5. Borrow Best Practices From Other Jurisdictions.

a) US CFAA[56] or the European GDPR[57]

Computer fraud and abuse cases in the United States are conducted by the Federal Bureau of Investigation (FBI) which has both the human and material resources to investigate such crimes. Yet in Cameroon, ANTIC is the agency taking on this assignment and providing assistance to law enforcement, doing the job of crime investigation. ANTIC could borrow from the best practices of the US FBI by allowing the competent organs in the country with powers in the investigation of crimes, to carry on with cybercrime investigation, which falls under the remit of law enforcement.

b) Cameroon Computer Incidence Response Unit (CIRT)

Cameroon has set up its CIRT- Computer Incidence Response Unit[58] within ANTIC; which is under the tutelage of the Ministry of Telecommunications and under the direct auspices of the Presidency of the Republic.[59] This means that police oversight of this agency is limited as it is answerable directly to the Presidency of the Republic unlike the Kenyan CSIRT (Computer Security Incidence Response Team) which is supervised by the Ministry of Information and the Kenyan Police.

c) CAMEROON INTERPOL

INTERPOL has been working with the government of Cameroon and in synergy with other African countries in the global efforts to combat transboarder crimes. However, considering that ANTIC is the organ that is providing Cameroon law enforcement agencies with assistance and information regarding cyber-

[55] ANTIC, 2019
[56] United States Computer and Abuse Act (CFAA) on acts and conduct related to computer misuse- came into force in 1996- with civil and criminal components. The civil component has been a major deterrent to cybercriminals
[57] The European General Data Protection Regulation (GDPR) on privacy which came into force in 2018 is more focused on securing the privacy of users on computer systems.
[58] Africa CERT is an African forum of computer incident response teams (CIRT) which Cameroon participates in
[59] United States Department of State

criminal activities, it is evident that the INTERPOL unit in the country is handicapped in the level of penetration it can conduct with respect to cybercrime investigation as it cannot override ANTIC which is answerable only to the Presidency of the Republic.

6. Amend the Law on Cybersecurity

The government is to be commended for enacting the 2010 law on cybersecurity and cybercriminality which has come at the right moment to address the threat posed by this common problem to the global community of nations. The law falls in line with both the Commonwealth Electronic Evidence Model Law, 2002[60] which states that "Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record" and also the Commonwealth Model Law on Computer and Computer-related Crime, 2002,[61] which stipulates that:

> "In proceedings for an offence against a law of [enacting country], the fact that: (a) it is alleged that an offence of interfering with a computer system has been committed; and (b) evidence has been generated from that computer system; does not of itself prevent that evidence from being admitted."

Article 56- 58 of the 2010 law in Cameroon respects these fundamental principles on admissibility of digital evidence to solve computer and computer related crimes. Nonetheless, amendments could be made to keep abreast of the fast changing nature of the digital environment and give prosecutors more oversight of the investigating units.

a) In the almost ten years since the law came into force, the implementing instrument for E-sign certificate is not yet available – online shoppers/buyers have no recourse should personal data be compromised from online commercial transactions.

b) Mobile telephone companies are still violating and infiltrating the privacy of most mobile phone users with unsolicited adverts/information, without prior consent authorization sought and even fail to stop when consent is refused by some conscientious users.

c) The law is narrow in its scope as it fails to incorporate online copyright related offences which are now the new avenue for the violation of intellectual property rights- trademarks are usurped, domain names hacked and piggybacked or cybersquatted. Although the Copyrights and Neighboring Rights Law of 2000[62] provides protection for copyrights protection in Cameroon, complemented by the Bangui Accord of 1999,[63] these laws do not tackle abuse of intellectual property perpetrated by this new and fast growing route used to access copyright/trademark rights on the cyber space.

VII. CONCLUSION

The cybersecurity and cybercriminality law of 2010 has come to put some semblance of order in the Cameroon cyber landscape which until prior lacked a clear view. Although the law has addressed many critical areas that can help tackle the problem of cybercriminality, those with investigative and prosecutorial powers need to be better empowered through formal education at training institutions and academies. To obtain a more comprehensive outlook, dedicated cybercrime units should be set up in courts and police/gendarmerie

[60] Commonwealth Electronic Evidence Model Law, 2002 on General Admissibility -article 3
[61] Commonwealth Model Law on Computer and Computer-related Crime, 2002- dealing with digital evidence
[62] Law relating to Copyrights and Neighboring Rights of 2000 is a national instrument dealing exclusively with copyrights and related rights of intellectual property.
[63] L'Organization Africaine de la Propriete Intellectuelle (OAPI) March 2, 1977, the Bangui Accord, as amended on 24 March 1999 and 14 December 2015, relating to intellectual property protection for the 17 West and Central African countries of French expression to which Cameroon is a party.

headquarters, while critical technical equipment and human resources are assembled to cover all other branches/units in the country. Cybercriminality is a phenomenon that has come to stay, so the need to develop a young crop of judicial police officers, advocates and magistrates who are coming through the academic and training institutions with the skills they need to address this 21st Century challenge is vital.

References

[1] Ecole Nationale d'Aministration et de Magistrature (ENAM) – ENAM is an elite training institution for the training of first grade magistrates and civil administrators in Cameroon.
[2] *BBC News,* "Edward Snowden: Leaks that exposed US Spy Programme"1 July, 2013 htttps://www.bbc.com/news/
[3] *Ibid* – The case of Cambridge Analytica on President Trump's 2016 election in the United States.
[4] Facebook Founder Mark Zukerberg has even been summoned by the US Congress and Google and Yahoo CEOs have also been questioned by the same House.
[5] *The Washington Post:* "Big Tech Hearing: Apple, Google, Facebook and Amazon CEOs testified before House (2020)www.washingtonpost.com
[6] A SIMBOX is a device that enables people abroad to place calls at local tariffs, causing huge financial losses to companies as well as the treasury.
[7] A practice whereby intimate photos of former lovers are published online in the event of a breakup to embarrass them.
[8] Illegal acquisition and use of information.
[9] United Nations, "10th Congress on the Prevention of Crime and the Treatment of Offenders," pp.86-87
[10] Supra, 9
[11] The Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism
[12] United Nations Office on Drugs and Crime, "Comprehensive Study on Drugs and Crime" Draft – February 2013
[13] *Ibid,* pp.12
[14] Commonwealth of Independent States, 2001, Annex 1(a) - Agreement on Cooperation in Combatting Offences related to Computer Information (Commonwealth of Independent States Agreement).
[15] Shanghai Cooperation Organization, 2010, Annex 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization.
[16] Convention on Cybercrime Articles 7- 9 - a person who produces USB 94 devices containing malicious software that destroys data on computers when the device is connected commits a crime.

[17] Asian School of Laws, "A to Z of Cyber Crime" LEXCODE: Regulatory Compliance" Technologies PVT. Ltd.
[18] Convention on Cybercrime, 2001
[19] The Council of Europe's Cybercrime Treaty
[20] Arjun Kharpal "Edward Snowden: US government 'reckless beyond words' after WikiLeaks doc show CIA hacking tools." Online *CBNC* 8 March 2017
[21] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime" International Journal of Cyber Criminology Vol. 8 Issue 1 January - June 2014 pp.2 -3
[22] Anthony Zurcher, "Hillary Clinton's emails- what's it all about?" Online *BBC* 6 November 2016
[23] Government infrastructures are also vulnerable as the US State Department's email system suffered the worst government compromise in November 2014, leading to a one week shut down of the e-mail system.
[24] ANTIC – "Rapport Sur La Cybercriminalite Et La Cybersecurite Au Cameroun De 2015 A 2017" ANTIC%20CYBERCRIME%20STATISTICS%20statistiques_2015_2017.pdf
[25] Decree N°. 2002/092/PR of 8 April 2002 creating the National Agency for Information and Communication Technologies (ANTIC) the agency was originally created to develop ICT in the country and foster growth. Then, Decree N°. 2012/180/PR of 10 April 2012- assigned new missions to the ANTIC - including the regulation of electronic security activities and the regulation of the internet in the country
[26] Law no. 98/014 of July 14 2010 creating the Telecommunications Regulatory Agency (TRA) in Cameroon.Cameroon Tribune. (2014, March 29). [Interview] Cameroun: Dr Ebot Ebot Enow Directeur Général de l'Agence Nationale des TIC. Afro Concept News. www.afroconceptnews.com/2014/03/29/interview-cameroun-dr-ebot-ebot-enow-directeur-general-delagence-nationale-des-tic
[27] ANTIC Report, *Supra.* 24
[28] United States Department of State ' Bureau of Democracy, Human Rights and Labor' "Country Reports on Human Rights Practices for 2018- Cameroon" pp.7-19
[29] The National Anti-Corruption Agency in Cameroon (CONAC) -investigates and reports high level corruption cases of more than 50,000,000frs perpetrated by public officials - to the Special Criminal Court for Prosecution.
[30] Skimming consists of criminals hacking magnetic cards with special devices inserted in automated teller machine.
[31] The National Anti-Corruption Agency in Cameroon (CONAC)
[32] A SIMBOX is a device that enables people abroad to place calls at local tariffs, causing huge financial losses to companies as well as the treasury.
[33] ANTIC - National Agency for Information and Communications Technologies
[34] IT New Africa: Cameroon has the Web's riskiest Domain (2010) www.itnewsafrica.com/2020
[35] Law No. 96-6 of 18 January 1996 to amend the Constitution of 2 June, 1972.
[36] Law no. 2016/007 of 12 July 2016 relating to the Penal Code Section 300(1) on tampering with correspondence.
[37] Law no. 2010/012 of 21 December, 2010- relating to cybersecurity and cybercriminality, Section 44: It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.
[38] Articles 65- 86
[39] Article 76 and 81-83
[40] Articles 53- 57
[41] Article 59
[42] Commonwealth Model Law on Computer and Computer-related Crime (2002), dealing with digital evidence
[43] Law no. 2010/013 of 21 December, 2010-to govern electronic communication
[44] Law n° 2010/021 of 21 December 2010 - on electronic commerce in Cameroon, Section 44: It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.
[45] Section 44: It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.
[46] Economic Community of West African States (ECOWAS).
[47] Decree N° 2002/092/PR of 8 April 2002 creating the National Agency for Information and Communications Technologies (ANTIC) and Decree N° 2012/180/PR of 10 April 2012- assigning new missions to ANTIC, including the regulation of electronic security activities and the regulation of the internet in Cameroon.
[48] Telecommunications Regulatory Agency (TRA) created by decree no. 98/014 of July 14, 1998

[49] Principally trains judicial officials in the country
[50] United Nations Office on Drugs and Crime, "Comprehensive Study on Drugs and Crime" Draft – February 2013,pp.12
[51] Journal Du Cameroun, "Law enforcement officers trained on cyber prosecution adjudication"5Th July 2018- A three-day seminar to enhance the capacities of magistrates and law enforcement officers in the West Region of Cameroon to prosecute and adjudicate cybercrime and make use of electronic evidence is underway in Bafoussam.
[52] The basic entry qualification for Police Constables and Gendarmes is First School Leaving Certificate: which is equivalent to 6-7 years of primary school education (or to 5th grade).
[53] Article 56
[54] Decree no. 2012/180/PR of 10 April 2012 - assigning ANTIC with new missions to regulate electronic security and internet activities.
[55] ANTIC, 2019
[56] United States Computer and Abuse Act (CFAA) on acts and conduct related to computer misuse- came into force in 1996- with civil and criminal component. The civil component has been a major deterrent to cybercriminals.
[57] The European General Data Protection Regulation (GDPR) on privacy which came into force in 2018 is more focused on securing the privacy of users on computer systems.
[58] Africa CERT is an African forum of computer incident response teams (CIRT) which Cameroon participates in.
[59] United States Department of State
[60] Commonwealth Electronic Evidence Model Law (2002) on General Admissibility -article 3
[61] Commonwealth Model Law on Computer and Computer-related Crime (2002) In 2002, dealing with digital evidence
[62] Law relating to Copyrights and Neighboring Rights of 2000 is a national instrument dealing exclusively with copyrights and related rights of intellectual property.
[63] L'Organization Africaine de la Propriete Intellectuelle (OAPI) March 2, 1977
(Bangui Accord), as amended on 24 March 1999 and 14 December 2015, relating to intellectual property protection for the 17 West and Central African countries of French expression to which Cameroon is a party.