DOI: https://doij.org/10.10000/IJLMH.119101

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

A Legal Appraisal of the Mechanism for the Execution of Measures to Combat Cyber Crimes in Contemporary Africa: The Cameroonian Perspective

DR. TASIKI DESVARIEUX NTOBENGWIA[1] AND DR. NDUNG CHANTAL MBONG[2]

ABSTRACT

''We cannot build a digital economy in Africa without cyber security''. The growing nature of cybercrimes in Africa has necessitated the growth of effective mechanisms for the execution of measures to combat these crimes. This study undertakes a legal appraisal of the mechanism for the execution of measures to combat cybercrimes in Cameroon, with a view to identifying the strengths and weaknesses of the existing framework. Using a doctrinal research approach, this study analyzes the Cameroonian Cybercrime Law of 2010, as well as other relevant laws and regulations. The findings of this research reveal that while Cameroon has made significant efforts to combat cybercrimes, the existing mechanism for the execution of measures to combat cybercrimes is inadequate and ineffective. The study recommends the adoption of a more comprehensive and nuanced approach to combating cybercrimes in Cameroon, including the development of specialized cybercrime units, the establishment of a national cybercrime reporting system, and the provision of training and capacity-building programs for law enforcement officials. This study therefore, contributes to the existing body of knowledge on cybercrime and the law in Africa, and provides a framework for the development of effective mechanisms for the execution of measures to combat cybercrimes in Cameroon and other African countries.

***Keywords**: Cybercrime, Cyber Security, Cameroon, Africa, Enforcement Mechanism, Legal Appraisal.*

I. INTRODUCTION

The arrival of the internet and other numerical technologies has transformed the way human being in contemporary Africa live, work, and interact with one another.[3] However, this digital

[1] Department of English Law, Dschang School of Law and Political Science, University of Dschang, Dschang, Cameroon.

[2] Department of English Law, Dschang School of Law and Political Science, University of Dschang, Dschang, Cameroon.

[3] Akpabio, I. (2020), "Cybercrime and the Nigerian Legal System", Journal of Law, Policy and Globalization, 84, 12-20.

revolution has also created new opportunities for criminal activity, including cybercrime.[4] Cybercrime refers to any criminal activity that involves the use of computers, computer networks, or other digital technologies to commit or facilitate illegal acts[5] or any acts in respect to cyber systems or "a range of offences including traditional computer crimes, as well as network crimes".[6]

In Africa, the rise of cybercrime has been particularly pronounced, with many countries on the continent struggling to develop effective mechanisms for combating these crimes.[7] Cameroon, in particular, has been identified as a hub for cybercrime activity in Central Africa.[8] The country's relatively well-developed telecommunications infrastructure, combined with its strategic location and lack of effective regulation, has made it an attractive target for cybercriminals.[9]

That is, the dominance of cybercrimes in Cameroon is disturbing. Cameroon today is one of the countries in Africa that have accepted the use of the internet and other technology tools to engage in personal and business activities. This wide acceptance of internet technology in Cameroon has led to an increase in cybercrimes in Cameroon. Cybercrime come in the form of; fraudulent electronic emails, identity theft, cyber harassment, spamming, pornography and hacking thus making internet extortion in Cameroon a threat to the lives of Cameroonians, their economy and the reputation of Cameroonians in the international scene thus combating cybercrime in Cameroon is necessary.

The government of Cameroon in his drive to fight against cybercrimes targeted to foreigners, individuals and corporate institution has promulgated the law on cybersecurity and cyber criminality in 2010.[10] That is, the Cameroonian government has taken steps to address the growing problem of cybercrime, including the passage of the Cybercrime Law of 2010.[11]

[4] Clough, J. (2015), Principles of Cybercrime, Cambridge University Press.

[5] Carter, Computer Crime Categories: How Techno-Criminals Operate", FBI Law Enforcement Bulletin, 1995, p21. Available at www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf, April. 25, 1995.

[6] M., Gercke, (2012, September 12), Understanding Cybercrime: Phenomena, Challenges and Legal Response. (2nd edition)‟ (On-line). p12). Available: itu.int/ITU-D/cyb/cybersecurity/legislation.htm

[7] Akinade, O. (2019), "Cybercrime in Africa: A Review of the Literature", Journal of African Law, 63(2), pp.147-163.

[8] Assongmo, "Cameroon is a Country vulnerable to cyber-criminality" USENET: https.//www.google.com/amp/s/www.businessincameroon.com/index.php, Sept. 9, 2016 (March 2, 2024).

[9] Brenner, S. W., (2012), Cybercrime and the Law: Challenges, Issues, and Outcomes, Northeastern University Press.

[10] Internet extortion in Cameroon takes the form of; phishing (theft of identity), theft of bank cards, cyber pornography, scams, software piercing, sales frauds & forgery data & airtime, charity fund, hacking and theft of network service. Here are some of the causes of internet extortion in Cameroon; unemployment, quest of wealth by youths, incompetent security and control on a personal computer.

[11] Law No.2010/012 of 21st December 2010, on Cyber Security and Cybercrime in Cameroon.

However, despite these efforts, cybercrime remains a significant challenge for the country. The lack of effective enforcement mechanisms, combined with inadequate training and resources for law enforcement officials, has hindered efforts to combat cybercrime in Cameroon.[12] Furthermore, the impact of cybercrime on individuals, businesses, and society as a whole cannot be overstated. Cybercrime can result in significant financial losses, damage to reputation, and compromised personal data.[13] In addition, cybercrime can also undermine trust in institutions and the rule of law, with far-reaching consequences for economic development and social stability.[14]

In light of these challenges, it is essential to conduct a comprehensive analysis of the mechanism for the execution of measures to combat cybercrime in Cameroon. This study aims to provide a critical examination of the existing framework, highlighting strengths and weaknesses, and identifying areas for improvement. By doing so, this research seeks to contribute to the development of effective mechanisms for combating cybercrime in Cameroon, and to inform policy and practice in this critical area.

II. An overview of the role of African state in the fight against cybercrimes

The government of African states, especially Cameroon plays a preeminent role as far as cyber security and cyber criminality is concerned. These roles shall be examined looking at the ratification of international treaties relating to the fight against cybercrimes, the enactment of domestic legislations, the establishment of institutional framework etc.

(A) Ratification of International Treaties Relating To the Fight against Cybercrimes

To address the problem of widespread of Cybercrime in contemporary Africa, so many governments in Africa have adopted collective legitimate frameworks to fight against cybercrime.[15] Cameroon has indeed taken steps to combat cybercrime and cyber security threats by ratifying and participating in several international treaties and conventions. In 1981, an International Telecommunication Convention (ITU) and additional protocols were adopted; granting member states the authority to stop any internet or cable transmission of private

[12] Mbarika, V. W. (2017), "Cybercrime in Cameroon: An Exploratory Study", Journal of Cyber security, 3(1), 1-12.

[13] African Union, (2014), "African Union Convention on Cyber Security and Personal Data Protection".

[14] Jaishankar, K., (2011), Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, CRC Press.

[15] 15 E., Akuta and J., Ongloa, (2011), “Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy and Practice.”J Peace Gender and Development studies, pp.129-137.

telegrams that may loom state security.[16] According to this law, States have the right to stop any transmission without necessarily notifying the State where it came from.[17] Cameroon is a member of the ITU and has participated in various conventions and agreements related to telecommunications and cyber security.

Also, the African Union implemented a Convention on Cyber Security and Personal Data Protection to enhance cooperation among African states in tackling cybercrime.[18] However, not all states have ratified this convention.[19] Although Cameroon is not yet a party to this convention, it has expressed commitment to enhancing cyber security and data protection in the region.

Furthermore, regional groups such as the Central Africa Economic and Monetary Community (CEMAC) have validated a General Convention on Judicial Cooperation, signed under the former African and Malagasy Common Organization, covering French-speaking countries in West and Central Africa. Stationary, there are agreements such as the Extradition Agreement among the Member States of the Central African Economic and Monetary Union (CAEMU/CEMAC) of 2004[20], the Extradition Agreement of the Economic and Monetary Community of Central Africa (CEMAC), and the London Scheme for Extradition within the Commonwealth. Another CEMAC Regulation was adopted in 2013 for the prevention and suppression of money laundering and financing terrorism in Central Africa. It is imperative to note that cyber terrorism involves unlawful attacks and threats against computers, networks, and stored information.[21] These cyber-attacks are sometimes committed to threaten or coerce a government or its people in search of political or social goals.[22]

Albeit global cooperation is the answer to better challenge and combat cybercrime, it sadly appears that the efforts made so far in African nations are inadequate, as cyber-attacks are still widespread today. As a matter of fact, Cameroon and most African nations are not parties to relevant international cybercrime conventions (like the Budapest Convention and the AU Convention on Cyber security), and that puts the African continent in a delicate and defenseless position to combat the wonder of cybercrime. The author therefore suggest that the indifference of Cameroon and other African nations in ratifying relevant international conventions relating

[16] Article 19(1) of the Constitution and Convention of the International Telecommunication Union 1981.
[17] Ibid, article 34(1).
[18] Article 28 of the African Union Convention on Cyber Security and Personal Data Protection.
[19] States like Cameroon, Nigeria, South Africa and a host of others are not party to the convention.
[20] A. Harriette and A. P. Samuel. “Extradition within the CEMAC Sub Region: Prospects and Perspectives”. International Journal of Trend in Scientific Research and Development (IJTSRD), Vol. 3(6), pp 566,575, 2019.
[21] C. Robert, H. Friman, et al., An Introduction to International law and Procedure (2nd Edt, Cambridge University Press, 2010) p343.
[22] M. N. Sirohi, (2018), Cyber Terrorism and Information Warfare, (New Delhi: Alpha Editions, 2015), p23.

to cybercrime contributes more to the reason why the crime upsurge over the internet is still perennial.[23] Thus, study undertakes a legal appraisal of the mechanism for the execution of measures to combat cybercrimes in Africa in general and Cameroon in particular, with a view to identifying the strengths and weaknesses of the existing framework.

(B) The Enactment of National Legislations

Nationally, plethora of domestic legislations exists in Cameroon for the fight against cybercrimes in Cameroon. The main piece of legislation governing Cyber Security and Cybercrimes in Cameroon is law no. 2010 relating to Cyber Security and Cybercrime.[24] This law specifically provides a framework for investigating, prosecuting, and punishing cybercrimes in Cameroon. This law also provides substantive and procedural rules relating to international cooperation.[25] There is also law no. 2016 relating to the penal code in Cameroon with provisions related to cybercrime, including articles on hacking, identity theft, and online harassment. Furthermore, there is also law No. 2000/018 of 20 December 2000 on Telecommunications which provides guidelines for the protection of personal data in the telecommunications sector. That is, this decree provides detailed guidelines for the protection of personal data, including the rights of data subjects and the obligations of data controllers.

Equally, there is law no. 2010 on electronic communication which provides guidelines for telecommunications operators to prevent and respond to cybercrimes.[26] There is also decree no. 2012[27] on the protection of personal data which provides detailed guidelines for the protection of personal data, including the rights of data subjects and the obligations of data controllers. Equally, there is also order no. 002 on the protection of personal data in the Telecommunications sector which provide guidelines for protecting personal data and preventing data breaches.[28] That is, this order provides guidelines for the protection of personal data in the telecommunications sector. Other laws regulate the cyber-criminal activities due to their inter relationships such as the Criminal Procedure Code[29] provides for the procedures for investigating and prosecuting cybercrimes. Section 52 (1) of the 2010 cyber law in Cameroon is to the effect that in case of any cyber offence, Criminal Investigation Officers with general jurisdiction and authorized officials of the Agency shall carry out investigations, in accordance

[23] U. O Jerome. "The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability?" Masaryk University Journal of Law and Technology, Vol. 12 N0 2, pp.90-129.

[24] Law No.2010/012 of 21st December 2010, on cyber security and cybercrime.

[25] Section 90(1)(2) of the cyber law op cit.

[26] Law No. 2010/013 of 21st December 2010 on electronic communication in Cameroon.

[27] Decree no. 2012/286 of 12 July 2012 on the protection of personal data.

[28] Order no. 002/CAB/MINPOSTEL of February 2014, on the Protection of Personal Data in the Telecommunications Sector in Cameroon.

[29]The Cameroon Criminal Procedure Code of 2005.

with the provisions of the Criminal Procedure Code. Searches and seizures shall be carried out in accordance with the provisions of the Criminal Procedure Code, taking into account the loss of validity of evidence.[30]

(C) The Creation of Institutional Frameworks for combating cybercrime

Under the institutional framework, several institutions have been set up in Africa in general and Cameroon in particular regulating cyberspace as seen below.

a. National Institutional Frameworks

The government of Cameroon in his action to combat computer crimes & security threats (cybercrimes) targeted to foreigners, individuals and corporate institution, has established several institutions that provide a framework responsible for regulating and monitoring the use of ICTs in Cameroon, including investigating cybercrimes. The different institutions include:

i. National Agency for Information and Communication Technologies (ANTIC)

In Cameroon, ANTIC is the national agency responsible for regulating and promoting the development of information and communication technologies (ICYs) in the country.[31] ANTIC works closely with other government agencies, private sector organizations, and international partners to achieve its objectives and promote the development of the ICT sector in Cameroon. ANTIC was also instituted to regulate Cameroon's cyberspace.[32] This agency has the prerogative to establish cooperation ties with other foreign authorities under section 90 of the Cyber law. ANTIC is responsible for regulating and monitoring the use of ICTs in Cameroon, including investigating cybercrimes.[33] The National Agency for Information and Communication Technologies (ANTIC) plays a crucial role in combating cybercrime in Cameroon such as:

- ANTIC helps raise awareness about cyber threats and strengthens the technical capacity to deter cybercrime and enhance cyber security;
- ANTIC works with the judiciary and law enforcement agencies to investigate cybercrimes and provide technical expertise;

[30] See section 54 of the 2010 cyber law op cit.

[31] Presentation of ANTIC, available at https://www.anti.cm/index.php/en/the-agency/presentation.htm/viewed on November 15, 2024.

[32]https://www.antic.cm/images/stories/laws/Law%20relating%20to%20cybersecurity%20and%20cybercriminality%20in%20Cameroon.pdf

[33] Section 8 (1), Cyber Law provides "… ANTIC shall be the Root Certification Authority (2) … ANTIC shall be the Certification Authority of the Public Administration."

- ANTIC participates in developing national strategies to fight cyber criminality, including organizing conferences and seminars;
- ANTIC collaborates with international organizations, such as the Commonwealth Telecommunications Organisation (CTO), to stay updated on best practices in cyber security;
- ANTIC provides training and capacity-building programs for magistrates, law enforcement officers, and the general public on cyber security and cybercrime.

By fulfilling these responsibilities, ANTIC plays a vital role in protecting Cameroon's digital economy and ensuring the safety of its citizens online.

ii. Ministry of Posts and Telecommunications (MINPOSTEL)

Personal data leakage, massive hacking of Facebook accounts particularly those of top officials, identity theft, fake news, hate speeches and fabricated images all aimed at discrediting Cameroon are some of the malicious acts practiced on the internet and social media. These acts have greatly contributed to the current prevailing socio-political climate in Cameroon. MINPOSTEL is responsible for developing and implementing policies related to ICTs, including cybersecurity.[34] That is, ANTIC is responsible for regulating and monitoring the use of ICTs in Cameroon, including investigating cybercrimes. Some of the key responsibilities of MINPOSTEL include:

- MINPOSTEL has organized workshops and forums to raise awareness about cyber security and cybercrime, and to develop strategies to combat these issues.[35]
- The ministry has developed emergency plans to tackle rising cybercrime threats, including fake social media accounts and business email compromise (BEC) attacks.
- MINPOSTEL partners with international organizations, such as the International Telecommunication Union (ITU) and the Commonwealth Telecommunications Organization (CTO), to stay updated on best practices in cyber security and cybercrime prevention.

[34] Order No. 002/CAB/MINPOSTEL of 24 February 2014 on the Protection of Personal Data in the Telecommunications Sector: This order provides guidelines for the protection of personal data in the telecommunications sector.

[35] Minister of Posts and Telecommunications Minette Libom Li Likeng, on Thursday 3rd March, 2022, in the conference hall of the ancillary building of her ministerial department, chaired a 1 day sectorial workshop on cybersecurity in Cameroon.

- The ministry works to harmonize laws and regulations on cyber security and cybercrime in the Central African region.
- MINPOSTEL builds capacity and raises awareness among stakeholders, including government institutions, private businesses, and citizens, to promote a culture of cyber security in Cameroon.[36]

By fulfilling these responsibilities, MINPOSTEL plays a crucial role in protecting Cameroon's digital economy and ensuring the safety of its citizens online.

iii. The Ministry of Justice

The Ministry of Justice is responsible for prosecuting cybercrime cases and ensuring that cybercrime laws are enforced. The Ministry of Justice in Cameroon plays a vital role in combating cybercrime. Ministry of Justice key responsibilities include:

- The Ministry of Justice works closely with law enforcement agencies to investigate and prosecute cybercrime cases.[37]
- The Ministry is responsible for developing and implementing laws related to cybercrime, including the Cyber security and Cyber criminality Law of 2010.[38]
- The Ministry collaborates with international organizations, such as the International Telecommunication Union (ITU), to stay updated on best practices in cyber security and cybercrime prevention.[39]
- The Ministry provides training and capacity-building programs for judges, prosecutors, and law enforcement officers on cyber security and cybercrime.[40]
- The Ministry raises awareness about cybercrime and its consequences among the general public, businesses, and government institutions.[41]

Overall, the Ministry of Justice plays a critical role in combating cybercrime in Cameroon by investigating and prosecuting cybercrime cases, developing and implementing cybercrime laws, collaborating with international organizations, providing training and capacity building, and

[36] https://www.minpostel.gov.cm/index.php/en/les-grands-chantiers/138-cameroon-digital-strategic-plan-2020

[37] See generally Prof. André Borainea, & Dr Ngaundje Leno Dorisb, The Fight against Cybercrime in Cameroon, International Journal of Computer (IJC) (2019) Volume 35, No 1, pp 87-100.

[38] Ibid.

[39] Fobellah Clinton Atabongakenga, et al, Delineating International Cooperation in the Fight against Cybercrime in Cameroon International Journal of Computer (IJC) - Volume 51, No 1, (2024), pp.99-114.

[40] See generally Prof. André Borainea, & Dr Ngaundje Leno Dorisb, The Fight against Cybercrime in Cameroon, International Journal of Computer (IJC) (2019) Volume 35, No 1, pp 87-100.

[41] Ibid.

raising awareness about cybercrime.

iv. The National Police Force

The National Police Force has a specialized unit, the Cybercrime Unit, which focuses on investigating and prosecuting cybercrimes. The national police force in Cameroon plays a vital role in combating cybercrime. Key Responsibilities are:

- The police force investigates cybercrime cases, including hacking, phishing, and online fraud.[42]
- The police force works closely with other agencies, such as the National Agency for Information and Communication Technologies (ANTIC), to share intelligence and best practices in cyber security.[43]
- The police force provides training and capacity-building programs for law enforcement officers on cyber security and cybercrime.
- The police force raises awareness about cybercrime and its consequences among the general public, businesses, and government institutions.
- The police force enforces laws related to cybercrime, including the Cybersecurity and Cyber criminality Law of 2010.

To effectively combat cybercrime, the police force has also established specialized units, such as the Cybercrime Unit, which focuses on investigating and prosecuting cybercrime cases.[44]

b. Specialized Units

Some of the specialized units put in place to investigate cybercrimes include the following:

i. Cybercrime Unit

The Cybercrime Unit is a specialized unit within the National Police Force that focuses on investigating and prosecuting cybercrimes. The Cybercrime Unit in Cameroon plays a crucial role in combating cybercrime such as:

- The Cybercrime Unit investigates cybercrime cases, including hacking, phishing, online fraud, and child pornography.
- The Unit collects and analyzes digital evidence, such as computer logs, network traffic, and mobile phone data, to build cases against cybercriminals.

[42]The Fight against Cybercrime in Cameroon available at www.ijcjournal.org.

[43] Ibid.

[44] Colloquium on Cyber Criminality and Cyber Security available at www.univ-dschang.org.

- The Unit conducts forensic analysis of digital devices, such as computers, mobile phones, and servers, to retrieve data and identify cybercrime patterns.
- The Cybercrime Unit collaborates with international partners, such as Interpol and the African Union, to share intelligence and best practices in cyber security.
- The Unit provides training and capacity-building programs for law enforcement officers, judges, and prosecutors on cyber security and cybercrime.
- The Cybercrime Unit raises awareness about cybercrime and its consequences among the general public, businesses, and government institutions.
- The Unit develops strategies to prevent and combat cybercrime, including the development of national cyber security policies and laws.

By fulfilling these responsibilities, the Cybercrime Unit plays a vital role in protecting Cameroon's digital economy and ensuring the safety of its citizens online.

ii. The Digital Forensics Unit

The Digital Forensics Unit is a specialized unit within ANTIC that focuses on analyzing digital evidence and providing technical support for cybercrime investigations. The Digital Forensics Unit in Cameroon plays a crucial role in combating cybercrime. Key Responsibilities include:

- The Unit conducts digital forensic analysis of digital devices, such as computers, mobile phones, and servers, to retrieve data and identify cybercrime patterns.
- The Unit examines digital evidence, such as emails, chat logs, and social media posts, to build cases against cybercriminals.
- The Unit uses specialized tools to recover deleted data from digital devices, which can be used as evidence in cybercrime cases.
- The Unit analyzes network traffic to identify and track cybercriminals, and to disrupt their operations.
- The Unit provides expert testimony in court to explain digital forensic evidence and help prosecute cybercrime cases.
- The Unit collaborates with law enforcement agencies to share intelligence and best practices in digital forensics.
- The Unit develops and uses specialized digital forensics tools to analyze digital evidence and track cybercriminals.

- The Unit provides training and capacity-building programs for law enforcement officers, judges, and prosecutors on digital forensics and cybercrime.

By fulfilling these responsibilities, the Digital Forensics Unit plays a vital role in supporting the investigation and prosecution of cybercrime cases in Cameroon.

c. Inter-Agency Coordination

This inter-agency coordination is made up of the following:

i. The National Cyber Security Committee

The National Cybersecurity Committee is an inter-agency committee that brings together representatives from various government agencies, including ANTIC, MINPOSTEL, and the Ministry of Justice, to coordinate national cybersecurity efforts. The National Cyber Security Committee in Cameroon plays a crucial role in combating cybercrime including:

- The committee develops national strategies to fight cyber criminality, including creating a national strategy to protect information infrastructure.[45]
- The committee coordinates the efforts of various stakeholders, including government agencies, private sector organizations, and civil society groups, to prevent and respond to cyber threats.
- The committee raises awareness about cybercrime and its consequences among the general public, businesses, and government institutions.
- The committee provides training and capacity-building programs for law enforcement officers, judges, and prosecutors on cyber security and cybercrime.
- The committee collaborates with international partners, such as the Commonwealth Telecommunications Organisation (CTO), to share best practices and stay updated on the latest cyber security threats and trends.[46]

Overall, the National Cyber Security Committee plays a vital role in protecting Cameroon's digital economy and ensuring the safety of its citizens online.

ii. The Cybercrime Task Force

The Cybercrime Task Force is an inter-agency task force that brings together representatives from law enforcement agencies, ANTIC, and other stakeholders to coordinate efforts to combat cybercrime. The Cybercrime Task Force in Cameroon plays a crucial role in combating

[45] Cameroon to develop national strategy to fight cyber criminality available at www.businessincameroon.com.
[46]Ibid.

cybercrime. Key Responsibilities:

- The Task Force investigates cybercrime cases, including hacking, phishing, online fraud, and child pornography.
- The Task Force conducts forensic analysis of digital devices and online activities to gather evidence and track cybercriminals.
- The Task Force collaborates with law enforcement agencies to share intelligence and best practices in cybercrime investigation and prosecution.
- The Task Force provides training and capacity-building programs for law enforcement officers, judges, and prosecutors on cyber security and cybercrime.
- The Task Force raises awareness about cybercrime and its consequences among the general public, businesses, and government institutions.
- The Task Force develops strategies to prevent and combat cybercrime, including the development of national cyber security policies and laws.
- The Task Force coordinates international cooperation to combat cybercrime, including collaborating with international organizations and law enforcement agencies.

By fulfilling these responsibilities, the Cybercrime Task Force plays a vital role in protecting Cameroon's digital economy and ensuring the safety of its citizens online.

d. International Cooperation

International cooperation includes:

i. INTERPOL

Cameroon is a member of INTERPOL and collaborates with the organization on cybercrime investigations and operations. Interpol plays a significant role in combating cybercrime in Cameroon through international cooperation. One notable example is the Africa Cyber Surge II operation, a joint initiative between Interpol, African countries, and private sector cyber security companies to prevent, mitigate, and disrupt cyber threats on the African continent.[47]

Key Contributions of Interpol include:

- Interpol shares actionable intelligence with national law enforcement agencies, enabling them to investigate and disrupt cybercrime operations.

[47] "The Global Cybercrime Landscape" by Interpol (2020) - This report provides an overview of the global cybercrime landscape, including the role of international organizations.

- Interpol provides on-the-ground operational support to national law enforcement agencies, facilitating the arrest of cybercrime suspects and the takedown of malicious infrastructure.
- Interpol offers training and capacity-building programs for law enforcement officers, judges, and prosecutors on cyber security and cybercrime.

The Africa Cyber Surge II operation resulted in the arrest of 14 suspected cybercriminals, the identification of over 20,000 suspicious cyber networks, and the disruption of malicious activities linked to financial losses exceeding $40 million. Interpol's contributions to this operation demonstrate the organization's commitment to supporting international cooperation in the fight against cybercrime in Cameroon and across Africa.[48]

ii. The African Union

Cameroon is a member of the AU and participates in regional efforts to combat cybercrime through the AU's Convention on Cyber Security and Personal Data Protection.[49] The African Union (AU) plays a significant role in combating cybercrime in Cameroon through various initiatives and programs.[50] Key contributions AU include:

- The AU has established the African Cybersecurity Convention, which provides a framework for African countries to cooperate in preventing and combating cybercrime;
- The AU has assisted Cameroon in developing its national cyber security policy, which outlines the country's strategy for preventing and combating cybercrime.
- The AU has provided training and capacity-building programs for law enforcement officers, judges, and prosecutors in Cameroon on cybersecurity and cybercrime.
- The AU has facilitated regional cooperation among African countries, including Cameroon, to share best practices and coordinate efforts in combating cybercrime.
- The AU has collaborated with international organizations, such as Interpol and the United Nations, to support Cameroon's efforts in combating cybercrime.
- The AU has launched awareness-raising campaigns to educate the public in Cameroon about the risks and consequences of cybercrime.

[48] Ibid.

[49] "Cybersecurity in Africa: A Review of the Current State" by the African Union (2019) - This report provides an overview of cybersecurity in Africa, including the role of international organizations

[50] "The African Union's Cybersecurity Strategy" by the African Union (2019) - This report provides an overview of the African Union's cybersecurity strategy, including the role of international organizations.

- The AU has provided support to national cybersecurity agencies in Cameroon, including the National Agency for Information and Communication Technologies (ANTIC), to enhance their capacity to prevent and combat cybercrime.

By providing these contributions, the AU plays a vital role in supporting Cameroon's efforts to combat cybercrime and promote cybersecurity in the region.[51]

iii. The United Nations Office on Drugs and Crime (UNODC)

Cameroon collaborates with UNODC on cybercrime prevention and capacity-building efforts. The United Nations Office on Drugs and Crime (UNODC) plays a significant role in combating cybercrime in Cameroon through various initiatives and programs.

Key contributions of UNODC include:

- UNODC provides technical assistance to Cameroon to strengthen its capacity to prevent and combat cybercrime.
- UNODC assists Cameroon in developing and implementing effective laws and policies to combat cybercrime.
- UNODC provides training and capacity-building programs for law enforcement officers, judges, and prosecutors in Cameroon on cybersecurity and cybercrime.
- UNODC facilitates international cooperation and information sharing between Cameroon and other countries to combat cybercrime.
- UNODC launches awareness-raising campaigns to educate the public in Cameroon about the risks and consequences of cybercrime.
- UNODC provides support to national cybersecurity agencies in Cameroon, including the National Agency for Information and Communication Technologies (ANTIC), to enhance their capacity to prevent and combat cybercrime.
- UNODC assists Cameroon in developing national cybersecurity strategies and action plans to prevent and combat cybercrime.

UNODC's efforts in Cameroon are guided by the organization's Comprehensive Study on Cybercrime, which provides a framework for understanding and addressing cybercrime.[52] By providing these contributions, UNODC plays a vital role in supporting Cameroon's efforts to

[51] "Cybersecurity in Africa: A Review of the Current State" by the African Union (2019) - This report provides an overview of cybersecurity in Africa, including the role of international organizations.

[52] "Cybercrime and Cybersecurity in Africa" by J. M. Eyo (Editor) (2020) - This book provides an overview of cybercrime and cybersecurity in Africa, including the role of international organizations.

combat cybercrime and promote cybersecurity.

III. An overview of the categories of risks associated with cybercrimes in Cameroon

The widespread nature of cybercrimes across Africa in general and Cameroon in particular is associated with different groups of risks as seen below:

(A) Financial Risks

Cybercrimes is associated with the following types of financial risks:

a. Identity Theft

Identity theft is a type of cybercrime where an individual's personal and sensitive information is stolen and used without their consent, often for financial gain. That is, cybercriminals can steal personal and financial information, leading to identity theft and financial loss.[53] Identity theft can occur through various means such as phishing[54], malware[55], social engineering[56], physical theft[57] etc.

The consequences of identity theft in Cameroon can be severe and long-lasting. For instance, victims of cybercrimes may suffer financial loss due to unauthorized transactions or loans taken out in their name; identity theft can damage a victim's reputation and credit score; victims may experience emotional distress, including anxiety and depression; and finally victims may face legal consequences, including arrest and prosecution, if their stolen identity is used to commit crimes.

To prevent and protect against identity theft in Cameroon, individuals can take the following measures such as using strong and unique passwords for all online accounts; being cautious when sharing personal information online or in person; regularly monitor bank and credit card statements, as well as credit reports, for suspicious activity; install and regularly update antivirus software to protect against malware and avoid responding to suspicious emails or messages that ask for personal information.

[53] This can include information such as full name, date of birth, national identity card number, passport number, bank account numbers, credit card numbers, email addresses passwords.

[54] Scammers send fake emails or messages that appear to be from legitimate sources, such as banks or government agencies, and trick victims into revealing their personal information.

[55] Malicious software is installed on a victim's device, allowing scammers to steal personal information.

[56] Scammers use psychological manipulation to trick victims into revealing their personal information.

[57] Thieves can steal physical documents, such as identity cards or passports, and use the information to commit identity theft.

b. Online Banking Fraud

Online banking fraud refers to the use of the internet to commit fraudulent activities against banks, financial institutions, and their customers. That is, cybercriminals can hack into online banking systems, leading to unauthorized transactions and financial loss. This banking fraud can take many forms such as:

- Scammers sending fake emails or messages that appear to be from a bank or financial institution, asking customers to provide sensitive information such as login credentials, credit card numbers, or account numbers.
- Malicious software is installed on a customer's device, allowing scammers to steal login credentials, account information, or other sensitive data.
- Scammers intercepting communication between a customer's device and the bank's website, allowing them to steal sensitive information or manipulate transactions.
- Scammers install malware on a customer's device, which appears to be a legitimate banking app but actually allows scammers to steal sensitive information.
- Scammers take control of a customer's online banking session, allowing them to perform unauthorized transactions or steal sensitive information.
- Scammers gain unauthorized access to a customer's online banking account, allowing them to perform transactions, steal funds, or steal sensitive information.

Online banking fraud has the following consequences such as customers may suffer financial loss due to unauthorized transactions or theft of funds; online banking fraud can damage a bank's reputation and erode customer trust; banks may face regulatory penalties for failing to implement adequate security measures to prevent online banking fraud; banks may incur increased security costs to prevent and respond to online banking fraud etc.

To tackle the issue of online banking fraud, Banks can adopt the following prevention and protection measures such as: Banks should implement strong authentication measures, such as two-factor authentication, to prevent unauthorized access to online banking accounts; Banks should use encryption to protect sensitive customer information, such as login credentials and account numbers; Banks should monitor transactions for suspicious activity and implement real-time fraud detection systems and Banks should educate customers on how to protect themselves from online banking fraud, such as avoiding phishing scams and using strong passwords.

c. Credit Card Fraud

Credit card fraud, also known as credit fraud, refers to the unauthorized use of a credit card or credit card information to obtain goods, services, or cash. Cybercriminals can steal credit card information, leading to unauthorized transactions and financial loss. This type of fraud can occur in various ways, including stolen credit cards, card skimming,[58] phishing, malware card not present (CNP) fraud, counterfeit cards[59] etc. Credit card fraud can make victims suffer financial loss due to unauthorized transactions; damage a victim's credit score; cause victims to experience emotional distress, including anxiety and stress and cause credit card companies to implement additional security measures, such as chip technology or biometric authentication

To solve the problem of Credit card fraud the following steps should be adopted: regularly review credit card statements for suspicious transactions; only use secure websites (https) when making online transactions; be cautious when receiving emails or calls asking for credit card information; use credit cards with chip technology, which provides an additional layer of security and immediately report suspicious activity to the credit card company:

(B) Data-Related Risks

Cybercrimes is associated with the following types of data-related risks:

a. Data Breach

A data breach is an unauthorized access, disclosure, or theft of sensitive, confidential, or protected data. Cybercriminals can hack into databases, leading to unauthorized access to sensitive information. This can include personal, financial, or proprietary information. Forms of data breaches are unauthorized access, data theft, data loss, data exposure etc. Causes of data breaches are malicious actors use hacking techniques to gain unauthorized access to data, authorized individuals intentionally or unintentionally compromise data security and devices or storage media containing sensitive data are stolen. Consequences of data breaches are data breaches can result in significant financial losses due to theft, fines, or reputational damage; data breaches can damage an organization's reputation and erode customer trust; organizations may face regulatory penalties for failing to protect sensitive data and organizations may be liable for damages resulting from data breaches.

Data breaches can be prevented and protected by implementing strong access control to limit access to sensitive data to authorized individuals; using encryption to encrypt sensitive data to protect it from unauthorized access; regularly updating software and systems to prevent exploitation of vulnerabilities; regularly auditing security measures to identify vulnerabilities

[58] Thieves attach a device to an ATM or credit card terminal to capture credit card information.

[59] Thieves create fake credit cards using stolen credit card information

and weaknesses; educate employees and customers on data security best practices and the importance of protecting sensitive data.

b. Data Loss

Data loss refers to the permanent or temporary loss of access to digital data, resulting in the inability to retrieve, use, or manage the data. That is, cybercriminals can delete or destroy data, leading to permanent loss of sensitive information. Data loss can occur due to various reasons, including technical failures, human error, or intentional deletion. Causes of data loss can be as a result of hard drives, solid-state drives, or other storage devices fail, resulting in data loss; software errors or corruption result in data loss or inaccessibility; accidental deletion, overwriting, or mismanagement of data results in data loss; malicious software attacks result in data loss or corruption; floods, fires, or other natural disasters result in physical damage to storage devices and data loss.

Consequences of data loss are data loss can result in significant financial losses, particularly if the lost data is critical to business operations; data loss can result in productivity losses, as employees may need to recreate lost data or spend time recovering from data loss; data loss can damage an organization's reputation, particularly if sensitive customer data is lost; organizations may face regulatory penalties for failing to protect sensitive data.

Data loss can be prevention and protection by regularly backing up critical data to prevent data loss; implementing data redundancy measures, such as RAID or mirroring, to ensure data availability; encrypting sensitive data to protect it from unauthorized access; implement access controls, such as authentication and authorization, to prevent unauthorized access to data; develop a disaster recovery plan to ensure business continuity in the event of data loss.

c. Data Manipulation

Data manipulation refers to the unauthorized or malicious alteration, modification, or falsification of digital data, resulting in inaccurate, misleading, or false information. That is, cybercriminals can manipulate data, leading to inaccurate or misleading information. Data manipulation can occur intentionally or unintentionally, and can have serious consequences. Types of data manipulation are intentional alteration or modification of data to achieve a specific goal or outcome; creation of false data or alteration of existing data to make it appear legitimate; unauthorized modification of data, such as changing dates, times, or values; unauthorized deletion of data, resulting in loss of information.

Causes of data manipulation are authorized individuals intentionally or unintentionally manipulate data for personal gain or malicious purposes; hackers or external actors manipulate data for malicious purposes, such as financial gain or disruption of operations; accidental data manipulation can occur due to human error, such as incorrect data entry or accidental deletion and exploitation of system vulnerabilities can allow unauthorized access and manipulation of data.

Data manipulation can occur intentionally or unintentionally, and can have serious consequences such as data manipulation can result in financial losses, particularly if false or altered data is used for financial transactions; data manipulation can damage an organization's reputation, particularly if false or altered data is used to make decisions or take actions; organizations may face regulatory penalties for failing to protect data from manipulation; data manipulation can lead to a loss of trust among stakeholders, including customers, employees, and partners.

Data manipulation can prevented and protected by implementing access controls, such as authentication and authorization, to prevent unauthorized access to data; by encrypting sensitive data to protect it from unauthorized access and manipulation; regularly backing up data and have a disaster recovery plan in place to ensure business continuity in the event of data manipulation; by regularly monitor and audit data for signs of manipulation or unauthorized access by educating and training employees on the importance of data integrity and the consequences of data manipulation.

(C) Reputation-Related Risks

Cybercrimes is associated with the following types of reputation-related risks:

a. Defamation

Defamation is the act of making false and damaging statements about someone, which can harm their reputation, character, or livelihood. That is, cybercriminals can spread false or damaging information about individuals or organizations, leading to reputational damage. Defamation can occur through various means, such as written or published statements that are false and damaging (libel) through spoken statements that are false and damaging (slander) in the eyes of the right thinking member of the society. Defamation can either be direct which entails making a direct, false and damaging statement about someone and indirect which equally entails making a statement that implies something false and damaging about someone or group defamation meaning making a statement that defames a group of people. Causes of Defamation are making false and damaging statements intentionally to harm someone's reputation; making false and damaging statements due to negligence or carelessness; defamatory statements can spread quickly through social media platforms.

Consequences of defamation are defamation can damage someone's reputation, making it difficult to regain trust and credibility; defamation can cause emotional distress, including anxiety, depression, and stress; defamation can result in financial losses, including lost business opportunities and damages awarded in court; defamation can lead to social consequences, including social isolation and loss of relationships. Defamation can be prevented and protected by verifying the accuracy of information before sharing or publishing it; by being cautious when sharing information on social media platforms; by respecting others' rights to their reputation and character; by seeking professional advice from lawyers or media experts if unsure about the accuracy of information and apologizing and correct false statements promptly to minimize damage.

b. Social Media Attacks

Social media attacks refer to the use of social media platforms to launch malicious attacks on individuals, organizations, or brands. That is, cybercriminals can launch attacks on social media platforms, leading to reputational damage and loss of business. These attacks can take many forms, including harassment, intimidation, or threats made through social media; false and damaging statements made about someone or something on social media; by making speech that promotes hatred or violence against individuals or groups on social media; scams that trick users into revealing sensitive information, such as passwords or credit card numbers; by manipulation users into performing certain actions or revealing sensitive information.

Social media attacks can be personal attacks (attacks targeted at individuals, including celebrities, politicians, or ordinary citizens), brand attacks (attacks targeted at organizations or brands, including hacking, defamation, or phishing), reputation attacks, (attacks aimed at damaging someone's reputation or credibility). Causes of social media attacks are social media platforms can provide a sense of anonymity, making it easier for attackers to hide their identities; social media platforms can be difficult to regulate, making it challenging to prevent or respond to attacks; social media platforms are easy to use, making it simple for attackers to launch attacks.

Consequences of social media attacks are social media attacks can damage someone's reputation or credibility; social media attacks can cause emotional distress, including anxiety, depression, and stress; social media attacks can result in financial losses, including lost business opportunities or damages awarded in court and social media attacks can lead to social consequences, including social isolation and loss of relationships.

Social media attacks can be prevented and protected by using strong and unique passwords for social media accounts; by being cautious when clicking on links or downloading attachments from unknown sources by regularly monitor social media accounts for suspicious activity; by reporting social media attacks to the platform or law enforcement and by educating yourself on social media safety and security best practices.

c. **Online Harassment**

Online harassment refers to the use of digital technologies, such as social media, email, text messages, or online forums, to harass, intimidate, or threaten individuals or groups. That is, cybercriminals can harass individuals or organizations online, leading to reputational damage and emotional distress.[60] Online harassment can take many forms, including repeated and intentional harassment or intimidation of an individual or group; repeated and intentional harassment or intimidation of an individual or group, often with the intent to cause fear or harm; posting inflammatory or provocative comments online to provoke a reaction, posting hostile or aggressive comments online and publishing personal information about someone online without their consent.

Online harassment can be personal attacks, group harassment or sexual harassment. Causes of online harassment are online environments can provide a sense of anonymity, making it easier for harassers to hide their identities; online environments can be difficult to regulate, making it challenging to prevent or respond to harassment and finally online environments are easy to use, making it simple for harassers to launch attacks. Consequences of online harassment are online harassment can cause emotional distress, including anxiety, depression, and stress; online harassment can damage someone's reputation or credibility; online harassment can lead to social consequences, including social isolation and loss of relationships; and in extreme cases, online harassment can lead to physical harm or even death.

To prevent and protect people against online harassment the following measures should be put in place such as using strong and unique passwords for online accounts; by being cautious when sharing personal information online; by regularly monitoring online activity for signs of harassment; by reporting online harassment to the platform, law enforcement, or a trusted authority figure and by educating yourself on online safety and security best practices.

(D) Operational Risks

Cybercrimes is associated with the following types of operational risk:

[60] Duggan, "Online Harassment (2017)," Internet: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/, Jul. 11, 2017 (February 6, 2024).

a. System Downtime

System downtime refers to the period of time when a computer system, network, or application is unavailable or inaccessible, resulting in disruptions to business operations, services, or activities. That is, cybercriminals can launch attacks that cause system downtime, leading to operational disruptions and financial loss.

System downtime can be caused by various factors, including failure of hardware components, such as servers, routers, or storage devices; failure of software applications, operating systems, or firmware; failure of network connections, including internet connectivity, local area networks (LANs), or wide area networks (WANs); power outages or electrical failures that affect system availability; accidental or intentional actions by users, administrators, or maintenance personnel that cause system downtime; malicious attacks, such as hacking, denial-of-service (DOS), or ransomware attacks, that compromise system availability; and scheduled or unscheduled maintenance, upgrades, or repairs that require system downtime.

Consequences of system downtime are system downtime can result in significant financial losses, including lost revenue, productivity, and opportunity costs; system downtime can damage an organization's reputation, eroding customer trust and confidence; system downtime can disrupt business operations, supply chains, and critical services, leading to delays, cancellations, or other consequences; system downtime can result in data loss or corruption, compromising business continuity and decision-making; and system downtime can expose organizations to compliance risks, particularly in regulated industries, such as healthcare, finance, or government.

System downtime can be prevented and protected by implementing redundant systems, networks, and infrastructure to ensure availability and minimize downtime; by regularly back up critical data and systems, and have a disaster recovery plan in place to quickly restore operations; by proactively monitor systems and perform regular maintenance to prevent failures and minimize downtime; by implementing robust cybersecurity measures, including firewalls, intrusion detection, and antivirus software, to prevent cyber-attacks; by educating users, administrators, and maintenance personnel on best practices for system management, troubleshooting, and maintenance.

b. Network Disruption

Cybercriminals can disrupt networks, leading to operational disruptions and financial loss. Network disruption refers to the interruption or degradation of network services, resulting in the inability to access or transmit data, communicate, or perform critical operations. Network disruptions can occur due to various reasons such as failure of network hardware, such as routers, switches, or servers; software bugs, glitches, or configuration errors that affect network performance; malicious attacks, such as hacking, denial-of-service (DoS), or distributed denial-of-service (DDoS) attacks; overload of network resources, resulting in slow data transfer rates or complete network unavailability; physical damage to network infrastructure, such as cables, fiber optic connections, or network equipment; power outages or electrical failures that affect network availability and scheduled or unscheduled maintenance, upgrades, or repairs that require network downtime.

Different types of network disruptions include total loss of network connectivity and services; loss of connectivity to specific network segments, services, or applications; degradation of network performance, resulting in slow data transfer rates; and unstable network connections, resulting in frequent disconnections or dropped packets. Network disruptions are associated with the following consequences: Network disruptions can result in significant financial losses, including lost revenue, productivity, and opportunity costs; network disruptions can damage an organization's reputation, eroding customer trust and confidence; network disruptions can disrupt business operations, supply chains, and critical services, leading to delays, cancellations, or other consequences; network disruptions can result in data loss or corruption, compromising business continuity and decision-making.

To solve the problem of network disruptions the following preventive and protective measures are adopted such as implementing redundant network infrastructure, including duplicate hardware, software, and connections; proactively monitoring network performance, detecting potential issues before they become disruptions; implementing robust cybersecurity measures, including firewalls, intrusion detection, and antivirus software, to prevent cyber-attacks; regularly performing maintenance, upgrades, and repairs to prevent network disruptions; developing a disaster recovery plan to quickly restore network services in the event of a disruption.

c. Supply Chain Disruption

Supply chain disruption refers to the interruption or disturbance of the flow of goods, services, or information within a supply chain, resulting in delays, cancellations, or other consequences. That is, cybercriminals can disrupt supply chains, leading to operational disruptions and financial loss. Supply chain disruptions can occur due to various reasons such as earthquakes, hurricanes, floods, or other natural disasters that damage or destroy supply chain infrastructure; malicious attacks on supply chain systems, including hacking, ransomware, or denial-of-service

(DoS) attacks; transportation disruptions, such as trucking or shipping delays, or warehouse management issues; bankruptcy or financial instability of suppliers, resulting in disruptions to material or component deliveries; production delays or quality control problems that impact the availability of finished goods; changes in laws, regulations, or trade agreements that impact supply chain operations; wars, terrorism, or other geopolitical events that disrupt supply chain operations.

Supply chain can be disrupted in multiple ways such as: disruptions to the supply of raw materials, components, or finished goods; changes in demand patterns, resulting in inventory shortages or overstocking; disruptions to transportation, warehousing, or other logistical operations; disruptions to the flow of information within the supply chain, resulting in delays or errors.

Consequences of supply chain disruptions are that supply chain disruptions can result in significant financial losses, including lost revenue, inventory costs, and expedited shipping fees; supply chain disruptions can damage an organization's reputation, eroding customer trust and confidence; supply chain disruptions can disrupt business operations, resulting in delays, cancellations, or other consequences; supply chain disruptions can result in inventory shortages or overstocking, leading to additional costs and operational challenges.

To solve the problem of supply chain disruptions the following preventive and protective measures should be adopted such as implementing visibility tools to monitor supply chain operations in real-time; conducting regular risk assessments to identify potential supply chain disruptions, developing contingency plans to mitigate the impact of supply chain disruptions; diversifying suppliers to reduce dependence on individual suppliers and finally implementing effective inventory management practices to minimize the impact of supply chain disruptions.

(E) National Security Risks

Cybercrimes is associated with the following types of National Security Risks:

a. Cyber Espionage

Cyber espionage refers to the use of digital technologies, such as computers, networks, and the internet, to gather sensitive or classified information from individuals, organizations, or governments without their consent. Cyber espionage is a form of cyber-attack that is typically carried out by nation-states, intelligence agencies, or other organized groups. That is, cybercriminals can engage in cyber espionage, leading to the theft of sensitive national security information.

The different types of cyber espionage include network exploitation; malware; phishing, insider threats etc. Motivations for cyber espionage are nation-states may engage in cyber espionage to gather intelligence on other countries' military capabilities, strategic plans, or diplomatic efforts; cyber espionage may be used to steal intellectual property, trade secrets, or other sensitive information that can provide a competitive advantage; and cyber espionage may be used to gather information that can be used to influence political decisions or disrupt democratic processes.

Consequences of cyber espionage are cyber espionage can compromise national security by revealing sensitive information about military capabilities, strategic plans, or diplomatic efforts; cyber espionage can result in significant economic losses due to the theft of intellectual property, trade secrets, or other sensitive information; cyber espionage can damage the reputation of individuals, organizations, or governments by revealing sensitive information or compromising their security and cyber espionage can erode trust between nations, organizations, or individuals, making it more difficult to collaborate or share information.

To salvage the problem of cyber espionage, the following preventive and protective measures should be adopted which include using firewalls, intrusion detection systems, and encryption to protect sensitive information; regularly assess security vulnerabilities and implement measures to address them; training employees on cybersecurity best practices and the importance of protecting sensitive information; using secure communication channels, such as encrypted email or messaging apps, to protect sensitive information; collaborating with law enforcement agencies to share information and coordinate efforts to prevent and respond to cyber espionage.

b. Critical Infrastructure Attacks

Cybercriminals can launch attacks on critical infrastructure, leading to national security risks and disruptions to essential services. Critical infrastructure attacks refer to the intentional disruption, destruction, or exploitation of critical infrastructure systems, such as energy systems; transportation systems; water systems; communication systems and financial systems.

The consequences of critical infrastructure attacks are that critical infrastructure attacks can result in loss of life, particularly if they affect critical services like healthcare or emergency response; attacks can disrupt economic activity, causing financial losses and instability; attacks can result in environmental damage, particularly if they affect critical infrastructure like water or energy systems; attacks can cause social unrest, particularly if they disrupt critical services like communication or transportation.

To prevent and protect critical infrastructure attacks the following measures can be adopted such as using robust security measures, which include firewalls, intrusion detection systems, and encryption, to protect critical infrastructure systems; by regularly assessing security vulnerabilities and implementing measures to address them; by developing incident response plans to quickly respond to and mitigate the effects of critical infrastructure attacks; by Collaborating with law enforcement agencies to share information and coordinate efforts to prevent and respond to critical infrastructure attacks and investing in research and development to improve the security and resilience of critical infrastructure systems.

c. **Terrorism**

Terrorism is the use of violence, intimidation, or threats to achieve political, ideological, or religious goals. Cybercriminals can use the internet to facilitate terrorist activities, leading to national security risks and threats to public safety. Terrorism can take many forms, including: bombings, shootings, kidnappings, and other forms of physical violence; using digital technologies to disrupt, damage, or destroy critical infrastructure, steal sensitive information, or spread fear and propaganda; using fear, intimidation, and propaganda to manipulate public opinion and achieve goals. Various forms of terrorism exists such as terrorism carried out by individuals or groups within a country against their own government or citizens (domestic terrorism); terrorism carried out by individuals or groups across national borders (international terrorism) and terrorism supported or sponsored by governments or government agencies (state-sponsored terrorism).

The different motivating factors for terrorism are terrorism motivated by political ideologies, such as extremism, nationalism, or separatism; terrorism motivated by religious ideologies, such as extremism or fundamentalism; terrorism motivated by economic grievances, such as poverty, inequality, or exploitation and terrorism motivated by social grievances, such as discrimination, oppression, or marginalization. The consequences of terrorism of include terrorism can result in loss of life, injury, and trauma; terrorism can disrupt economic activity, causing financial losses and instability; terrorism can cause social unrest, fear, and mistrust; and terrorism can undermine political stability, erode trust in government, and create power vacuums.

To prevent and protect against any act of terrorism the following preventive and protective measures should be adopted which include: gathering and analyzing intelligence to identify and disrupt terrorist plots; making use of law enforcement agencies to investigate and prosecute terrorist activities; implementing counter-radicalization programs to prevent the spread of extremist ideologies; collaborating with international partners to share intelligence, coordinate efforts, and address global terrorist threats; and by engaging with local communities to build trust, promote social cohesion, and prevent radicalization.

(F) Social Risks

Cybercrimes is associated with the following types of Social Risks:

a. Social Unrest

Social unrest refers to a state of disturbance, disorder, or instability within a society, often characterized by protests, demonstrations, riots, or other forms of collective action. Cybercriminals can spread false or misleading information, leading to social unrest and public disorder. Social unrest can be caused by various factors, including disparities in wealth, income, or access to resources; perceived unfairness or discrimination based on factors like race, gender, religion, or sexual orientation; restrictions on civil liberties, freedom of speech, or assembly; issues related to pollution, climate change, or natural resource depletion; and conflicts between different cultural or ethnic groups.

Several types of social unrest can occur such as non-violent demonstrations, marches, or rallies; violent disturbances, often involving property damage or clashes with authorities; widespread disorder, often involving multiple groups or communities; organized efforts to bring about social change, often involving protests, boycotts, or other forms of collective action.

Consequences of social unrest can be risk of injury or death to individuals involved in or affected by social unrest; destruction or damage to property, including businesses, homes, or public infrastructure; disruption to economic activity, including losses to businesses, industries, or entire economies; exacerbation of social divisions, leading to increased tensions and conflict between different groups; potential for government instability or collapse, particularly if social unrest is widespread or prolonged.

Social unrest can be prevented by addressing the underlying causes of social unrest, such as economic inequality or social injustice; by encouraging open and respectful dialogue between different groups and stakeholders; by strengthening institutions, such as the judiciary, media, and civil society organizations; by encouraging civic engagement and participation in the democratic process; by developing emergency response plans to manage and respond to social unrest.

b. Cyber Bullying

Cyber bullying refers to the use of digital technologies, such as social media, text messages, emails, or online forums, to harass, intimidate, or threaten individuals, often repeatedly and with the intention of causing harm or distress.[61] Cybercriminals can engage in cyber bullying, leading to emotional distress and psychological harm.[62] Cyber bullying can be repeated and unwanted contact, including messages, emails, or comments that cause fear or anxiety; posting inflammatory or provocative comments online to provoke a reaction; posting false or damaging information about someone online; creating a fake online identity to harass or intimidate someone and excluding someone from online groups or communities.[63]

The different causes of cyber bullying include the anonymity of the internet can embolden individuals to engage in cyber bullying; cyber bullies may lack empathy for their victims or may not fully understand the impact of their actions; cyber bullies may use their online presence to exert power over others; and cyber bullies may be influenced by peer pressure or social norms that encourage aggressive behavior.

Consequences of cyber bullying are that cyber bullying can cause significant emotional distress, including anxiety, depression, and suicidal thoughts;[64] cyber bullying can lead to social isolation, as victims may avoid online interactions or social situations; cyber bullying can damage a person's reputation, particularly if false or damaging information is posted online; in extreme cases, cyber bullying can lead to physical harm, as victims may be threatened or intimidated.

To prevent cyber bullying, individuals should be educated about the consequences of cyber bullying and the importance of online etiquette;[65] encourage parents to monitor their children's online activities and engage in open conversations about cyber bullying; establish reporting mechanisms for cyber bullying incidents, such as online reporting tools or school counseling services; impose consequences for cyber bullies, such as suspension from school or online communities; and provide support for victims of cyber bullying, including counseling services and peer support groups.[66]

[61] E. Menesini and A. Nocentini, (2009), “Cyberbullying definition and measurement: Some critical considerations”, Journal of Psychology, vol. 217, pp.230-232.

[62] Jerry Hea, & Lisa Chalaguine, (2023), Natural Language Processing for Cyber bullying Detection, International Journal of Computer (IJC) - Volume 49, No 1, pp.84-97.

[63] Ngange, K. L., Nkengafack, E., & Mesumbe, N. N. (2024), Analysing Differences in Social Media Use and Cyberbullying among Male and Female Students of University of Buea in Cameroon. Advances in Journalism and Communication, 12, 306-334. https://doi.org/10.4236/ajc.2024.122016.

[64] M. Mickey. “A 15-year-old boy died by suicide after relentless cyber bullying, and his parents say the Latin School could have done more to stop it.” Internet: https://www.cbsnews.com/chicago/news/15- year-old-boy-cyberbullying-suicide-latin-school-chicago-lawsuit/, Apr. 25, 2022 [Jan. 19, 2025].

[65] M.A. Al-Ajlan and Y. Mourad, (2018),“Deep learning algorithm for cyberbullying detection.” International Journal of Advanced Computer Science and Applications, vol. 9, pp. 199-205.

[66] V. Balakrishnan, S. Khan, and H.R. Arabnia,“Improving cyberbullying detection using Twitter users’ psychological features and machine learning.” Computers & Security, vol. 90, pp. 101710, Mar. 2020.

c. Human Trafficking

Human trafficking is the recruitment, transportation, transfer, harboring, or receipt of people through force, coercion, or deception, with the aim of exploiting them for labor, sex, or organs. Human trafficking is a form of modern-day slavery and is considered a serious human rights violation. Cybercriminals can use the internet to facilitate human trafficking, leading to social risks and human rights abuses.

Examples of human trafficking include the recruitment, transportation, or harboring of people for the purpose of forced commercial sex; the recruitment, transportation, or harboring of people for the purpose of forced labor or services; the recruitment, transportation, or harboring of people for the purpose of forced organ removal; and the recruitment, transportation, or harboring of children for the purpose of exploitation.

The causes of human trafficking are poverty and lack of economic opportunities can make individuals vulnerable to trafficking; limited access to education and awareness about trafficking can make individuals more susceptible to exploitation; situations of conflict, crisis, or natural disasters can create opportunities for traffickers to exploit vulnerable individuals; and corruption and complicity among government officials, law enforcement, or other authorities can facilitate trafficking.

Consequences of human trafficking are that: human trafficking can result in physical and emotional harm, including torture, rape, and psychological trauma; trafficking can result in exploitation, including forced labor, sex, or organ removal; trafficking can result in the loss of identity, including the loss of passports, identification documents, or other personal belongings; and finally trafficking can result in social isolation, including separation from family, friends, and community.

To solve the problem of human trafficking, awareness should be raise about human trafficking and its consequences; strengthen laws and policies to prevent trafficking and protect victims; support services for victims of trafficking, including counseling, healthcare, and legal assistance; collaborate with law enforcement agencies to investigate and prosecute trafficking cases; and finally addressing the root causes of trafficking, including poverty, lack of education, and conflict.

(G)Economic Risks

Cybercrimes is associated with the following types of economic risks:

a. **Economic Loss**

Economic loss refers to a decline in economic value or a reduction in financial resources, resulting from various factors such as business disruption, market fluctuations, regulatory changes, natural disasters, Cyber-attacks etc. Cybercriminals can cause significant economic loss through various types of cybercrime, including identity theft, online banking fraud, and credit card fraud.

Economic loss can be direct financial losses, such as damage to property, equipment, or inventory; indirect financial losses, such as loss of business, revenue, or productivity; and the cost of missed opportunities, such as lost sales, revenue, or market share. Causes of economic loss include external factors, such as natural disasters, market fluctuations, or regulatory changes; internal factors, such as poor management, inadequate risk management, or inefficient operations; and human error, such as mistakes, negligence, or intentional acts.

Consequences of economic loss are that: economic loss can lead to financial instability, including bankruptcy, insolvency, or liquidity crises; economic loss can disrupt business operations, supply chains, or services; economic loss can damage a company's reputation, eroding customer trust and confidence; economic loss can result in job losses, impacting employees, their families, and the broader economy.

To salvage the problem of economic loss, cyber victims should implement robust risk management practices to identify, assess, and mitigate potential risks; develop business continuity plans to ensure continuity of operations during disruptions; consider insurance options to transfer risk and protect against economic loss; diversify business operations, revenue streams, and investments to reduce dependence on a single market or sector; and regularly monitor and review business operations, financial performance, and risk exposure to identify areas for improvement.

b. **Job Loss**

Job loss refers to the involuntary termination of employment, which can be a highly stressful and emotional experience. It's not just about losing a paycheck, but also about losing a sense of identity, purpose, and social connections.[67] Cybercriminals can cause job loss through various types of cybercrime, including system downtime, network disruption, and supply chain disruption. When someone loses their job, they may experience a range of emotions, including

[67] Melinda Smith, M.A., (2025), Job Loss and Unemployment Stress, HelpGuide.org, pp.1-8. Available at https: www.helpguide.org/mental-health/stress/job-loss-and-unemployment-stress. Last viewed on March 1st, 2025, at 8:22pm

shock, denial, anger, and sadness. It's essential to acknowledge these feelings and allow yourself to grieve the loss of your job. This process can help you come to terms with the situation and move forward.[68]

Job loss can be caused by various factors, such as company restructuring, economic downturns, or individual performance issues. In some cases, it may be due to circumstances beyond one's control, like a pandemic or natural disaster.[69] The consequences of job loss can be far-reaching, affecting not only the individual but also their family and overall well-being. It's crucial to seek support from loved ones, professionals, or support groups to cope with the emotional and financial challenges that come with job loss.[70]

c. Investment Loss

Cybercriminals can cause investment loss through various types of cybercrime, including phishing, ransomware, and business email compromise. Investment loss refers to a decline in the value of an investment, resulting in a financial loss for the investor. Investment losses can occur due to various factors, such as fluctuations in market conditions, such as changes in interest rates, commodity prices, or currency exchange rates; poor performance of the company or organization in which the investment was made; economic downturns, such as recessions or depressions, that affect the overall market or industry; changes in laws, regulations, or policies that affect the investment or industry; and fraudulent activities or mismanagement of funds by investment managers or companies.

Types of investment loss include capital loss, opportunity loss, and paper loss. Causes of investment loss are failure to diversify investments, making them vulnerable to market fluctuations; making investment decisions based on emotions, inadequate research, or unrealistic expectations; exposure to market risks, such as interest rate risk, credit risk, or liquidity risk; and failure to implement risk management strategies, such as hedging or stop-loss orders.

Consequences of investment loss are that investment losses can result in significant financial losses, impacting an individual's or organizations financial well-being; investment losses can erode confidence in the investment or the market, leading to risk aversion or emotional decision-making; investment losses can result in opportunity costs, as the lost capital could have been invested elsewhere.

[68] Ibid.
[69] Ibid.
[70] Ibid.

To solve the problem of investment loss victims of cybercrimes should diversify investments to minimize risk and maximize returns; implement risk management strategies, such as hedging or stop-loss orders, to limit potential losses; conduct thorough research and due diligence before making investment decisions; regularly rebalance investment portfolios to ensure alignment with investment objectives and risk tolerance; and seek advice from financial professionals or investment advisors to make informed investment decisions.

IV. JUDICIAL INTERVENTION FOR THE ENFORCEMENT OF MEASURES TO COMBAT CYBERCRIMES IN CAMEROON

Judicial intervention plays a crucial role in enforcing measures to combat cybercrimes in Cameroon. The country has established a legal framework to combat cybercrimes, including the Cybercrime Law of 2010. This law provides for the prevention, investigation, and prosecution of cybercrimes, including hacking, identity theft, and online harassment.

(A) Judicial Measures

- Prosecution: The law provides for the prosecution of cybercrime offenders, with penalties ranging from fines to imprisonment.
- Confiscation of Equipment: The court can order the confiscation of equipment and devices used in the commission of cybercrimes.
- Restitution: Cameroon has established specialized courts to handle cybercrime cases, including the Court of First Instance and the Court of Appeal. The state has provided training for judges and prosecutors on cybercrime laws and procedures to ensure effective prosecution and adjudication of cybercrime cases. The court can order the perpetrator to pay restitution to the victim for damages suffered as a result of the cybercrime.

(B) Administrative sanctions on cybercrimes

In Cameroon, administrative sanctions on cybercrimes are imposed by the Ministry of Posts and Telecommunications (MINPOSTEL) and other relevant authorities. Below are some administrative sanctions that can be imposed on cyber criminals in Cameroon such as:

- MINPOSTEL can impose fines on individuals and organizations that commit cybercrimes, ranging from XAF 1 million to XAF 10 million (approximately USD 1,700 to USD 17,000);

- The Cybercrime Law of 2010 provides for penalties, including fines and imprisonment, for cybercrime offenses;
- MINPOSTEL can suspend or revoke the licenses of telecommunications operators and internet service providers that fail to comply with cybersecurity regulations;
- The government can block websites that host or promote cybercrime activities;
- Law enforcement agencies can seize equipment and devices used in the commission of cybercrimes;
- MINPOSTEL can issue warnings to individuals and organizations that commit minor cybercrime offenses;
- The government can require individuals and organizations to undergo training and education on cybersecurity best practices; and
- Law enforcement agencies can monitor the activities of individuals and organizations that have committed cybercrimes.

(C) Criminal sanctions on cybercrimes

In Cameroon, criminal sanctions on cybercrimes are imposed by the courts, in accordance with the Cybercrime Law of 2010 and the Penal Code. Some criminal sanctions that can be imposed on cyber criminals include imprisonment, fines and other sanctions. As far as imprisonment is concern:

- Anyone who hack into a computer system or network will face imprisonment term of up to 5 years and a fine of up to XAF 10 million (approximately USD 17,000);
- Anyone who is involve into any form of identity theft will face imprisonment term of up to 3 years and a fine of up to XAF 2 million (approximately USD 8,500);
- Anyone who is involve into any form of online harassment will face imprisonment term of up to 2 years and a fine of up to XAF 2 million (approximately USD 3,400).

As far as fines is concern:

- Anyone who is involve into any form of cyber stalking will pay a fine of up to XAF 5 million (approximately USD 8,500);
- Anyone who is involve into any form of spamming will pay a fine of up to XAF 2 million (approximately USD 3,400);

- Anyone who is involved into any form of unauthorized access to a computer system or network will pay a fine of up to XAF 1 million (approximately USD 1,700).

Other sanctions include the court can order the confiscation of equipment and devices used in the commission of cybercrimes; the court can order the perpetrator to pay restitution to the victim for damages suffered as a result of the cybercrime; and the court can sentence the perpetrator to probation, with conditions such as community service or counseling.

V. CHALLENGES FACED IN THE FIGHT AGAINST CYBER CRIMES IN CAMEROON

Some challenges faced in the fight against cybercrimes in Cameroon include technical, human capacity, institutional and regulatory, socioeconomic and international challenges. Technically, Cameroon's telecommunications infrastructure is still developing, making it difficult to effectively monitor and track cybercrime activities; law enforcement agencies lack the necessary technology and tools to investigate and prosecute cybercrimes and the digital divide between urban and rural areas, as well as between different socioeconomic groups, makes it difficult to implement effective cybersecurity measures. (Technical challenges).

At the level of human capacity challenges, there is a shortage of skilled personnel with expertise in cybersecurity, digital forensics, and cybercrime investigation; law enforcement agencies and other stakeholders lack access to regular training and capacity-building programs to enhance their skills and knowledge in combating cybercrime; and that the brain drain of skilled IT professionals to other countries has depleted the pool of expertise available to combat cybercrime.

Institutionally and legally, Cameroon's laws and regulations on cybercrime are still evolving and are not yet comprehensive enough to effectively combat cybercrime; there is a lack of coordination and cooperation among different stakeholders, including law enforcement agencies, telecommunications operators, and financial institutions and corruption remains a significant challenge in Cameroon, which can hinder efforts to combat cybercrime(Institutional and regulatory). At the level of socioeconomic challenges, poverty and unemployment can drive individuals to engage in cybercrime activities; there is a lack of awareness among the general public and businesses about cybercrime risks and prevention measures and cultural factors, such as the lack of trust in institutions, can hinder efforts to combat cybercrime. Internationally, cybercrime is a transnational issue, making it difficult for Cameroon to combat cybercrime alone; there is limited international cooperation and coordination in combating cybercrime, which can hinder efforts to track and prosecute cybercrime perpetrators; and Cameroon's dependence on international expertise and assistance, can create challenges in building local capacity to combat cybercrime.

VI. Conclusion

The fight against cybercrime across Africa in general and Cameroon in particular is a complex and multifaceted issue that requires a comprehensive and coordinated approach. As the country continues to develop its digital infrastructure and online presence, it is essential to prioritize cyber security and protect against the growing threat of cybercrime. This study has highlighted the various the various risks associated with cybercrimes, efforts made so far to combat cybercrimes and challenges faced in combating cybercrime, including technical, human capacity, institutional, socioeconomic, and international challenges. Despite these challenges, there are opportunities for Cameroon and other countries in Africa to strengthen its cyber security framework and improve its response to cybercrime.

The Cameroonian government for example has taken steps to address cybercrime, including the passage of the Cybercrime Law of 2010 and the establishment of the National Agency for Information and Communication Technologies (ANTIC). However, more needs to be done to build capacity, increase awareness, and enhance coordination among stakeholders. Ultimately, combating cybercrime in Cameroon for instance requires a collective effort from government, civil society, the private sector, and individuals.

(A) The way forward

By working together and prioritizing cyber security in Africa, Cameroon in particular can take the following steps:

- Cameroon can create a safer and more secure online environment that supports economic growth, innovation, and social development;
- Cameroon should review and update its cyber security laws and regulations to ensure they are comprehensive and effective;
- The government and other stakeholders should launch awareness campaigns to educate the public about cybercrime risks and prevention measures;
- Cameroon should invest in building the capacity of law enforcement agencies, judiciary, and other stakeholders to combat cybercrime, and enhance coordination among them;
- Cameroon should strengthen international cooperation with other countries and organizations to combat cybercrime and share best practices and coordinate efforts to combat cybercrime;

- Increase funding for law enforcement agencies and judicial institutions to improve their capacity to combat cybercrime; and
- Launch public awareness campaigns to educate the public and businesses about cybercrime risks and prevention measures.

By implementing these recommendations, Cameroon can strengthen its cyber security framework and reduce the threat of cybercrime, promoting a safer and more secure online environment for all.

*****

VII. References

1. E. Akuta and J. Ongloa, (2011, Oct), “Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy and Practice.”*J Peace Gender and Development studies,* [On- line]. Pp.129-137.

2. Fobellah Clinton Atabongakenga et al., (2024), Delineating International Cooperation in the Fight against Cybercrime in Cameroon, *International Journal of Computer (IJC)* - Volume 51, No 1, pp. 99-114.

3. G. K. Muhammad, A. Nawaz and A. Robina, (2014), “Digital Revolution, Cyber Crime and Cyber Legislation: A Challenge to Governments in Developing Counties”, *Journal of Information Engineering and Application,* Vol 4(4).

4. Jerry Hea, * Lisa Chalaguineb, (2023), Natural Language Processing for Cyber bullying Detection, *International Journal of Computer (IJC)* - Volume 49, No 1, pp.84-97.

5. Law N° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality (hereinafter referred to as Cyber law).

6. Ngange, K. L., Nkengafack, E., & Mesumbe, N. N. (2024), Analysing Differences in Social Media Use and Cyberbullying among Male and Female Students of University of Buea in Cameroon, *Advances in Journalism and Communication,* 12, 306-334. https://doi.org/10.4236/ajc.2024.122016.

7. Prof. André Borainea &, Dr. Ngaundje Leno Doris, The Fight against Cybercrime in Cameroon, *International Journal of Computer (IJC)* (2019) Volume 35, No 1, pp.87-100.

8. Rekha, (2024), A study on cybercrime and it’s categories, *International Journal of Criminal, Common and Statutory Law*, pp.1-3.

9. U. O Jerome, (2018), “The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?” *Masaryk University Journal of Law and Technology*, Vol. 12 N0. 2, pp 90-129.

*****