PIONEER
ACADEMIC PUBLISHING LIMITED

Journal of Research in Social Science and Humanities
ISSN 2709-1910
www.pioneerpublisher.com/jrssh
Volume 3 Number 10 October 2024

Digital Warfare: Exploring Cyber Criminality Amidst Armed Conflict in Southwest Region of Cameroon

Fonjock Harris Kunju[1]

[1] PhD Research Fellow in Law University of Buea, Cameroon
Correspondence: Fonjock Harris Kunju, PhD Research Fellow in Law University of Buea, Cameroon.

doi:10.56397/JRSSH.2024.10.06

Abstract

This research investigates the alarming rise of cyber criminality in the Southwest region of Cameroon, a trend significantly influenced by the ongoing armed conflict that has engulfed the area. Employing a doctrinal research methodology, the study conducts a rigorous content analysis of both primary sources such as case law, treaties, legislative texts, direct observations, and policy documents and secondary sources, including scholarly textbooks, journal articles, comprehensive reports, and various online materials. The analysis utilizes diverse legal reasoning methods, including deductive, inductive, and analogical reasoning. Findings reveal a troubling surge in cyber-criminal activities since the onset of the armed conflict in English-speaking Cameroon, driven by interrelated factors such as rampant unemployment, pervasive economic hardship, widespread illiteracy, and the displacement of individuals. In light of these findings, it is crucial for the Cameroonian government to devise and implement effective strategies that not only combat cyber-crime but also address the socio-economic challenges exacerbated by the conflict. Such comprehensive measures are vital for restoring stability and security in the Southwest region and for fostering a resilient society capable of overcoming the dual impacts of cybercrime and armed conflict.

Keywords: digital warfare, cyber criminality, armed conflict

1. Introduction

The concept of crime is as old as humanity[1] with the advent of technology new categories of crimes have surfaced one of which are crimes committed within the cyberspace; these crimes are termed 'cyber-crimes'. Nowadays, Cyber-crime has become a common phenomenon in the world. Cyber-crime is that group of activities made by people through the creation of disturbance in networks, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own. Cyber-Crime has gained grounds especially as the computer which is the main tool of cyber criminality has become the central device in the commercial, entertainment,

[1] Volo Museum: (2020). The History of Crime and Punishment. Available at https://www.volocars.com>blog (Visited on 2/11/2023)

and government sectors worldwide.[1]

Cyber-Crime can be defined as any criminal activity which takes place through the media of computers, internet or communication technologies recognized by the Information Technology Act.[2] There are a number of illegal activities which are committed over the internet by technically skilled criminals. The first time a cyber-crime was recorded was in the year 1820. This was facilitated by the invention of abacus, which is the earliest form of a computer around 3500 B.C. which was used in India, Japan and China. However, the era of modern computers, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology which marked the ever first recorded cybercrime.[3] This led to the surfacing of other forms of cyber-crime which has today increasingly become a threat to world peace in the domain of technological rights and the use of Cyberspace for E-commerce and other technology and online related activities.

Other recent categories of newly emerged cyber-crimes are cyber-stalking, cyber terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation and so on.[4] Nowadays not all conflicts are fought on physical battlefields. Moreover, some battles are fought digitally through the use of cyber-criminality as tool of conflict. In this regard, Cyber space has become a modern battle field for parties in conflict[5]. Hence, conflicts whether being physical, mental, internal or external can be used as a mode of promoting cyber-criminality. When two or more persons have different point of views on the same subject matter, they tend to spread propagandas and threat against one another through the internet. Furthermore, most African youths as a result of unemployment caused by armed conflicts tend to commit internet fraud and scams as means of income. Thus, Africa as a continent is vulnerable to a range of online criminal activities, including financial fraud, drugs, human trafficking and terrorism.[6] In addition, conflicting parties use conflicting situations as a way of bullying and threatening their opponents online. This situation is very common in the aspect of armed conflicts. Conflict is the contradiction which occur a result of people or parties having different opinions or views of the same matter.[7] Armed conflicts make lots of civilians to lose their jobs. This eventually causes unemployment and poverty which indeed are major causes of cyber-criminality in Africa. Most internally displaced youths (I.D.P) use internet fraud as their last result for survival. Armed Conflict could be international or non-international.

The armed conflict in the English part of Cameroon serves as a breathing ground for cyber- criminality. The armed conflict serves as a cyber space for the commission of cyber-crimes such as online fraud, cyber bullying and identity theft. Moreover, the most engaged cyber-criminals are internally displaced youths (IDP) from the English-Speaking regions of Cameroon where the conflict is highly felt. Many of IDP are forced to abandon their jobs due to insecurity in their areas. As a consequence of unemployment, they engage in cyber- criminality as means for survival. In addition, school boycotts from 2017-2018 in the English-speaking regions as a result of the armed conflict has rendered most youths from those regions idle and uneducated. "*An Idle mind is the devil workshop*"; so, does the idleness of youths emanating from the conflict inspire students to engage in the malicious act of cyber criminality as a mode occupying themselves.

How did the armed conflict in the

[1] Power, ed., "2000 CSI/FBI Computer Crime and Security Survey." Available at https//: govtech.com>archive>Report:CSI/FBI Computer Crime and Security. p. 6 (visited on 7/11/2023)

[2] Osman Goni. (2022, April 1st). The Concept of Cyber-Crime. *Journal of Technology Innovations and Energy*, p. 2. The Wise Publisher, (visited on 8/11/2023).

[3] http://cybercrime.planetindia.net/intro.htm (visited on 10/11/2023)

[4] Osman Goni. (2022, April 1st). The Concept of Cyber-Crime. *Journal of Technology Innovations and Energy*, p. 3. The Wise Publisher (visited 13/11/2023).

[5] Ghernaouti Solange., *Cyber Power,* (1st edition, EPFL Press, Lausanne Switzerland) page ix (visited on 15/11/2023)

[6] Henry Osborn Quarshire "Fighting cybercrime in Africa", Available at http://article.sapub.org>10.5923.j....Fighting Cybercrime in Africa google.com. (visited on 17/11/2023)

[7] Asherry Magalla "Conflict theory in relation to cybercrime Act No.14 of 2015" Available at https.//www.google.com/url?sa=t&source=web&rct=https://papers.ssrn.com (visited on 19/11/2023)

English-speaking regions of Cameroon start? The armed conflict started on 9th September 2017 and it is ongoing. It was so severe that schools in the hinterlands of the English-speaking regions of Cameroon became ineffective as it was unsafe for children to go to school due to secessionist's activities. The conflict emerged from legal and educational grievances in 2016 and has rapidly escalated into a secessionist, political conflict that is threatening the unity of the country with the potential to generate into complex emergency[1]. The conflict is rooted in Cameroon's colonial history which made Cameroon bilingual. Cameroon before the end of WW1 was originally a German territory as a result of the Germano-Duala Treaty of 14th July 1884. Cameroon became a Mandate "B" territory of the League of Nations under the guardianship of Britain and France due to the Treaty of Versailles in 1919 following the defeat of Germany in WW1. Cameroon after the failure of the condominium[2] was split by both Britain and France into 20% and 80% respectively under the Milner-Simon Agreement of 10th July 1919.[3] The French section achieved independence on January 1st 1960 as "La Republic du Cameroun" while their English counterparts were under the British Administration had the option to either merge with La Republic du Cameroun or Nigeria. During a United Nations Plebiscite conducted on February 11th, 1961 the British Southern Cameroons voted to reunite with French Cameroon to form the "The Federal Republic of Cameroon"[4].

In 1972, the Federal Structure of Cameroon was changed to unitary state with name "The United Republic of Cameroon". On February 4th 1984 the name was further changed into "Republic of Cameroon". Since the union of the two Cameroons, the English-speaking Cameroonians who currently constitute around 14% of the population have been complaining of marginalization[5]. This was compounded by the change of name viewed as many as an attempt to erase the minority English-speaking identity and forcefully assimilate them in to the French system. As a consequence, they started several protests against perceived unfair economic and institutional discrimination, marginalization and inequality in the appointments of public administrators. Since the union in 1961, the English-speaking Cameroonians have always complained about Francophone dominance in the state key institutions and government ministries[6].

The current phase of the armed conflict started as a peaceful street demonstration in October 2016 by lawyers and teachers trade union, who amongst many grievances were against the mandatory use of French language in schools and national law courts in the two English-speaking regions. The government responded by inhibiting the protest leaders as a remedy to calm down the situation. The response was the advent of armed secessionist groups since January 2018 demanding for an Independent English-speaking State. Since then, they have been violent armed confrontations between militants of the secessionist group and the central Cameroonian military[7]. The armed conflict has had lots of impact ranging from human rights violation to economic impacts.

The armed conflict is characterized by human rights violation. On January 17, 2017 the government shut down the internet access amongst the population in the conflicting zone. This was regarded by many local and international organizations as an outright violation of the constitutional and human rights to access information and freedom of

[1] Henry Ngenyam Bang and Azibo Balgah. (2022). The Ramification of Cameroon Anglophone Crisis. The conceptual analysis of as a looming complex disaster emergency. *Journal of international humanitarian action*, 2-3 (visited on 21/11/2022).

[2] A joint administration of Cameroon by both Britain and France

[3] Milner-Simon Agreement 1919. Available at https:/jusmundi.com>en-…Milner-Simon Declaration (1919) google.com (visited on 22/11/2023)

[4] Nsonzefe K. (2019). Cameroon-Anglophone crisis: NW Governor partially withdraws ban on motorbike circulation in three subdivisions. Available at http://www.cameroon-info.net/article/cameroon-anglophone-crisis-nw-governor-partially-withdraws-ban-on-motorbike-circulation-in-three-subdi visions-346050.html. (visited 23/11/2023)

[5] Konings P, Nyamnjoh F. (1997). The anglophone problem in Cameroon. *J Mod Afric Stud.*, *35*(2), 207–229. Available at https://doi.org/10.1017/S0022278X97002401. Krippendorf K. (2004). *Content analysis: An introduction to its methodology*, 2nd edition. Sage, London (visited 25/11/2023)

[6] Chereji C, Lohkoko E. (2012). Cameroon: the Anglophone problem. Conflict studies quarterly. Available at https://www.researchgate.net/publication/259178198_Cameroon_the_Anglophone_Problem. (visited 26/11/2023)

[7] HRW. (2018). These killings can be stopped: abuses by government and separatist groups in Cameroon's Anglophone regions. Available at https://www.hrw.org/report/2018/07/19/these-killings-can-be-stopped/abuses-governmentand-separatist-groups-cameroons. (Visited 28/11/2023)

expression[1]. As the saying goes; when two elephants fight the grass suffers. Civilians who are middlemen as a result of the conflict are usually caught up in beatings, torture, untimely death or sexual exploitation from either of the conflicting parties. Most civilian houses have had their houses burnt down as a result of the conflict. This includes houses in more than 170 villages in the conflicting regions. Young girls have been victims of sexual exploitations[2].

In social aspects, the armed conflict has made over 900,000 internally displaced persons (IDP) and 60,000 refugees[3]. Thousands of people have fled to the French-speaking regions and across the border into Nigeria. In villages that are battle fields between national military and secessionists forces, around 80% of the inhabitants have fled to the bushes and neighbouring Nigeria. The armed conflict is having a serious toll on the health of the population. Internally displaced persons and the populace that fed to the bushes are living in unsanitary and unhygienic conditions. There is rampant open-air defecation enabling the possible spread of diseases in the crowded living conditions in the bushes. The most vulnerable are the elderly, pregnant/lactating women, young girls out of school, and children below the age of five years. The insecurity has caused the closure of many health facilities and hospitals especially in rural areas due to numerous attacks and burned downs. Many medical personnel and hospital staff for fear of a strait bullet and kidnapping have fled from hospitals and clinics in such areas[4].

The armed conflict is having huge economic and financial repercussions. Cameroon's Gross Domestic Product growth rate, which was 5.8 in 2015 prior to the crisis, was downgraded to 3.9 in 2019. The Internet shutdown seriously affected Cameroon's economic growth with an estimated loss of Franc CFA 499 billion (US$ 846 million)[5]. Weekly "ghost towns", restrictions on movement and insecurity are hindering business the flow of goods, people, and services. Businesses and transport vehicles that refuse to respect "ghost town" days have been threatened and targeted. A plethora of business premises and markets have experienced vandalism and arson as a result of the conflict. Consequently, hundreds of businesses have been paralysed in the region[6]. Insecurity has forced production and operational activities of the biggest companies in the region like the Cameroon Tea Estate, the Upper Nun Valley Development Authority, and the Cameroon Development Corporation to dwindle. Exports of the major products from the region like banana, palm oil, coffee, and rice production dropped dramatically. Indeed, the Cameroon Development Corporation reduced its operational capacity to 26% and recorded a net loss of Franc CFA 32 billion (around $55.3 million) during the 2018 fiscal year[7]. This has huge implication for employment since the Cameroon Development Cooperation (located on the slopes of Mount Cameroon) is Cameroon's second largest employer with employees from all regions of the country. Unemployment has soared in the region with over 30,000 more people rendered jobless due to the armed conflict. Cameroon's Employers' Association estimated that the formal economy of the region had lost around 6434 jobs by July 2018 and a further 8000 jobs were at risk.

The unemployment rate in Buea the regional capital of the South West Region, for instance rose to 70%. The North West Region's custom department reported revenue losses of over Franc CFA 200 million (around $362,000) for the

[1] Calis T. (2018). Cameroon shuts down the internet for 240 days. Available at https://techtribes.org/cameroon-shuts-down-the-internet-for-240-days/. (visited 30/11/2023)

[2] This is a legal theory developed by Henry Shue in 1986 opining for all states to respect, protect and fulfil the rights of her citizens. It postulates the state as "right bearers" and the state as "duty holder" of human rights of citizens.

[3] Craig J. (2020). Violence and obstruction: Cameroon's deepening aid crisis. https://www.thenewhumanitarian.org/news/2020/03/18/cameroonconfict-aid-crisis. (Visited 30/11/2023)

[4] Egeland J. (2019). OPINION: Africa's next full-blown war can still be averted. https://news.trust.org/item/20190605144519-wlnet. (Visited on 1/12/2023)

[5] Mboumien E. (2018). Assessing the socio-economic internet shut down in the English-speaking regions of Cameroon from a multistakeholder and multisector perspective. Available at https://static1.squarespace.com/static/5a9efdd2f2e6b149480187ea/t/5ad4f4fb88251b5c5ddebd93/1523905789279/ (visited on 4/12/2023)

[6] World Bank. (2017). Country partnership framework for the Republic of Cameroon for the period FY17-FY21. Available at http://documents.worldbank.org/curated/en/480711490925662402/pdf/CPF-CM-Board-vf-February-28-03062017.pdf. (visited on 4/12/2023)

[7] Mbodiam B. (2020). CDC expected to partially resume activities in Q3, 2019. Available at https://www.businessincameroon.com/agriculture/2907-9386-cdc-expected-to-partially-resume-activities-in-q3-2019. (visited on 5/12/ 2023)

2018 fiscal year and the overall losses to Cameroon's economy were estimated at Franc CFA 269 billion (around $489 million) for the same period[1]. Most jobless youths due to the armed conflict tend to practice cyber-criminality as a means for survival. Thus, it is a common phenomenon to find youths creating the image of selling illegal and non-possessed materials online such as drugs and fire arms. In correlation, some sell what they do not possess as in the cases of phishing scams. In addition, offences such as cyber threats, cyber-bullying, intellectual property infringement and hacking and also practiced.[2].

It is very common for individuals to impersonate the separatist fighters of the armed conflict and threaten to attack innocent civilians if ransom is not paid. This is the case of mobile money scam, cyber bullying and conditional threat. Unfortunately, most individuals fall prey to this nature of scam and send huge sums of money for fear of losing their lives. Moreover, these phone call scams are always committed by normal civilians who are not engaged in the armed confrontations of the armed conflict. In addition, cyber-criminals have created fake NGOs pretending to help IDP and victims of the armed conflict. Upon receiving donations, the money is kept in their pockets.

In addition, some cyber-criminals go as far illegally using the logos of honest and renown organizations as the United Nations and International Red cross to commit cyber-crimes as a result of the armed conflict; thereby committing the act of online intellectual property infringement. Moreover, some unemployed IDP youths commit the offence of engaging in telephone sex and cyber-sex. This is done by exposing their body parts through a telephone video call or computer social chat applications respectively for money. Individuals involve in this illegality mostly fall prey to online harassment, cyberbullying and non-consensual distribution of intimate images.

[1] Kindzeka E. (2019). Cameroon's second largest employer crippled by separatist conflict. Available at https://www.voanews.com/africa/cameroons-second-largestemployer-crippled-separatist-confict. (Visited on 5/12/2023)

[2] Phishing scam is the act of creating fake social media accounts to deceive and dupe persons on the internet. Cyber threatening is the act of bullying someone with his/her private information such as one's nudity. Online intellectual property infringement is the illegal use of a company website and logo online. Hacking is the illegal access to an internet account.

2. Regulatory Measures for the Fight Against Cyber Criminality Amidst Armed Conflict in the Southwest Regions of Cameroon

In response to the escalating threat of cyber criminality, Cameroon has adopted a plethora of institutional and regulatory measures aimed at effectively managing modern information and communication technologies. Central to this framework are several key pieces of legislation. Law No. 98/014 of July 14, 1998, which governs telecommunications, establishes the foundational principles for regulating telecommunication services, ensuring fair competition and consumer protection. This law is complemented by Law No. 2010/013 of December 21, 2010, which addresses Electronic Communications. The subsequent amendment in April 2015 further refines its provisions to adapt to the rapid technological advancements and emerging challenges in the digital landscape.

Additionally, Law No. 2010/012 of December 21, 2010, specifically targets Cyber Security and Cybercrime, providing a comprehensive legal framework for preventing and combating various forms of cyber criminality, such as hacking and identity theft. This law establishes penalties for offenders and outlines the responsibilities of service providers in maintaining security protocols. Furthermore, Law No. 2010/021 of December 21, 2010, governs Electronic Commerce, facilitating safe online business transactions while ensuring consumer protection and fostering trust in electronic trading environments. Together, these legislative measures create a cohesive legal structure that addresses the multifaceted nature of cyber crime.

To enhance the effectiveness of these laws, Cameroon has established various institutional mechanisms. The Ministry of Post and Telecommunications plays a crucial role in formulating policies related to telecommunications and managing information technologies. In tandem, the Ministry of Communication oversees media regulation and public awareness initiatives regarding cyber security issues, promoting safe online practices among citizens. The Telecommunication Regulatory Board acts as an independent regulatory body ensuring compliance with telecommunications laws and monitoring service providers' adherence to security standards.

Moreover, the National Agency for Information and Communication Technology (ANTIC) is pivotal in implementing national strategies for cybersecurity and information technology development. ANTIC conducts research, provides technical assistance, and collaborates with international partners to bolster cybersecurity measures. Additionally, Cameroon works with INTERPOL to facilitate cooperation among member countries in combating transnational cyber crime. The national judiciary also plays a significant role in adjudicating cyber crime cases, interpreting relevant laws, and establishing legal precedents that shape the enforcement of cyber crime legislation. Despite these efforts, ongoing challenges such as inadequate technical infrastructure and limited public awareness necessitate continued investment in capacity-building initiatives and public-private partnerships to enhance the nation's resilience against cyber threats.

The Cameroonian government has implemented various legal and institutional measures to address the complexities of cyber-criminality, particularly in the context of the ongoing armed conflict in the English-speaking regions. The legal framework includes significant statutes such as the 1996 Constitution, which enshrines fundamental rights and freedoms, and Law No. 2014/028 on the Suppression of Terrorism, which criminalizes acts of terrorism and provides a basis for prosecuting cyber-related offenses linked to such activities. Additionally, the Penal Code encompasses provisions that address cyber-crimes, allowing law enforcement agencies to tackle offenses such as hacking, identity theft, and online harassment, thereby enhancing the state's capacity to respond to the evolving landscape of digital threats.

Institutional mechanisms play a crucial role in complementing these legal frameworks. The establishment of the Bilingualism Committee aims to foster understanding and cooperation among diverse linguistic communities, potentially mitigating tensions that could lead to cyber-criminal activities. Furthermore, the creation of Common Law Benches at both the Supreme Court and the National School of Administration and Magistracy (NSAM) signifies an effort to integrate common law principles into the judicial system, which may enhance legal predictability and fairness in handling cyber-crime cases. These institutions not only provide legal training but also promote a more cohesive approach to justice, which is essential in a region grappling with conflict.

In response to the unique challenges posed by the armed conflict, the government has also initiated measures such as Internet seizures in conflict areas. While this can be seen as a means to prevent the dissemination of harmful content or coordination among insurgents, it raises concerns regarding freedom of expression and access to information. Striking a balance between security and civil liberties remains a critical challenge for authorities. Additionally, the re-education of Cameroonian history in universities aims to foster national unity and resilience against extremist narratives that often proliferate online, thus addressing one of the root causes of cyber-criminality.

Finally, the rehabilitation of ex-secessionist soldiers represents a proactive approach to reintegration and peacebuilding. By providing these individuals with opportunities for education and employment, the government seeks to reduce the likelihood of their involvement in cyber-criminal activities. This multifaceted strategy underscores the importance of not only punitive measures but also restorative practices in combating cyber-crime. Overall, while these legal and institutional measures are commendable steps towards addressing cyber-criminality in Cameroon, ongoing evaluation and adaptation will be crucial to ensure their effectiveness in an ever-evolving digital landscape.

3. Effectiveness of Measures for the Fight Against Cyber-Criminality Amidst the Armed Conflict in the South West Region of Cameroon

Despite the existence of a regulatory framework, the ongoing armed conflict in the English-speaking regions of Cameroon has significantly worsened cyber-criminality in the region. An interview with registrars at the High Court of Fako revealed a staggering 30% increase in incidents of cyber-terrorism since the conflict began. Additionally, MTN Cameroon has reported an alarming 80% rise in mobile money scams in the South West region during this period. Although several regional instruments address cyber-criminality, there is no unified, internationally recognized binding law governing this issue. The limited applicability of these instruments is due to many states not having signed or ratified them. This

lack of a cohesive legal framework presents considerable challenges for investigating and prosecuting cyber criminals, especially given the cross-border nature of many offenses. Often, perpetrators reside in one country while their victims are located in another, highlighting the urgent need for international collaboration between the state where the crime occurred, and the state affected by its consequences.

According to reports from the ANTIC regional office for the South West, there has been a notable rise in cybercrime linked to the armed conflict, with conditional threats increasing by 29%, scams by 21%, cyber-terrorism by 14%, and cyber-blackmail by 11%. Secondly, with reference to the recent UN General Assembly resolution on cyber security,[1] which addresses cybercrime as one major challenge, though it is difficult to quantify the impact of cybercrime on society, one may say without contradiction that cybercrime has made it difficult for developing countries to promote e-business and participate in online service industries. [2] In 2014, anti-corruption commission reported that "cyber criminality cost 3.5 billion to Cameroon between November and December 2013".[3] For Abeng, scammers are still doing a brisk business because there has been more talk than action. He recounted the story of a British national who came to Cameroon to track down scammers who fleeced out millions of pounds, but unfortunately, he was found dead in the capital city of Cameroon, Yaoundé.[4] These statistics indicate the growing trend of cyber criminality in Cameroon in the past years which has been orchestrated primarily by the recent upsurge in the number of internet users and the lack of employment in Cameroon causing many youths to engage in such activities.

Furthermore, from the recent report of The National Agency for Information and Communication Technologies (ANTIC over 90% of software and operating systems used in Cameroon are hacked including email addresses and social media accounts of businesses, individuals and government members resulting to lamentable losses for operators, individuals, businesses and the state.[5] Assongmo has elaborated on the prevalence of telephone fraud in Cameroon, highlighting alarming statistics. In 2015, the mobile phone sector reported losses of 18 billion FCFA for operators and an additional 46 billion FCFA for the state. These significant losses have created more opportunities for internet fraudsters to exploit online platforms for cybercrimes. In response to the growing threat of cyber-criminality, Cameroon has implemented several measures aimed at controlling this issue. Key legal frameworks include the 2010 Law on Cybersecurity and Cyber-criminality, the 2016 Penal Code, and the 2005 Criminal Procedure Code. These laws outline the procedures for investigating cyber offenses and designate Judicial Police Officers as the officials responsible for these investigations.

Furthermore, to combat the rising tide of cybercrime, the Cameroonian government has established forensic centers dedicated to training students in effective cybersecurity practices. These centers aim to enhance the protection of cyberspace and equip future professionals with the necessary skills to address cyber threats.[6] This is still very challenging as many culprits to walk home free because of evidence to prove beyond reasonable doubt facts that can incriminate them caused mainly by the complex nature of cybercrime. Magistrate Eware Ashu affirms the complex nature of cyber, crimes and the difficulty in proving them, but held that "... it should not be an excuse for resorting to illegal short cuts to secure a conviction."[7]

Furthermore, this research explores the challenges encountered in the investigation for the prosecution of cyber-criminality and as per data obtained at the police station in Buea. According to the department in charged in the investigation and tracking of cyber-criminals in

[1] UNGA Resolution: Creation of a Global Culture of Cyber Security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[2] M. Gercke. (2012, September 12). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. (2nd edition) pp. 4-12. Available: itu.int/ITU-D/cyb/cybersecurity/legislation.htm [date accessed Jun. 4, 2019]

[3] voa.com. "Cameroon urged to Act against cybercrime." USENET: https://www.google.com/amp/151740.htm, Feb. 10, 2011 [Feb.10, 2018].

[4] *Ibid*, 408.

[5] Assongmo. (2016, Sep. 9). "Cameroon is a Country vulnerable to cyber-criminality" USENET: https.//www.google.com/amp/s/www.businessincameroon.com/index.php [Mar. 24, 2019].

[6] In 2015 a center for digital forensic and cybersecurity under the University of Buea in partnership with the Ministry of Post and Telecommunication and university of Bloomsburg in the U.S. according to the director of the centre, Joan Waka, their mission is to "train young Cameroonians on how to protect the country's cyberspace."

[7] CFIB/015f/2012 unreported.

Molyko Buea Police station the main difficulty in accomplishing this task is the lack of tools which are used for the investigation of such crimes. Hence, the only mean available to them through investigation is through social engineering which according to them is not producing the needed result reasons why cyber-crime remains on a steady rise[1].

Furthermore, the challenging nature of the eradication of cyber-crime in Cameroon and particularly in the south west region of Cameroon is as a result of the fact that cyber-crime has taken a multi-dimensional approach recently, as they exist conditional threat, cyber pornography, cyber-sex, sexting, mobile money scam and so on. The tools made available to ensure the security of cyberspace and investigation of cyber-criminals are therefore insufficient and cannot stand the test of time particularly with the skyrocketing nature of cyber-criminality in the southwest region. This situation is further escalated by the fact that the unit of national security of the National Gendarmerie are the one and ANTIC are the sole persons at the disposal of these tools. Thus, many reported cases of cyber-crime at the level of police can only be investigated through social engineering which today with modern techniques of cyber-criminality are not efficient.[2]

4. Conclusion and Recommendations

Historically, crime has required both intent and a physical act, necessitating the presence of both the perpetrator and the victim. However, in recent times, criminal activity has shifted towards cyber-criminality, where many offenses are committed solely in cyberspace. In Cameroon, the rise in cyber-criminality can be attributed to a lack of awareness among the population and insufficient measures to combat these crimes. Since early 2018, the increasing rate of cyber-criminality has become alarmingly evident. The regional branch of ANTIC for the South West region has reported that the rate of cyber-crime has skyrocketed, particularly in the Fako Division, largely due to the ongoing armed conflict. It is clear that this conflict has exacerbated the level of cyber-criminality in the South West region of Cameroon.

This research study concludes that the recent surge in cyber-criminality in the South West region of Cameroon is driven by several factors, primarily unemployment and poverty, both of which have been exacerbated by ongoing armed conflict. This conflict has displaced many individuals from their homes and jobs, resulting in significant suffering, property destruction, and temporary business shutdowns. Consequently, citizens are left in precarious survival situations, which significantly contributes to the rise in cyber-criminality.

Additionally, this study provides an in-depth conceptual analysis of cyber-criminality and its relationship with armed conflict. It explores various types of cyber-crime and defines the concept itself. The study also examines armed conflict, particularly in the context of the two English-speaking regions of Cameroon, framing it within the scope of non-intentional armed conflict and its link to cyber-criminality, especially in light of the ongoing situation in the North West and South West regions.

Furthermore, the research highlights challenges faced by institutions responsible for investigating and prosecuting cyber-criminals. The investigation of cyber-crime falls under the jurisdiction of judicial police officers, who may lack expertise in this area. This issue is compounded by the fact that investigative tools are primarily available to the National Gendarmerie, leading to situations where reported cases of cyber-crime go uninvestigated. In many instances, judicial police officers are limited to using social engineering techniques, which may not be effective given modern technological advancements.

The study also sheds light on a compendium of legal provisions adopted by the Cameroonian legislature, including laws, decrees, and international conventions ratified by the state to govern and regulate cyber-crime and cyber security. The promulgation of these laws serves a deterrent effect, discouraging potential offenders from committing cyber-crimes due to fear of punishment. The alarming increase in cyber-crime over the past two decades poses significant challenges. The transnational nature of these offenses has intensified recently, undermining globalization efforts and hindering e-commerce, which is vital for today's business landscape. Various stakeholders, including civil society organizations (CSOs), non-governmental organizations (NGOs), and the Cameroonian government, have implemented numerous

[1] Based on an interview carried out at the Molyko-Police Station Buea on the 6th of August 2024.

[2] Interview obtained at Molyko Police department in charge of tracking and investigation of cyber-criminals.

measures aimed at curbing cyber-crime in the South West region and ensuring cyberspace security.

This research is highly relevant as it addresses issues with far-reaching negative repercussions for both the national and international business economy of Cameroon. Based on the findings outlined above, the study presents several recommendations. First, the research recommends the establishment of a specialized branch within both the police force and the national gendarmerie, specifically a "Special Force for the Investigation of Cybercrime" or a "Department for the Investigation of Cybercrime."

Additionally, it is recommended that cybercrime and cybersecurity be incorporated as core courses for all Judicial Police Officers. According to the Cameroonian Criminal Procedure Code, these officers are tasked with investigating crimes within their jurisdiction. This training will enhance their knowledge and effectiveness in investigating cyber-related offenses. The study also strongly advocates for the creation of Divisional and Sub-Divisional sections of the National Agency for Information and Communication Technologies (ANTIC). Currently, ANTIC has only a national bureau in Yaoundé and regional branches in each of the ten regions, leaving towns in the South West region—such as Kumba, Tombel, Mamfe, and Menji—without divisional representation.

Furthermore, the research suggests implementing cybersecurity and cybercrime education at the secondary and high school levels in Cameroon. This is crucial because many victims of cybercrime are individuals with little or no knowledge of how to navigate cyberspace securely. According to a 2020 ANTIC awareness seminar, the rising incidence of cybercrime is largely due to users' lack of essential knowledge, making them vulnerable to exploitation. The regional director of ANTIC for the South West region expressed concern that without proactive awareness campaigns, cybercrime will continue to rise.

The study also recommends establishing a commission to monitor the activities of institutions responsible for investigating and prosecuting individuals suspected of cybercrimes. This oversight will promote accountability and transparency in the investigative process, as current efforts appear insufficient, likely due to the lucrative nature of cybercrime. Moreover, the research proposes creating a cyber-security sector within all telecommunications networks in Cameroon. This would facilitate tracking cybercriminals who utilize services from MTN, ORANGE, or CAMTEL. Establishing this sector would enhance internet security for users and provide security codes and customer care services. Users who suspect any manipulation on their online platforms could quickly report issues for immediate identification and temporary suspension of those platforms for rectification.

Finally, the study recommends extending mobile network services to remote areas lacking connectivity. This recommendation arises from challenges faced by law enforcement in tracking cybercriminals in regions with inadequate or nonexistent network signals. The destruction of stationary network equipment, such as antennas and satellite dishes, has further exacerbated access issues in these areas.

References

Adejoke Oyewunmi. (2013). The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions. *British Journal of Arts and Science*.

Adejoke, O. (2013). The ICT Revolution and Commercial Sectors in Nigeria: Impacts and legal inventions. *British Journal of Arts and Science*, 234-247.

Adidi, S.A.H. (1990). *Communication, Information and Development in Africa*. Uganda: Abidi Publishers.

Ajapokvi, M. (2001). Domain Names and Trademarks in Nigeria. *Modern Practice Journal of Finance and Investment law*, 202-207.

Ajayi, E. F. (2016). Challenges to Enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*, 1-12.

Ajibade, A. (2008, October). A Synopsis: Rights, Responsibilities, and Role of Human Rights NGOs under International Law. *Electronic Journal*, p. 9.

Al-gasseer, N., Dresden, E., & Brumbaught, G. (2010). Status of Women and Infants in Complex Humanitarian Emergencies. *Midwifery & Women's Health*, *49*(1).

Ali, S. (2010). ICT, the New Media (Internet) and Development: Malaysian Experience. *The*

Innovation Journal, *15*(1), 5-15.

Alvaro, C. (2006). Who cares about corruption? *Journal of International Business Studies*, *37*(6), 807-822.

Beth, A. (2006). Breaching the Vacuum: A consolidation of the role of International Human Rights Law in the operations of International Financial Institutions. *The International Journal of Human Rights*, *10*(8), 389-398.

Boraine, A. & Ngaundje, L. (2019). The Fight against Cyber Crime in Cameroon. *International Journal of Computer (IJC*), *35*(1), 87-100.

Bryan A.G. (1999). *Black Law Dictionary*. USA: West Publishing Co.

C. Michael. (2008). *Scene of the Cybercrime*. Location: Syngress Publishing Inc, London, p. 35.

Chinasa, M. (2014). The telecommunication industry and the policy making process: an Appraisal under the Nigerian Communication Act 2003. *University of Jos Law Journal*, *9*(2), 299-316.

Coaldrake, P. & Seidman, L. (1998). *On the Brink.* Brisbane: University of Queensland Press.

Ellen L. Latz. (2006). Understanding Human Rights Violations in Armed Conflict. Julie A. Mertus and Jeffrey W. Hellsing (Eds.), *Human Rights Laws and Peace Building*, Washington DC, United States Institute of Peace.

Emmanuela-Chiara Gillard. (2016, October). Promoting Compliance with International Humanitarian Law. *International Law Programme*.

Giesela Rühl. (2011). Consumer Protection in Choice of Law. *Cornell International Law Journal*, *44*.

Giesela, R. (2011). Consumer Protection in Choice of Law. *Cornell International Law Journal*, *44*, 571.

Gillian, H. (1998). Information-Based Principles for Rethinking Consumer Protection Policy. *Journal of Consumer Policy*, *21*, 34.

Hawkins, G. (1979). *The evolution of corrections in America*. Chicago: West Publishing series.

Ikengha, K. E. (2014). The Internet and its Facility for Criminality: Some unique difficulties for prosecution. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 12-26.

J.W.C. Turner. (1966). *Kenney's Outlines of Criminal Law*. 19th Edition, University Press, Cambridge.

Lerner, D. (1958). *The Passing of Traditional Society: Modernizing the Middle East.* New York*:* The Free Press.

Lydesdorff, L. (2001). *A Sociological Theory of Communications: The Self-Organization of Knowledge-based Society*. London: Universal Publishers.

Maras, M. (2016). *Criminology.* New York: Oxford University Press.

Mills, A. (2014). Rethinking Jurisdiction in International Law. *British Yearbook of International Law*, *84*(1), 187-239.

Nwabueze C. (2017). Reflections on Legal Uncertainties for e-Commerce Transactions in Cameroon. *The African Journal of Information and Communication*, *20*, 171-180.

Organski, A.F.K., & Kugler, J. (1980). *The War Ledger*. Chicago: University of Chicago Press.

Pye, L. (1963). *Communications and Political Development*. New Jersey: Princeton University Press.

Roxanna Willis. (2019, October 30th). Human Rights Abuses in The Anglophone Crisis. University of Oxford Faculty of Law.

Schramm, W. (1964). *Mass Media and National Development: The Role of Information in the Developing Countries*. Stanford, California: Stanford University Press.

Shue, H. (1980). *Basic Rights: Subsistence, Affluence and US Foreign Policy*. Princeton: Princeton University Press.