4-2022

Cybercrimes and the Rule of Law in West-Africa: The Republic of Cote d'Ivoire as a Case-Study.

John N. Adu

Cybercrimes and the Rule of Law in West-Africa: The Republic of Cote d'Ivoire as a Case-Study.

Submitted to:

Golden Gate University, School of Law in Fulfilment of The Requirements for The Conferment of The Degree of Scientiae Juridicae Doctor (S.J.D.)

Department of International Legal Studies

By

John N. Adu

Golden Gate University, School of Law (California-USA)
Master of Law – LLM in US Legal Studies
University of Ivory Coast, School of Law (Cote d'Ivoire, West-Africa)
Master in business law
Bachelor in Private Law
Francophone Institute for Entrepreneurship (Canada/Mauritius)
Master in business administration

Dissertation Committee

Professor Dr. Sophie Clavier (Chair)

Professor Dr. Remigius Chibueze (Member)

Dr. Gustave Lele (Member)

San Francisco, California

April 2022

DEDICATION

To:

My Mother**:** Yaoua Noume Odette,

My late Father**:** Ackah Sey John,

My wonderful siblings**:** Annica, Charlotte, Clarisse, Daniel, and Patrick.

Acknowledgements

I would like to express my gratitude to Professor Okeke, Director of the doctoral program, for his unyielding understanding of the physical and mental state I carried with me throughout this research. His many suggestions, advice and expertise have helped me a great deal.

My special thanks to the Committee Members (Professor Sophie Clavier, Professor Remigius Chibueze and Professor Gustave Lele) for their expertise, support and understanding of my unique situation. Your timely feedback has been vital in writing a well-crafted dissertation.

I am grateful for your kindness and patience throughout this research that took more time than allotted.

I also want to thank my beloved siblings Clarisse, Charlotte, Patrick and especially Annica who never stopped encouraging me to pursue this research when I was in a state of deep depression.

I obviously want to thank my mother, Yaoua Odette for her prayers, encouragement, and persistent demand that I finish what I started.

I also want Donna Castelli, my counselor to know that I will always remember our weekly sessions during which she encouraged me to find the strength to write my dissertation. She never gave up on me even when I was not motivated to do anything. She is my guardian Angel and I want her to know that.

Finally, I give praise to my Lord, God, and Savior Jesus Christ, the Virgin Mary, and the legendary Saint Pio of Pietrelcina. They have been with me every step of the way.

To all, your support was priceless./.

Abstract

Since becoming independent nations in the 60s, West-African countries have enacted laws and regulations with the goals of ensuring peace and justice within their respective borders. On the paper, there was no difference between the justice systems of those newly independent nations and the justice systems of their former masters.

Unfortunately, the rule of law in West-African nations since gaining independence, has not always been followed for a myriad of social, cultural, political, and economic reasons. Most justice systems in West-Africa including in Cote d'Ivoire are deeply corrupted, thus rendering the goal of a peaceful society through a fair justice system mute.

With the emergence of a new type of crimes taking place in cyberspace, there has been a logical need to enact new laws to protect the public using the added information and communication technologies (ICT). Over the past few years, multiple cyber-legislations have sprung-up all over Africa including in Cote d'Ivoire.

The fundamental question is to ask whether the enforcement of cybercrimes laws is more successful than the enforcement of traditional laws.

The problem of the enforceability of these cybercrime legislations is compounded by the very nature of cyberspace which is "borderless." Faced with the complexity of those computer crimes taking place in the virtual space, do West-African countries in general and specifically Cote d'Ivoire have the infrastructure, the knowledge, and the workforce to efficiently investigate and prosecute cybercrimes?

This research tries to investigate, expose the theoretical inadequation between cybercrimes legislations and the enforcement capabilities of the Ivorian state, based on the deficiencies of enforcement of traditional laws and the need to stem the tide of corruption in general and specifically in the justice system.

This research uses the case-study method because case studies are in-depth investigations of a single person, group, event, or community. Our findings have confirmed our assumptions that the enforcement of cybercrime laws is flawed due to the lack of proper equipment, skills of law enforcement personnel, even though the country has put in place many agencies to fight against cybercrimes.

The social, cultural, political, and economical determinants that have always inhibited the fair and just enforcement of traditional laws is exerting the same kind of pressure on the capabilities of Law enforcement when it comes to the investigation and prosecution of cybercrimes in Cote d'Ivoire.

This research, far from being exhaustive, needs a follow-up research in the future when the country retrieves its past stability and social peace which will allow a more open cooperation between researchers and the different authorities leading the fight against cybercrimes./.

Acronym

AU: African Union

ABA: American Bar Association

CSIS: Center for Strategic and International Studies

CoE: Council of Europe

CIA: Central Intelligence Agency

DITT: Directorate of Computing and Technological Traces

DoD: Department of Defense

DoJ: Department of Justice

ECOWAS: Economic Community of West-African States

FBI: Federal Bureau of Investigation

GDPR: General Data Protection Regulation

ICT: Information and Communication Technology

SMS: Short Message System

ITU: International Telecommunications Union

PLCC: Platform for the Fight Against Cybercrime

LCN: Digital Forensics Laboratory

TI: Transparency International

UNDP: United Nations Development Program

UNODC: United Nations Office on Drugs and Crime

UN: United Nations

Table of Contents

CHAPTER 1: INTRODUCTION

1-1: Background

Since the dawn of mankind, societies the world over, have created set of rules by which every member of the community must abide by. The more sophisticated the society, the more complex the rules are. In West-Africa, before the arrival of Europeans, African kingdoms were organized around rules whose enforcement felt into the hands of the chief of the village or the King.

These set of rules were known as traditional laws and/or customs. Were they binding?

Yes, because as *M'Begniga Abdoulaye* and Professor *Ma Guang* put it, "no society can function without establishing rules that have binding characteristics and therefore guide the conduct of people in society"[1].

The enforcement of those traditional laws considered, the culture, the social structure, and the political order of the community dating back thousands of years. The arrival of the Europeans in the nineteenth century saw the collapse of the traditional order, replaced with different European legal systems, the English common law, and the French civil law.

The rule of law based on these European legal systems inherited from colonial times, has been difficult to enforce in African societies post-independence, because as Professor *Makau Mutua* put it "the Western concept of the rule of law cannot be simply transplanted to Africa[2]."

1 M'Begniga, Abdoulaye & Guang, Ma. (2017). African Customary Law and Modern Law from Western*:* An Overview on Their Roles and Impacts in African Societies. 5. 188-192.

[2] Mutua, Makau, Africa and the Rule of Law (July 7, 2016). SUR 23 - v.13 n.23, 159 - 173, 2016, Available at SSRN*:* https://ssrn.com/abstract=2838309.

He went on to argue that "the concept must be adapted accordingly to take into account the cultural, geographic and economic peculiarities of each state"[3]. The issue of the effective application of the rule of law sometimes takes a form of competition between the common law and the civil law depending on what legal system one is talking about.

According to *Sandra Joireman*, Common law lawyers and judges tend to believe that the Common law system is superior. She explained that "this opinion is based on the idea that the Common law system inherited from the British is more able to protect the rights of the individual than civil law individual systems[4]".

One must recognize the fact that, irrespective of the type of legal system – English common law or French civil law-, the enforcement of the rule of law in post-colonial African societies has been dismal since the independences at the end of the 50s and earlier 60s.

John Harbeson and Donald Rothchild posit that "elites chose first to consolidate their own power. They stifled dissent, dismantled liberal constitutions, retreated to ethnic loyalties, and buttressed the patrimonial state[5]." This situation created an environment ripe for corruption at every level including the justice system in the majority of African countries.

In most West-African countries, including in Cote d'Ivoire, the object of this research, like in the rest of Africa, the rule of law suffers in the words of Professor Makau, "from the lack of internal cohesion, ethnic rivalries, cultural dissonance, and external interventions[6]."

3 Makau, Africa and the Rule of Law (supra note 2) P.1.
4 Joireman, S. (2001). Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy. The Journal of Modern African Studies, 39(4), 571-596. Retrieved January 22, 2021, from *http://www.jstor.org/stable/3557341*
5 John W. Harbeson and Donald Rothchild, eds., Africa in world politics: reforming political order, 4th ed. (Boulder, Colorado: Westview Press, 2008).
6 Makau, Africa and the Rule of Law (supra note 2) P.1.

The question then becomes: can a society in which the rule of law suffers from multiple defects, allow the proper tackling of a new set of threats like cybercrimes which have solidly taken roots in West-Africa?

Although this research does not pretend to outright answer the question, it will seek to expose some of the flaws of the rule of law in African countries, already denounced by other researchers, and propose a few avenues by which the threat of cybercrimes to African countries can be effectively dealt with.

> *We are living through the most significant period of change that has ever taken place in human history-the digital revolution.*[7]

Over the past thirty years, the world has experienced an exponential growth in the field of new information and communication technologies (ICT). We now live in a "digital world", thanks to the Internet, mobile devices (Smartphone) and the WI-FI. This technological leap forward has helped to cement the concept of globalization.

Nowadays, distances and even languages are no longer a barrier to business, tourism, and communication. The mail (snail mail), the fax and the telex have been replaced by the e-mail, the short message system (SMS) and the chat, thus fostering exchanges between people from around the world at a faster pace.

The over-digitalization of modern societies has created an over-dependency on technology to the point where a major disaster is plausible if we are suddenly disconnected from our digital devices. "If someone were able to switch every digital and electronic device off today, planes would drop out of the sky, cars would stop working, supermarkets would close, large companies would not

7 Raef, Meeuwisse. Cybersecurity for beginners. London, UK: Cyber Simplicity Ltd, 2017. P. 3.

know who worked for them and most banks would probably have no idea about who owed who what".[8]

Unfortunately, besides our over-dependency on technology, which is somewhat concerning, the digital world is also ripe with crimes of all sorts. Criminals in the real world have turned into cybercriminals wreaking havoc all over the world. No entity escapes the dangers of cybercrimes; the victims range from businesses to governments to citizens. "We are all living in an age of perpetual cyber threat. We no longer trust our computers-and everybody is at risk".[9]

The financial losses due to Cyber Criminality around the world are estimated in the hundreds of billions of dollars. Cyber criminality has been engulfing the entire world over the past decade.

Although this study is focused on West-Africa, especially Cote d'Ivoire, one must understand that cybercrimes are a worldwide issue.

In fact, as Dr. Michael Maguire argued in a recent study[10], cyber-crime "has evolved into an entire economy rife with professionalization and filled with parallels to legitimate industries". According to the Center for Strategic and International Studies (CSIS)[11], in 2015, the revenues in cybercrime activities around the world totaled $445 billion.

The West Coast of Africa is one of the regions of the world profoundly plagued by cyber criminality.

8 Meeuwisse. Cybersecurity for beginners (supra note 7) P.3.
9 Paul, Day. Cyber Attack: The truth about digital crime, cyberwarfare, and government snooping. London, UK: Carlton Publishing Group, 2014.
10 Dr. Michael McGuire. Into the Web of Profit: Understanding the Growth of the Cybercrime Economy. Bromium Inc. 2018.
11 Center for Strategic and International Studies. Economic impact of cybercrime. 2018 *https://www.csis.org/analysis/economic-impact-cybercrime* (accessed on 02/03/19).

For *Atta-Asamoah*[12], it all started in the 80s by unsolicited mails sent around the world from West Africa, whose content ranged from business proposals, inheritance reclamation, to money transfers and property sales, among others.

It was then known as the "Nigerian letter" since it originated from Nigeria. Today the phenomenon is known as the "West-African letter"[13] because it has spread in most west-African states.

Nowadays, Cote d'Ivoire is one of the West-African countries plagued by cybercrimes whose impact is felt around the world.

To bring the scourge of cybercrimes under control, the Ivorian government has enacted several laws, some inspired from outside the country. The concern is to know if the application of the rule of law is strong enough to defeat cybercrimes in the country.

Before answering this fundamental question, it is important to first, define the rule of law and analyze the state of the rule of law in West-Africa.

The emergence of cybercrimes around the world has prompted countries and regional organizations to enact a multitude of legislations to fight against the scourge of the twenty first century and cyberwarfare for that matter.

In most countries throughout the developed world like the European Union, those cyber laws are more or less effective in their day-to-day enforcement; the main reason being that the rule of law is qualitatively better applied where there is a need.

European nations and North American nations for that matter, are old democracies where the rule of law endures generations after generations, notwithstanding, their checkered history[14]. On the

12 Andrews, Atta-Asamoah. Understanding the West African Cybercrime process. Institute for security studies: African Security Review Vol 18. No 4.
13 Ibid.
14 Makau, Africa and the Rule of Law(supra note 2) P.1.

other hand, most African nations are young, having gained independence in the 1960s. The rule of law in those recently independent countries is far from perfect. In fact, it is a big concern for human rights advocates the world over, because as the United Nations observes, "corruption remains the most daunting challenge to good governance, sustainable economic growth, peace, stability and development in Africa[15]."

Cote d'Ivoire, like most African countries, remains fragile when it comes to following the rule of law due in part to the spread of corruption everywhere in the land but also due to the political instability that the country has been navigating in for the past two decades.

This state of affairs in Cote d'Ivoire, makes it fundamental to question the success in the fight against cybercriminality within the context of a weak and corrupt justice system, notwithstanding the enactment of an arsenal of laws to guard against it.

To fight cybercrimes around the world, lawmakers in different countries have proposed laws to combat what amount to be the most serious scourge of the 21st century, cybercriminality. Some regional organizations like the Council of Europe have produced a treaty technically called "The Budapest Convention[16] which is at present, the only binding international instrument on cybercrime.

West-African countries have followed the international trend of mounting an arsenal of cyber laws covering ecommerce, privacy, and data protection to safeguard the public interacting in cyberspace. All the experts agree that cyberspace is transnational in nature and that while the victim of a romance scam may be living in Rome, the perpetrator is certainly living in West-Africa.

[15] *Africa*. (2020, September 15). United Nations. https://www.un.org/en/sections/issues-depth/africa/index.html
[16] Council of Europe. (2018). Budapest Convention and related standards. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

This novel paradigm in terms of law enforcement operations beyond the physical borders raise questions about the capabilities of African Law Enforcement Authorities to enforce those cyber laws efficiently, skilfully, and fairly on the book, especially in the contest of an environment plagued with corruption, judicial interference, and cultural taboos?

This research aims to explore the determinants affecting the fair application of the rule of law in the case of Cote d'Ivoire and to compare what is being done legislatively to fight cybercrimes, with other countries both in West-Africa and beyond in order to answer a few questions:

- Is the rule of law in Cote d'Ivoire strong enough to facilitate the fight against cybercriminality?
- Are the Ivorian Law Enforcement Authorities well equipped, skilled, and motivated enough to safeguard the reputation of Cote d'Ivoire around the world by being without mercy against cybercriminals?
- Does a strong cooperation between Cote d'Ivoire and some advanced countries necessary to win the "war on cybercrimes"?
- Could the fight against cybercriminality help to strengthen the rule of law around the country?

These are some of the questions we intend to find answers to with regard to the legal fight against cybercrimes in the context of determinants negatively affecting the delivery of the rule of law in Cote d'Ivoire.

Studying cyber criminality in West-Africa in general and in Cote d'Ivoire in particular, assumes that we have an efficient method to capture the essence of what we are trying to convey or expose.

In this research, we consider the general environment in the target geography which is West-Africa to put in context what is happening in Cote d'Ivoire. We also delve although lightly into cyber-crimes around the world.

To achieve our goals, we use the Case Study Method. Case studies are in-depth investigations of a single person, group, event, or community. Typically, data are gathered from a variety of sources and by using several different methods (e.g., observations & interviews)[17].

Chapter 1 begins the journey with an introduction to African societies pre-colonial times, to show that the rule of law existed in African societies and well enforced based on the traditions and customs of each African tribe or kingdom.

However, the arrival of the Europeans in the 19th century, and the imposition of the European model of rule law helped destroyed the social that pre-existed their arrival. This historic flaw in how African societies deal with the rule of law will have a serious impact on the social, cultural, economic, and political stability of most African countries.

These determinants (social, cultural, economic, political) play a huge role in rendering obsolete the rule of law in African nations. Therefore, the emergence of cybercriminality in Africa at the beginning of the 21st century, with its own complexities will be a huge challenge to the rule of law in Africa and especially in Cote d'Ivoire.

Chapter 2 describes the emergence of cybercrimes in Cote d'Ivoire at the end of the 20th century, first through nationals of neighbouring countries, and later through Ivorian nationals. We also delve into how cybercrimes committed in and from Cote d'Ivoire have had a negative impact on

[17] McLeod, S. A. (2014, Feb 05). *Case study method*. Retrieved from https://www.simplypsychology.org/case-study.html

the reputation of the country around the world. We will also describe the nomenclature of cybercrimes in Cote d'Ivoire.

Chapter 3 combines and dissect laws against cybercrimes adopted by Cote d'Ivoire to successfully root out cybercriminality in the country. This chapter also describes the influence of international and regional treaties and their impact on the laws adopted by the Ivorian legislator.

Chapter 4 deals with the difficult enforcement of cyber laws in Cote d'Ivoire in light of the powerful entrenchment of old determinants like the social, cultural, economic, and political factors which are an obstacle to the proper enforcement of the rule of law.

Chapter 5 summarizes the research and suggests avenues of solutions to the issues of the day to the stakeholders, both in Cote d'Ivoire and in West-Africa.

This dissertation focuses primarily on cyber-crimes in the Republic of Cote d'Ivoire as a case-study.

To put the Ivorian case in proper context, we have dedicated an important portion of the study on the rule of law in West-Africa. You cannot accurately assess the implications of cyber criminality in Cote d'Ivoire without analyzing the bigger picture of how cybercrimes started and spread all over West-Africa and beyond.

The world has become a "true" global village, and we have also analyzed the adequation between the lofty goals surrounding the enactment of cyber laws in African countries and the reality of a corrupt justice system which in turn, mirrors the generalized corruption in third world countries.

It is obvious that we cannot answer all questions we raised at the beginning of this research but have tried to compare what is done in the target country, Cote d'Ivoire and elsewhere in Africa

and beyond. It will be important to continue to dig into the subject of the rule of law in poor countries and the mechanisms that strengthen or weaken it. That work is for future research.

1-2: Definition of the rule of law

It is better for the law to rule than one of the citizens. Aristotle[18].

The online encyclopedia Britannica[19] defines the rule of law as "the mechanism, process, institution, practice, or norm that supports the equality of all citizens before the law, secures a nonarbitrary form of government, and more generally prevents the arbitrary use of power."

The expression "rule of law" according to *Tom Bingham*[20], was first coined by Professor A.V. Dicey in his book, "An Introduction to the Study of the law of the Constitution," published in 1885. Based on the definition above, the rule of law "supports the equality of all citizens before the law"[21]. One must recognize that the rule of law does not always supports that equality of all citizens before the law. One must remember the rule of law in South Africa during the Apartheid era. Black South-Africans were not on an equal footing with the white minority as far as the rule of law was concerned.

Here in the United States, the Jim Crow Laws[22] created a separation between whites and Black people in the south in which, the equality element of a rule of law was grossly missing in those laws. The American Bar Association[23] (ABA) in its definition of the rule of law, emphasizes the existence of clear and fair processes for enforcing laws, with an independent judiciary before which, human rights are guaranteed for all.

18 Bingham, T. (2011). The Rule of Law (Reprint ed.). Penguin UK
19 Choi, N. (2019, August 27). Rule of law. Encyclopedia Britannica. https://www.britannica.com/topic/rule-of-law (Accessed on 01/19/2020)
20 Bingham, T. (2011). The Rule of Law (supra note 18) P.11.
21 Choi, N. Rule of law. (Supra note 19) P.11.
22 University of Southern California. (2020, March 19). Brief History of Jim Crow Laws | Online LLM Degree. Online International LLM Degree Program. https://onlinellm.usc.edu/a-brief-history-of-jim-crow-laws/ (Accessed on 01/29/2021).
23 American Bar Association. (2019). Rule of Law. ABA. https://www.americanbar.org/groups/public_education/resources/rule-of-law/ (Accessed on 02/07/2020)

The truth of the matter is that human rights are not always guaranteed around the world based on the definition by the United Nations[24] which says that human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. It added that human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more.

The good news is that the rule of law existing during the Apartheid, or the Jim Crow Laws have been sent to the dustbin of history. When we talk about the rule of law in West-African countries and especially in the republic of Cote d'Ivoire, we are dealing with historic paradigms linked to colonialism followed by the birth of young nations learning to self-govern.

Those paradigms include but are not limited to the transplantation of foreign legal systems in most African nations on top of traditional laws and customs, the instability of the young nations of Africa and the social divisions within African countries along ethnic lines, economic status which is often determined by one's political affiliation or not.

For this reason and many more, it is a foundational requisite to review although summarily, the state of the rule of law in West-African countries primarily, before determining the fate of the fight against cybercrimes by African nations and the republic of Cote d'Ivoire./.

24 United Nations. (2020). Human Rights. UN. https://www.un.org/en/sections/issues-depth/human-rights/ (Accessed on 02/23/2019).

1-3: State of the rule of law in West-Africa

The state of the rule of law in West-Africa is qualitatively the same as in the rest of Africa: at best, seriously flawed, and at worst, non-existent. This situation is the reason why *Dr. Nicholas A. Curott*[25] thinks that it is nonsensical to expect . . . economic development in Africa without addressing the institutional factors, such as the lack of Rule of Law, which are responsible for Africa's failure to develop in the first place.

Most West-African countries including Cote d'Ivoire became independent in the 60s from colonial masters Great-Britain, France, and Spain. These newly independent nations inherited the legal system put in place by their respective colonial master.

The non-democratic nature of most governments of the region, compounded by the extreme poverty of the newly independent countries and the obvious lack of technical skills to govern properly, created the sense of social, political, and judicial chaos in the first few decades of independence. As *Mutua Makau*[26] reminded us, opaque and oppressive one-party states and military dictatorships proliferated on the continent. The rule of law which in the word of Professor Mutua, is a pillar of governance notwithstanding, its checkered history was the first victim in those West-African nations. Nigeria, Niger, Mali, Togo, Benin, Sierra-Leone, and Ghana went through military coups while others experienced a civil war as in the case of Nigeria.

The oil crises[27] of the 70s will make things worse leading to the birth of organized crime in West-Africa.

25 N.A. Curott, Foreign Aid, the Rule of Law, and Economic Development in Africa, 11 U. BOTS. L.J. 3, 14 (2010).
26 Makau, Africa and the Rule of Law *(supra note 2)* P.1.
27 United Nations Office on Drugs and Crime report. Transnational organized crime in the West African Region, P.4.

The justice systems in most West-African nations including Cote d'Ivoire suffered and continue to suffer from the original sin which was the transplantation of foreign legal systems unknown to African populations pre-colonialization.

The lack of democratic governance which is a pillar of a fair and just legal system in those countries gave birth to a massive corruption at all levels of society. *Charlotte Heyl*[28] points out the insidious fact that African courts experience undue interference.

It is obvious that not having a legitimate government in place always lead to an abuse of power be it in the political or in the judicial arena.

On the other hand, the existence of a legitimate form of government does not always guarantee the rule of law as defined by *Choi*[29], which is to support the equality of all citizens before the law. Over the past two decades, many West-African nations have been holding fair elections leading to more stable societies with legitimate governments.

Countries like Nigeria, Ghana, Senegal, Benin, and others can now be considered democracies although that distinction can be narrowed to the process of holding fair elections only. The other aspects of a society governed by the rule of law, like the protection of individual rights, fair access to justice remains at best, a work in progress and at worst non-existent./.

[28] Heyl, C. (2019, July 29). The Judiciary and the Rule of Law in Africa. *Oxford Research Encyclopedia of Politics.* Retrieved 31 Jan. 2021, from https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1352. "African courts experience undue interference—which frequently takes place informally. Informal interference can occur through the biased appointments of judges, verbal and physical threats, violent attacks, the payment of bribes, or the ouster of sitting judges. Informal networks—held together by ties based on shared educational trajectories, common leisure activities, religion, kinship relations, or political affiliations—are the channels through which such pressure can be transmitted."

[29] *Choi, N. Rule of law (supra note 19)* P.11.

The Rule of Law in Cote d'Ivoire

Over the past few decades, the West-African region has become a major hub when it comes to cybercrimes. Hamadoun Touré, an ex-secretary-general of the International Telecommunications Union (ITU) said a few years ago that "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity"[30].

The enormous challenges posed by cybercriminals in West-Africa to the different governments come on top of more traditional law enforcement issues. For once, the cyberspace in which the crimes occur in the words of Bryan Harley[31] is "transnational in nature." West-African law enforcements in most cases lack the skills and the infrastructure to fight efficiently cybercrimes.

The rule of law in these countries including Cote d'Ivoire, is problematic in that it is impossible to defeat cybercrimes if the justice system is plagued with multiple defects like corruption, political pressure and interference and other social ills.

Although, Cote d'Ivoire deserves some praise for tackling earlier on the scourge of cybercriminality by enacting several laws, the issue is in their implementation in the real-world. To do that successfully, it is fundamental to have a society in which the rule of law applies equally to everyone, without interference, and in which the public has a fair amount of trust. Now, the question becomes, is Cote d'Ivoire a "good student" when it comes to having a just and fair justice

[30] Kshetri N. (2013) Cybercrime and Cybersecurity in Sub-Saharan African Economies. In: Cybercrime and Cybersecurity in the Global South. International Political Economy. Palgrave Macmillan, London. https://doi.org/10.1057/9781137021946_8

[31] Brian Harley "A Global Convention on Cybercrime?" March 23, 2010. The Columbia Science and Technology Law Review. Volume XX (2010-2011). http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/ (Accessed on 05/09/19).

system trusted by the social corpus? Depending on the answer to this vital question, will we know if it has a good chance to fight and win against cybercriminals who are young and educated for the most part; in other words, those who represent the future of Cote d'Ivoire.

The purpose of this dissertation is to compare the chances of success of the Ivorian legal arsenal to fight cybercrimes in the context of the state of the rule of law in the country. The cyber laws enacted by the Ivorian government to fight cybercriminals obviously do not exist in a vacuum. They are part of the general legal apparatus that the country relies on to foster social peace and resolve disputes between people and/or between the state and individuals. Epistemologically, it is crucial to first dissect the state of the rule of law in Cote d'Ivoire and points out the different determinants preventing a more forceful and fair application of the rule of law. The second step is to analyse the legal arsenal put in place by the Ivorian government to fight cybercrimes.

We will compare the Ivorian effort with other West-African countries, the ECOWAS *Directive on the Fight Against Cybercrimes* and as a last resort, study the adequation between the Ivorian legal effort with the African Union *Convention on Cybersecurity and Personal Data Protection*[32].

Finally, we will explore other avenues related to cybercrimes treaties like the *Budapest Convention*[33] and the *General Data Protection Regulation* (G.D.P.R)[34] and determine if Cote d'Ivoire could benefit from these international treaties.

[32] Antonio, F. (2018). *Library â€ ¢ ICT Policy Africa*. A.U. https://ictpolicyafrica.org/
[33] Council of Europe. (2018). *Budapest Convention and related standards*. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention
[34] GDPR.eu. (2019, February 19). General Data Protection Regulation (GDPR) Compliance Guidelines. https://gdpr.eu/

One of the goals of this study was to verify on the ground the enforcement of the laws enacted to combat cybercriminality in Cote d'Ivoire within an environment in which the rule of law is applied according to the customer's head.

Thus, the main issue is not the existence of specific laws to fight a social scourge like cybercriminality but their effective enforcement free from any interference whatsoever./.

2-1: Historical background

> *Rule of law is at risk around the world. … It is by reintroducing the rule of law, and confidence in its impartial application, that we can hope to resuscitate societies shattered by conflict.*[35] *Former UN Secretary General,* ***Kofi Annan****.*

The year (2004) Secretary-General Kofi Anan made the above declaration, Cote d'Ivoire was in the midst of a civil war opposing northern rebels to the central government in the south. The rule of law during those years was gravely endangered by the generalised atmosphere of suspicion, fear, and overt hate between the warring sides.

Extrajudicial executions took place in many parts of the country whose authors to this day have yet to feel the weight of justice.

Unfortunately, since its independence from France, Cote d'Ivoire like the rest of African countries, has yet to guarantee a fair and just justice system for its citizens irrespective of their ethnicity, social status, and political affiliation.

Before the arrival of European colonists in Africa, including in Cote d'Ivoire, the native populations had their own legal systems within the confines of the different kingdoms. We can speculate about the sophistication of these local legal systems, but as the maxim goes "ubi societas, ibi jus[36]."

[35] Human Rights Watch Briefing Paper. (2004). *Côte d'Ivoire Accountability for Serious Human Rights Crimes Key to Resolving Crisis*. H.R.W. https://www.hrw.org/legacy/backgrounder/africa/cote1004/accountability.pdf

[36] *Ubi societas, ibi ius*. "Wherever there is society, there is law." A maxim meaning that law may be found in all forms of stable ... (2011). Oxford Reference. https://www.oxfordreference.com/view/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-2028?rskey=8TGbxr&result=2029

Those customary laws were relegated to the back burner during colonial times or as Mbambi V.K put it "rather than talking about the coexistence of rights, it is appropriate to speak of the subjugation of African legal systems by Western law[37]."

In practice, customary laws were narrowly applied alongside the official law (French Civil Code) with different audiences[38]. The Code civil applied to the settlers while the customary laws were applied uniquely to Ivorians.

The juxtaposition of the European legal system over traditional laws in African societies and particularly in Cote d'Ivoire created some sort of a "rebellion" against the law of the "white man[39]."

Thierry Verhelst[40] foretold this situation back in 1968 when he said "the imposition of a foreign legal system may result either in failure of the law to receive acceptance and enforcement, or in

[37]Mbambi, V. K. (2005). Originally African rights in recent codification movements: the case of French-speaking sub-Saharan African countries. Les Cahiers de droit, 46 (1-2), 315–338.https://doi.org/10.7202/043841ar (Accessed on 02/12/2021). "This resulted in a kind of a "war of standards" translated by the euphemism "dualism" or "Legal pluralism" or, again, by "legal syncretism". In his enterprise of legal acculturation, the colonizer did not content to legislate on certain matters likely to establish its authority or power. This enterprise lasted for about a century, in other words, the time of colonization. With political emancipation movements, political demands often accompanied by legal claims, it seemed necessary for Africans to dismantle colonial philosophy, including its instrument of domination: the colonial law. In the eyes of Africans, the Civil Code of the French does indeed appear as an ideological instrument, both literally and figuratively. Indeed, if it is accepted that most of the provisions of the Napoleon Code of 1804, enacted or adopted in full philosophical and economic liberalism, have served to sublimate liberal society, it is also possible to recognize that it served other purposes: political domination, assimilation, acculturation legal through ignorance or disregard for otherness ...".

[38] *Africa: Laws and Legal Systems*. (2016). Laws and Legal Systems. https://geography.name/laws-and-legal-systems/ (Accessed on 02/17/2021). "The French, like the British, developed a dual system for Africans and non-Africans. They appointed traditional authorities to deal with matters involving Africans under customary law. In addition, the French tried to record local laws and codify them so that they could be applied in a consistent manner. These efforts made little headway, though, because of the sheer size of the task, the lack of personnel to accomplish it, and the difficulty of standardizing a body of law that is flexible by nature.
When codified versions of some customary laws were produced, the African laws were altered to reflect French views and legal traditions. These revised versions ignored local standards of conduct and social behaviour and so were less effective than the original laws in dealing with local disputes."

[39] The African usual way to identify Europeans instead of the country of origin.

[40] Thierry Verhelst. (1968). *Safeguarding African Customary Law: Judicial and Legislative Processes for its Adaptation and Integration*. African Studies Center University of California, Los Angeles, California. https://escholarship.org/content/qt33g2v27d/qt33g2v27d_noSplash_42d5da862de9136b469c2414312669d6.pdf

unnecessary and harmful wrenching of the social fabric of the society concerned. This in turn might lead either to the undermining of the authority of the law, or to the disruption of society."

It is important to note that customary laws have not disappeared totally in Cote d'Ivoire, exist alongside the "imported legal system" to this day, but the suspicion toward the official legal system inherited during colonial times, does persist in some corners of the country. This historic determinant compounded by new determinants post-independence will become an important obstacle to the delivery of a fair and just rule of law in the land.

We can classify these determinants in four (4) groups comprising the social (1) determinant, the cultural (2) determinant, followed by the Economic (3) and the Political (4) determinants which taken together, negatively inhibit the application of the rule of law in Cote d'Ivoire. Let us dissect those obstacles and see if they can negatively impact the fight against cybercriminality in Cote d'Ivoire and in the rest of Africa for that matter.

2-2: Determinants inhibiting the Rule of Law.

> *A social norm, even made compulsory by a legal text, will only apply if it is sociologically practicable. The justice pursued by the rule of law based on a system of values must always be accompanied by a study of sociological practicability*[41].

The inefficiency of the rule of law in Africa and in Cote d'Ivoire derives from at least four types of "inhibitors" whose overall impacts are sometimes catastrophic for the social peace.

The four (4) inhibitors to the rule of law in Cote d'Ivoire and in the rest of Sub-Saharan Africa for that matter, are respectively the Social and Cultural determinants, followed by the Economic and the Political determinants. Let us start with the social "inhibitor" to the rule of law in Cote d'Ivoire.

2-2-1: Social Determinant inhibiting the Rule of Law.

As Matala-Tala[42]pointed out above, a social norm, even made by a legal text, will only apply if it is sociologically practicable. In West-African societies and especially in Cote d'Ivoire, people have since immemorial times, settled their disputes within the confines of the community which in fact, means the tribe to which we belong, irrespective of where we live in the nation.

If the protagonists are from different ethnic backgrounds, the heads of both communities will sometimes intervene to settle the dispute peacefully. The efficacy of those traditional mechanisms for dispute resolution in Cote d'Ivoire have been so successful over many generations that, after the second civil war in 2011, the United Nations borrowed this social mechanism with the objective to "reinforce community dialogue and participatory democracy" with a view to "enhancing social cohesion and the enhancement of democratic values at local level[43]".

---

[41] Matala-Tala, L. (2013). The ineffectiveness of positive law in sub-Saharan Africa [1]. Civitas Europa, 2 (2), 239-260.https://doi.org/10.3917/civit.031.0239 (Accessed on 02/18/2021).
[42] Ibid.
[43] The United Nations Democracy Fund-UNDEF-. (2016). UDF-IVC-11-417*:* Promotion of democratic dialogue and social cohesion in western Côte

The practicability of laws in a poor country like Cote d'Ivoire is in question due to the complexity and time consuming of legal procedures to resolve disputes between citizens or even between citizens and the State. The Ivorian Civil Code being in most aspects a mirror image of its French counterpart does not always take the specificities of local customs and behaviour into account.

The rule of law in Africa and in Cote d'Ivoire specifically is complex and tend to provoke a conflict between two completely different conceptions of life in society: the western approach based on individualism and the African approach based on community. Moyran[44] argued that "the approach is legitimate but probably impossible for lack of meeting of the conditions which allowed its development." He pointed out that "contrary to Europe, African socio-political entities are of the community"[45]. As Chantal Yoroba[46] reminds us, at independence, a minority of people are subject to French civil law, while the rest of the population is governed by customary law.

To remedy the situation, the country enacted the civil code of 1964 which President Felix H. Boigny[47] defended as being necessary to modernise the legal apparatus of the newly independent

d'Ivoire.https://www.un.org/democracyfund/sites/www.un.org.democracyfund/files/cote_divoire_-_udf-11-417-ivc_-_evaluation_report.pdf (Accessed on 02/18/2021).

[44] Moyrand Alain. Reflections on the introduction of the rule of law in French-speaking black Africa. In: International review of comparative law. Vol. 43 N°4, October-December 1991. pp. 853-878; doi: https://doi.org/10.3406/ridc.1991.4401 https://www.persee.fr/doc/ridc_0035-3337_1991_num_43_4_4401

[45] Ibid. He then explained that "We are therefore in the presence of an inverse diagram to that which we have described above, since here it is the primacy of the collective over the individual that prevails. In fact, man "is never isolated: he belongs to a lineage, to a family, he is a member of a village, of a corporation, of a caste, of a clientele. Within his lineage, he feels in a space of freedom: the solidarity of all guarantees the safety of each. This social structuring has important repercussions at the level economic. The solidarity that unites the members of the group "excludes any accumulation of wealth. Better, social prestige is a function, in traditional Africa, of the capacity to share (or waste) wealth during sumptuary ceremonies consecrated by the community (marriage, birth, mourning, initiation). It is the economy of gift that opposes the economy of savings and the concentration of riches in the same hands". These values are at odds with those of economic liberalism and it is hardly surprising to observe that the conception of the subsistence economy specific to African communities constitutes a powerful obstacle to the introduction of the structures of industrialized countries".

[46] Chantal VLÉÏ-YOROBA, "Family law and family realities: the case of Côte d'Ivoire since independence," Clio. History ,women and societies [Online], 6 | 1997, posted on January 01, 2005, Accessed February 19, 2021. URL: http://journals.openedition.org/clio/383 ; DOI : https://doi.org/10.4000/clio.383 .

[47]Ibid. The President said "When it appeared to us that the survival of certain traditions constituted an obstacle or a brake on the harmonious development of our country, we did not hesitate to make the necessary changes. Thus, after a long campaign of explanation undertaken by our activists and our political and administrative leaders with the

nation. In reality, the "revolutionary" Ivorian civil code was a photocopy of the French civil code. For example, as Chantal Yoroba pointed out, the law repeats in article 2 paragraph 1, the formula of article 147 of the French civil code "No one may contract a new marriage before the dissolution of the preceding one".

Here, polygamy[48] and dowry which were a staple of African life long before colonial times were suppressed. In the real world, however, the populations found ways to violate these two legal prescriptions either for the man to legally marry a woman and then to customarily "marry" more women. This was the case in my own family.

For the dowry, the enforcement was just impossible since families do not report each other when the dowry is involved. The burning desire of the Ivorian government to "modernise" the law, or what Granger Roger[49] called a "legal decolonization" resulted in an inflation of texts more formal than real.

In practice, these legal reforms had negligible impact on the target population which found ways to outsmart the system by strongly leaning on those values transmitted from generation to

concerned populations, essential texts have emerged. A renewed Civil Code consecrates the abolition of polygamy and reforms the dowry; a modern civil status is in place".

[48] Chantal VLÉÏ-YOROBA, "Family law and family realities.*(supra note 46)* P.22.

"In other words, polygamy is purely and simply suppressed. Regarding the fate of polygamous unions contracted before the date of entry into force of this new law, the polygamous spouse retains the acquired right for his previous marriages but may not contract a new marriage until after dissolution of the marriages in which he was previously engaged".

[49] Granger Roger. Tradition as a limit to legal reforms. In: International review of comparative law. Flight. 31 N ° 1, January-March 1979. pp. 37-125;doi: https://doi.org/10.3406/ridc.1979.3348 https://www.persee.fr/doc/ridc_0035-3337_1979_num_31_1_3348 (Accessed on 02/24/2021). The author detailed the path followed by third world countries: "With regard to the relationship between traditional law and modern law, these States theoretically had the choice between three solutions. The traditional law was fully restored, tolerating some additions of modern law. This is partially the case with the Democratic Republic of the Congo with its return to African authenticity. Either modern law swept away customary law: it is the choice of China rejecting feudal law and bourgeois law. Or again, the State maintained the coexistence of traditional law and modern law in variable proportions: this is the position adopted by most of the Third World countries. This option between traditional law and modern law is revealed to be exceedingly difficult and depends, as we shall see, on complex factors, sociological, economic, political. One of these factors needs to be pointed out now in order to understand the varying resistance of tradition to law reform. This is the theory of the double sector, in the social structure of developing countries, traditional sector and modern sector."

generation and are based on the sacred meaning within the confines of the tribe. Unlike western nations which have been de facto nations for millennia, African nations are noticeably young, most having acceded to independence after World War two as Granger reminds us.

In fact, as he correctly pointed out, the State pre-existed the Nation in most African countries if we agree that the concept of a nation is defined as a geographic land, a population and an institutionalized power recognized by the outside world and within the confines of the State. In Cote d'Ivoire, before the creation of the colony of the same name, there were small kingdoms interacting among them on a bilateral or sometimes on a multilateral basis.

They are called "intra-ethnic alliances[50]" and span the entire country and beyond. Here is **a list of few alliances**:

Ethnic group	Allies
ABBEY	Dida, Abouré, Abidji, M'Batto
ABIDJI	Adjoukrou, Abbey, Dida, M'Batto
ABOURÉ	Appolo, Ébrié, Abbey, Attié
ABRON	Koulango, Agni, Baoulé, Senoufo, Dioula, lobi, Ashanti (*)
ADJOUKROU	Ahizi, Abidji
AGNI	Baoulé, Abron, Attié, Ano
AHIZI	Adjoukrou, Alladian
ALLADIAN	Ahizi, Adjoukrou

Source:Lifemag-ci.com.

[50] Kotto, R. (2019, January 14). Chez nous pays: Discover the inter-ethnic alliances in Côte d'Ivoire | Life Magazine. Lifemag-Ci. https://lifemag-ci.com/chez-nous-pays-decouvrez-les-alliances-inter-ethniques-en-cote-divoire/ (Accessed on 02/24/2021). Here is an explanation about intra-ethnic alliances: "No one shows their village with their left hand. In some alliances, there is one people who is superior to another according to the history that created the alliance. But over time, collective memory has almost put this shutter under fire. Becomes the leader of the other, the one who knows how to use the word and inflict mockery and bullying. As an illustration, take the case of the Niaboua and the Baku. During the funeral ceremonies of a niaboua village chief (Béliéguhé, 21 km from Issia), a bakoue interrupted the ceremony. He forced "his slaves" niaboua to find him 5,000 FCFA in 5 FCFA coins in addition to a bottle of gin. The villagers returned where they were supposed to and found him as demanded the sum of 5,000 FCFA in currency of 5 FCFA. Such scenes are everywhere across the country and despite town planning, metropolises, alliances resist time. We can cite, for example, the case of the Fulani who runs a kiosk in a district of Adjamé. A Yacouba from the same neighbourhood as he eats there every night and pays as he sees fit, just because according to history, the Fulani are the slaves of the Yacouba. Inter-ethnic alliances allow all kinds of mockery and abuse but prevent violence between allied peoples. Moreover, it calls for assistance to the allied people in the event of an external attack, famine, or health crisis."
*Ethnic group from neighbouring Ghana.

The ethnic group is preponderant in Ivorian society and tend to supersede the notion of nation. People tend to identify first as Abron, Baoulé, Senoufo before considering themselves Ivorians. In fact, Granger[51] considers the ethnic group as being the most important aspect in third-world nations and that is true in Cote d'Ivoire as well.

The sociology of the Ivorian society, similar to the rest of African nations is such that more than half a century after gaining independence from France, the notion of the rule of law is still dependent on the social structures of the country.

That means, those inter-ethnic alliances play a key role when it comes to dispute resolutions and to facing the official justice system. The inter-ethnic alliances being primarily based on "non-aggression," or non-violence obligate citizens to help each other in any situation: that means that an Abron who has legal troubles and who learn that the judge in his case is Koulango will not hesitate to seek the judge's leniency based on this alliance dating back centuries.

In fact, the inter-ethnic alliances in Cote d'Ivoire are so vital that the United Nations Educational, Scientific and Cultural Organization (UNESCO)[52] announced in 2020, that it was developing a

[51] Granger Roger. Tradition as a limit to legal reforms *(supra note 49)P*.23."The most important aspect is the division of the country into ethnic groups. These differ from each other in customs, language, religion, level of education and economic development. Ethnic patriotism risks preventing patriotism at all. When the state is in fact in the hands of a dominant ethnic group, tensions and conflicts arise and sometimes go as far as civil war, Ibos in Biafra, violent ethnic clashes in India, Pakistan, etc. An example of the difficulties encountered in the legal establishment of the state is in the application of constitutional rules. Most of the countries have imported from the West different model constitutions, a few parliamentary constitutions, many presidential constitutions, and a few constitutions from Eastern Europe. Very quickly these constitutional regimes changed profoundly. The tradition of the "leader" has accentuated the presidential dominance. A transposition of the custom of unanimous decision-making has played a role, along with other factors, for the generalization of the single party."

[52] UNESCO announces the creation of a mobile application for interethnic alliances in Côte d'Ivoire. (2020). Abidjan.Net. https://news.abidjan.net/h/682520.html (Accessed on 02/25/2021). "We are developing a mobile application for interethnic alliances in Côte d'Ivoire to raise awareness among young people about conflict prevention and management. We want to recall the importance of interethnic alliances in this electoral context," explained in a press conference, Anne Lemaistre, the representative of the UNESCO office in Abidjan.

mobile application for interethnic alliances in Côte d'Ivoire, with the aim to promote this cultural mechanism of "non-aggression" between peoples.

The social determinant is certainly an obstacle to the rule of law as it distorts the relationship between citizens and the law through a web of alliances that have endured for generations. Thus, the fight against cybercrimes in Cote d'Ivoire, to succeed must consider the social determinant and all other inhibitors to the rule of law for that matter and find appropriate solutions to restore the image of Cote d'Ivoire both in the eyes of its citizens and of the outside world.

A few recommendations to tackle the social inhibitor to the delivery of a fair and peaceful rule of law.

Recommendations

The Ivorian Authorities could use the concept of "Inter-Ethnic Alliances" to effectively fight the social inhibitor through the prospect of "shaming" members of an inter-ethnic alliance who are caught violating the law in general but specifically committing cybercrimes since they destroy the image of the country around the world.

To do that, an effective campaign within communities throughout the country is needed. The key word here, is to tell community[53] leaders, that they should sensitize their members against cybercrimes because if caught, it is the entire community that will feel the shame brought on by the few. I must recognize that there is a risk of stigma among the population whenever cybercriminals are identified by ethnic group.

[53] Community here refers to ethnic communities living in urban areas like Abidjan, the commercial hub.

To avoid that, it is the prospect of shaming that should be instilled inside communities, not the execution of the threat itself. One other way to proceed would be to give the total initiative to community leaders within ethnic groups.

These community leaders should get some financial aid from the government to deploy targeted campaigns around the country. They should insist on the image of Cote d'Ivoire around the world and that cybercrimes destroy countless opportunities for the Ivorian youth.

2-2-2: Cultural Determinant inhibiting the Rule of Law.

Culture is defined as "the customary beliefs, social forms, and material traits of a racial, religious, or social group[54]." The general culture in Cote d'Ivoire is an obstacle to the rule of law in that it is deeply ingrained in the social fabric of the different ethnic groups forming the nation.

The inter-alliances between ethnic groups originally based on non-aggression because there were wars between ethnic groups, now extends to the everyday life situations like two (2) people from allied ethnic groups having some dispute and deciding to resolve it customarily instead of going before a judge.

A priori, this behaviour has positive aspects in that it is a traditional form of alternative dispute resolution (ADR) which is used in the modern justice system. The issue arises when the cause in dispute is something more serious like an accidental death during a hunting party or in a case of drowning. According to Professor Amoa Urbain[55], in the case of a direct alliance between

[54] *Culture*. (2020). The Merriam-Webster.Com Dictionary. https://www.merriam-webster.com/dictionary/culture (Accessed on 02/27/2021).

[55] Stability pacts and confidence building in the process of social cohesion. (2011).https://gerflint.fr/Base/Afriqueouest3/amoa2.pdf (Accessed on 02/27/2021). "Level 1: (direct alliance): between two allied peoples (blood pact, assistance pact, good neighbourly agreement, non-aggression pact ...): the rule is applied systematically. Even in the event of a fatal accident (hunting, drowning, etc.) nowhere does the

the parties, the modern court does not intervene despite the seriousness (loss of life) of the situation. This demonstrates the power of the legal culture derived from customary law over the modern legal system. Another area where the cultural determinant inhibits the rule of law, sometimes in bloody ways (when the official law is applied) is in the field of land laws. Despite the existence of those land laws[56] since colonial times, in the real world, most land transactions were based on customary law.

As Daniel Lopes et al.[57] explained in their report, for a long time, "land management was governed by customary law." This culture of trying to resolve any issue by customary means, although positive at times, can prevent litigants from sizable compensations if the issue was brought before the tribunal. It has created among the populace this sentiment that every violation of the law (official), can be and should be dealt with through traditional means which extend to the justice system itself by way of "corruption;" Litigants do not necessarily believe

modern court intervene arbitration is conducted under customary authority. - Level 2: (indirect alliance): in the event of a direct non-alliance between two peoples, the delegation responsible for intervening in a conflict may be made up of several people, including one or two from one or two allied peoples. Thus, if a Wè conflicts with a Senufo, one or the other can bring in a Gouro, a people allied with both the Wè and the Senufo. This second level of reading cannot be done systematically: the Agni are allies of the Bron (Abron) and the Ano, but the Bron are not, for the Ano, joking parents."

[56] Legal pluralism in land matters in West Africa: the case of Côte d'Ivoire. (2016). Sylvia Soro, Daniel Lopes, Seynabou Samb. https://www.legitimus.ca/static/uploaded/Files/Documents/Rapports/Rapports2/Le-pluralisme-juridique-en-matiere-fonciere-en-Afrique-de-l%E2%80%99Ouest---le-cas-de-la-Cote-d%E2%80%99Ivoire.pdf (Accessed on 03/01/2021). The report goes on to dissect the land law in historic terms: "The analysis of the data shows that the relationship between state and customary legal orders follows an initial vertical dynamic. This vertical dynamic starts from the colonial period until the adoption of Law No. 98-750 of 23 December 1998 on rural land. During this period, land management was based on the rules of customary law despite the existence of colonial legislation. The final adoption of the Rural Land Law of 1998 leads to a hierarchical dynamic which gives modern law a superior place and customary law a secondary place in land management. This dynamic in fact follows a process of absorption of customary rules by modern law.

[57] Ibid. "Indeed, before the adoption of the law on rural land of 1998 and as we mentioned in the first report, customary rules have for a long-time governed land management in the forest zone in Côte d'Ivoire as everywhere else across the country. Even the colonial decree of 1935 did not change this as Indigenous peoples sold their lands to foreigners and nationals on the basis of customary rules in exchange for a symbolic purchase price. This is why customary law was for a long time and continues to be qualified as "living law" unlike modern law."

that soliciting the help of judges with whom they have some familial, ethnic, or inter-ethnic connection is corruption.

They see it as an extension of customary attitudes that should be preserved one way or another. The pervasive nature of these practices and beliefs is such that whenever a legal matter arises anywhere in Cote d'Ivoire, the reflex is to ask or look for potential family or ethnic allies to resolve it: looking for and hiring an Attorney to deal with the matter is the least of their concerns, unlike in the West where it is the opposite.

The Ivorian social fabric is ingrained by the culture of finding a "helping hand" within the system. This state of affairs does not spare the world of cybercrimes in Cote d'Ivoire. The actors are the same and the attitudes remain stubbornly "alive" when it comes to the fair delivery of the rule of law.

Most cybercriminals in Cote d'Ivoire are young people who are educated and can be found in all ethnic groups. The transnational nature of cybercrimes does not elicit the activation of ethnic networks when the justice system must punish the authors of cybercrimes. The same mechanisms of inter-ethnic alliances play a huge role in the enforcement of the laws about cybercrimes, notwithstanding the enactment of a multitude of laws against cybercrimes.

Another aspect of the cultural determinant as an obstacle to the rule of law in Cote d'Ivoire is the fact that, depending on whether you live in urban areas or in rural areas, the application of the law is quite different as Granger[58] argued in his report with regard to third world countries in general.

[58] Granger Roger. Tradition as a limit to legal reforms.*(Supra note 49)P*.23. "The rights of persons of all Third World countries recognizes equality between people. An individual cannot, as a human being, be legally unequal to another. Old and strong traditions of inequalities between people, with a religious and sociological basis, remain, despite the

Although, there is officially no caste system in Cote d'Ivoire, the reality is that not everyone is allowed to marry anyone they love. Within families, young men and women are sometimes advised not to marry someone from X ethnic group for a myriad of mundane reasons.

Secondly, most people living in poor rural areas are either too poor or illiterate or a combination of the two, to go before a judge when a dispute arises whereas in urban areas, the rate of use of the justice system, notwithstanding the corruption involved, is much higher in comparison to the rural areas./.

Recommendations

The single most powerful recommendation we can think of would be for the Ivorian government to reaffirm the pre-eminence of the Civil Code over customary laws, and to declare a war on corruption because these traditional ways of dealing with the justice system are without an ounce of doubt, a form of corruption tolerated and seen as a vector of social peace.

In fact, it is dangerous for the peace if at some point, some social groups feel like they do not benefit from the system because they do not have enough representations in the levels of power.

solemn proclamation of the principle of equality. A first example is found in the maintenance of the caste regime. India is always referred to because it is the country where the caste system has been most institutionalized. But the system is found in other states. In Madagascar marriage to a person of a caste lower is socially prohibited, while the Civil Code decrees the most complete freedom in the choice of spouse. In India, the caste regime was officially abolished in 1949. Anyone who stays in India for a short time immediately realizes that the caste has not disappeared."

2-2-3: Economic Determinant inhibiting the Rule of Law.

Access to the court must be easy for litigants ... This is a condition of good justice[59].

The single most important obstacle to the rule of law in African countries, has to do with severe poverty among the populations, notwithstanding the clout that customary law and inter-ethnic alliances exert on the national psyche.

On the paper, most African nations are parties to the United Nations charter on the Universal Declaration on Human Rights of December 10th, 1948 (Art. 8)[60] and the International Covenant on civil and political rights of December 16th, 1966 (Art. 2-3)[61]. Cote d'Ivoire is party to these international declarations on top of prescribing the free access to justice to its citizens in the national constitution of 2016 (Art. 6)[62].

[59]Degni-Segui, R. (1995). Access to justice and its obstacles. *Law and Politics in Africa, Asia, and Latin America, 28*(4), 449-467. Retrieved March 4, 2021, from http://www.jstor.org/stable/43110616.

[60]United Nations. (1948, December). *The Universal Declaration of Human Rights*. un.org. https://www.un.org/en/universal-declaration-human-rights/ (Accessed on 03/03/2021). Art. 8: "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law".

[61]United Nations Human Rights. (1966, December). *International Covenant on Civil and Political Rights*. ohchr.org. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed on 03/03/2021). Art.2: "1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its authority the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status. 2. Where not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant. 3. Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; (c) To ensure that the competent authorities shall enforce such remedies when granted". Art.3: "The States Parties to the present Covenant undertake to ensure the equal right of men and women to the enjoyment of all civil and political rights set forth in the present Covenant".

[62] Cote d'Ivoire Constitution, Art. 6: "The right of everyone to free and equal access to justice is protected and guaranteed. Everyone has the right to a fair trial and to judgment rendered within a reasonable period as determined by law. The State promotes the development of local justice."

The issue is that Cote d'Ivoire is a poor country whose GDP per capita was $2.290 with a life expectancy at 57 years. The poverty headcount ratio which is the percentage of the population living below the national poverty lines is 44.4[63]. The literacy rate of Cote d'Ivoire according to the United Nations Educational, Scientific and Cultural Organization (UNESCO)[64] is 47.17% for all adults with the male literacy standing at 53.66% while the female rate is 40.5% showing a big gap between the sexes.

Cote d'Ivoire has de facto, one of the highest illiteracy rates in West-Africa due in part to the extreme poverty of the population and the lack of substantial investments in girl's education by the government. These economic, literacy and financial issues have a negative impact on the rule of law for many reasons.

It is obvious that a litigant who is illiterate, poor, and living anywhere in the country, not just in rural areas, will not dare to take his case to court for fear of being unable to pay the fees, securing counsel etc…

In fact, the complexity of the justice system is such that even being well educated is no guarantee of access because many factors are at play like knowing and understanding your rights as a citizen or being able to secure a quick judgement on your case and many more.

The economic inhibitor to the rule of law in Cote d'Ivoire also impacts the justice system itself for there are few judges and they lack funding[65] with an uneven presence in the different regions of the country.

---

[63] *Cote d'Ivoire Data*. (2020). The World Bank. https://data.worldbank.org/country/cote-divoire

[64]UNESCO Institute for Statistics. (2020). *Côte d'Ivoire | UNESCO UIS*. Sustainable Development Goals. http://uis.unesco.org/en/country/ci (Accessed on 03/03/2021).

[65]USAID. (2020). *Increasing Access to Justice*. U.S. Agency for International Development. https://www.usaid.gov/cote-divoire/fact-sheets/increasing-access-justice (Accessed on 03/03/2021). The USAID launched a project called Projustice: "Côte d'Ivoire has well-qualified lawyers and judges, but the justice system has

Another reason based on ignorance which derives from a lack of education is the fact that some people equate the justice system to prison; in other words, they prefer the traditional way of resolving disputes than going through the justice system where they think the probability of going to jail is extremely high.

Once again, the economic factor is at play because… well learning your rights costs money. This not to say Ivorians avoid the justice system altogether like the plague, but to expose the reality of a justice system unaffordable for the average Ivorian citizen.

That is why we encourage a number of reforms; some already being implemented thanks to the friendship of countries such as the United States through the US Agency for International Development (USAID)[66]. Other international institutions like the world bank, also intervene to make it easier for Ivorians to access the justice system.

Recommendations

In terms of recommendations, we would encourage the Ivorian government to invest more in the hiring and training of judges. The national constitution having recognized "the right of everyone to free and equal access to justice," there should not be an uneven presence of courts around the country.

become polarized and politicized. Magistrates lack motivation and adequate funding, clerks lack accountability, and rulings come slowly and lack uniformity. The cost of accessing the system has traditionally been inflated due to the fee scale and the ubiquity of "middlemen" who interpret legal procedures for uneducated populations. Procedures are cumbersome and lack transparency while justice sector staff have inadequate working conditions and security concerns. The United States and Ivoirian governments both see judicial reform as central to the reconstruction and reconciliation process. This necessary support of the judicial sector is implemented by Tetratech with a five-year, $19 million project called **Projustice**. The goal of this project is to make the justice sector more effective, accessible, and equitable through a robust training program targeting key actors in the justice sector, equipment supports and infrastructure rehabilitation."

[66]USAID. (2020). *Increasing Access to Justice (supra note 65)P.33*.

An effort should also be done through non-governmental organizations to educate the population about its basic rights and obligations because in the end, the complexity of the justice system, compounded with the fact that a substantial number of people are illiterate and or poor make it impossible for the average citizen to know their basic rights.

The United Nations Office on Drugs and Crime (UNODC)[67] in collaboration with the UNICEF has put in place a manual to give legal assistance to children which could be extended to the population at large. Cote d'Ivoire could benefit from it through a large campaign around the country./.

[67] Child-friendly legal aid in Africa. (2011). https://www.unodc.org/documents/justice-and-prison-reform/Child_Friendly_Legal_Aid_in_Africa.UNICEF.UNDP.UNODC.fr.pdf (Accessed on 03/12/2021).

2-2-4: Political Determinant inhibiting the Rule of Law.

The political aspect as an obstacle to a fair and vigorous rule of law is undeniably the most widespread, powerful and the top of all determinants inhibiting the rule of law in Cote d'Ivoire and in the rest of Africa for that matter. Those who control the levers of power in most third-world countries like Cote d'Ivoire dictate the terms of the game as far as the rule of law is concerned.

Most human rights organizations in the country have been denouncing the inefficiencies and the corrupt character of the justice system in Cote d'Ivoire. The 2019 Human Rights report by the United States Embassy[68] in Cote d'Ivoire details the various abuses in the judicial system. The political pressure compounded by the general atmosphere of corruption gangrening the judicial system make it extremely difficult if not impossible to achieve the fundamental goal of building a rule-based society in Cote d'Ivoire.

[68] Cote d'Ivoire 2019 Human Rights Report. (2019). US Embassy. https://ci.usembassy.gov/wp-content/uploads/sites/29/COTE-DIVOIRE-2019-HUMAN-RIGHTS-REPORT.pdf (Accessed on 03/11/2021). The Report states among other: "d. Arbitrary Arrest or Detention**:** The constitution and law prohibit arbitrary arrest and detention, but both occurred. The DST and other authorities arbitrarily arrested and detained persons, often without charge. They held many of these detainees briefly before releasing them or transferring them to prisons and other detention centers, but they detained others for lengthy periods. The limit of 48 hours pretrial detention by police was not enforced. Although detainees have the right to challenge in court the lawfulness of their detention and to obtain release if found to have been unlawfully detained, this rarely occurred. Most detainees were unaware of this right and had limited access to public defenders. Arrest Procedures and Treatment of Detainees: In December 2018, the government introduced a new penal procedural code, which contains, among other things, the state's right to detain a suspect for up to 48 hours without charge, subject to renewal by an appeals court magistrate. An investigating magistrate can request pretrial detention for up to four months at a time by submitting a written justification to the national prosecutor. First-time offenders charged with minor offenses may be held for a maximum of five days after their initial hearing before the investigative magistrate. Repeat misdemeanor offenders and those accused of felonies may be held for six and 18 months, respectively. Police often arrested individuals and held them without charge beyond the legal limit. While the law provides for informing detainees promptly of the charges against them, this did not always occur, especially in cases concerning state security or involving the DST. A bail system exists but was used solely at the discretion of the trial judge. Authorities allowed detainees to have access to lawyers, but in cases involving national security, authorities did not allow access to lawyers and family members. For other serious crimes, the government provided lawyers to those who could not afford them, but offenders charged with less serious offenses often had no lawyer. Attorneys often refused to accept indigent client cases they were asked to take because they had difficulty being reimbursed by the government as prescribed by law. Observers reported multiple instances in which detainees were transferred to detention facilities COTE D'IVOIRE 6 Country Reports on Human Rights Practices for 2019 United States Department of State Bureau of Democracy, Human Rights and Labor outside their presiding judge's authority, in violation of the law. The vast majority of the country's attorneys reside in Abidjan; detained persons outside the city had particular difficulty obtaining legal representation."

The Report[69] corroborates this sad reality when it states that: "There were also numerous reports of judicial corruption, as bribery or intimidation-influenced rulings. In January two unions of magistrates denounced "threats, intimidation, and interference" by the country's executive and legislative bodies, urging the government "to enforce the principle of separation of powers enshrined in the Ivoirian constitution."

Unfortunately, when elected officials in government exert pressure on judges and magistrates in order to obtain rulings that favour their personal interests to the detriment of the country as a whole, everyone else is left to fend for themselves.

Rightly or wrongly, ordinary people do not see the need to obey the law or follow the normal procedures due to the fact that in their mind, everyone is gaming the system. It becomes obvious that in order to win the war against the proliferation of cybercrimes in Cote d'Ivoire, one cannot rely on the justice system as it is functioning at the moment, notwithstanding the enactment of strong anti-cybercrimes law by the state.

There is even the risk that the fight against cybercrimes due to its transnational nature and the need for developed nations to help poor ones, will be diverted from its original aim to become a big business for those in government leading the so-called war on cybercrimes. If that scenario is to come to life, developed countries will be twice defrauded: first, by the actions of cybercriminals in the country, and second, by representatives of the government in charge of fighting the war on cybercrimes.

The most famous cybercriminal in Abidjan, Raimi Abdoulaye, A.K.A "Commissaire 5500", was arrested in 2016 and let go, officially for "lack of proof" by the authorities. He is the one who once

[69] Cote d'Ivoire 2019 Human Rights Report. (2019). US Embassy *(Supra note 68)P*.36.

said that if pulled over by a police officer, he would give 2.000.000 CFA (= $4000) to the officer whose salary does not exceed $ 400 per month.

There is no reason to believe that the corruption stops with the Police, it feeds an ecosystem of corrupt officers, judges, Attorneys, and elected officials.

Recommendations

Making recommendations for the Authorities to change their own behaviour is challenging at best, and mission impossible at worst. That being said, it is always a clever idea to make those recommendations hoping that some among them will take and apply them seriously.

Some of the recommendations that come to mind are linked to the understaffing and under skilled personnel at the Ministry of Justice. There needs to be a more vigorous hiring of skilled Lawyers to work for the Ministry of Justice.

Their salaries should be tripled from what it is now to entice them to dedicate their time and effort for the triumph of the rule of law in Cote d'Ivoire. The Justice Ministry should be effectively independent from the Executive and the Legislative bodies, notwithstanding, the fact that it is part of the Executive.

The Report[70] previously cited, argued that "inadequate staffing in the judicial ministry, judicial inefficiency, and lack of training contributed to lengthy pretrial detention." This shows a structural deficiency within the Ivorian justice system. Advocating urgent reforms is the best recommendations one can give to the Ivorian government.

[70] Cote d'Ivoire 2019 Human Rights Report. (2019). US Embassy *(Supra note 68)P*.36.

It is fundamental that allegations of abuse of power by any branch of the government should be thoroughly investigated and those found guilty be sentenced to a time in state prison. It is the best signal the Ivorian government could send to the country as a whole that whoever violates the law irrespective of their social status, will feel the weight of justice.

Once ordinary folks start seeing “powerful” people who violate the law being hailed into court and sentenced when found guilty, increased people will avoid the route of undue influence over the actors of the justice system.

CHAPTER 2: Emergence of Cybercrimes in Cote d'Ivoire

The republic of Cote d'Ivoire is located in West-Africa between Liberia to the West, Mali and Burkina-Faso to the North, Guinee to the North-West, Ghana to the East and the Atlantic Ocean to the South. Cote d'Ivoire became a French colony[71] in 1893. Cote d'Ivoire gained its independence from France on August 7th, 1960. The official language is French while there are dozens of local dialects spoken by the natives.

After independence and under the leadership of its first President and the father of the nation, Felix Houphouet Boigny, Cote d'Ivoire enjoyed a rapid economic development. President Houphouet Boigny who was himself a farmer, encouraged the Ivorian people to invest in agriculture. The country became within a few years, a net exporter of agricultural crops, mainly cocoa and coffee beans around the world.

The country was also self-sufficient in food production and consumption. The immediate effect of this rapid development in a stable country was to attract millions of migrants from West-Africa and beyond. Development experts impressed by the Ivorian model of development based on agriculture, dubbed it "The Ivorian miracle". As the saying goes, 'you don't change a winning team or a winning method'.

Few Ivorians dared to contest Houphouet Boigny's hold on the country through the only political party legally allowed in the land.

Unfortunately, the decline in commodity prices (cocoa, coffee) on the international markets earlier in the 80s, plunged Cote d'Ivoire into a recession from which the country never fully recovered.

[71] https://en.wikipedia.org/wiki/Ivory_Coast (Accessed on 01/14/2020)

The domino effect of this situation coupled with the fact that the first President became too old to govern, led to a political upheaval in the 90s that will change the face of Code d'Ivoire forever.

The unthinkable happened at the end of the 90s through first, a coup d'état, followed by two civil wars.

3-1: Historical background

There is scant evidence of earlier human activity in the Neolithic period in the area we now call Cote d'Ivoire. As Boddy-Evans, Alistair argued in an article, a more thorough investigation is needed[72]. The now known country of Cote d'Ivoire was part of the West-African trade route used by Europeans in the 15th century.

The French and the Portuguese respectively named the land, the "Cote d'Ivoire" and "Costa Do Marfim*",* both literally meaning "The Coast of Ivory"[73]. Like other places named based on the type of natural resources found there, (Gold Coast = Ghana), the name "Ivory Coast" reflected the major trade that occurred on that coast: the export of ivory.

The French who at first were not that much interested in the land due to the difficulties of access to the hinterland, abandoned the place toward the end of the 18th century, only to come back in the mid-nineteenth century.

[72] Boddy-Evans, Alistair. "A Very Short History of Côte D'Ivoire." ThoughtCo, Feb. 11, 2020, www.thoughtco.com/very-short-history-of-cote-divoire-43647. "Oral histories give rough indications of when various peoples first arrived, such as the Mandinka (Dyuola) people migrating from the Niger basin to the coast during the 1300s. In the early 1600s, Portuguese explorers were the first Europeans to reach the coast. They initiated trade in gold, ivory, and pepper. The first French contact came in 1637—along with the first missionaries. In the 1750s the region was invaded by Akan peoples fleeing the Asante Empire (now Ghana). They established the Baoulé kingdom around the town of Sakassou."

[73] https://en.wikipedia.org/wiki/Ivory_Coast (Accessed on 01/17/2020). "There was also Pepper Coast, also known as the "Grain Coast" (present-day Liberia), a "Gold Coast" (Ghana), and a "Slave Coast" (Togo, Benin, and Nigeria).

In 1843–4, French Admiral Louis Edouard Bouet-Willaumez, signed treaties with the kings of Grand-Bassam and Assinie regions, making their territories a French protectorate[74]. In 1893, Cote d'Ivoire became officially a French colony after Britain recognized French sovereignty in the area in 1889. Nevertheless, one will have to wait until 1915 for the French to complete the total pacification of the territory due to clusters of revolt throughout the colony.

From 1890 until 1915, starting with Samory Touré who was fighting to create an empire, to the Abron and later the Baoulé, the French military had to face many although unsuccessful revolts from the local populations.[75] Once the pacification of the country done, the colonial Administration launched large infrastructure projects to facilitate the export of raw materials to France.

To do this, they ordered all Ivorians males to work for free ten days each year known as the "head tax". Obviously, the locals were not pleased with the Authorities who took such decision, thus forcing the colonial administration to "import" manpower from the upper volta.

Cote d'Ivoire became part of the Federation of French West-Africa[76], known by its French acronym "AOF". Its counterpart in central Africa was known (literally) as French Equatorial Africa or "AEF". Within the Federation of French West-Africa, Cote d'Ivoire was the richest colony even though the federation was headquartered in Dakar, Senegal.

---

[74] https://en.wikipedia.org/wiki/Ivory_Coast (Supra note 71)P.41. "French explorers, missionaries, trading companies, and soldiers gradually extended the area under French control inland from the lagoon region."

[75] Source: US Library of Congress. http://countrystudies.us/ivory-coast/3.htm (Accessed on 1/29/2020) "Over the next twenty years, French administrators used the military to subdue African populations that, with few exceptions, openly resisted French intrusions. In the 1890s, Samori Touré, seeking to construct a kingdom across much of the Sahel, including northern Côte d'Ivoire, withstood French (and British) forces until he was captured in 1898. At about the same time in eastern Côte d'Ivoire, the Agni (Anyi) and Abron peoples first resisted the French and, after military setbacks, either sabotaged or circumvented the colonial administration. In the early twentieth century, the Baoulé of central Côte d'Ivoire openly defied colonial authorities until forcibly subdued in a bloody, so-called pacification campaign undertaken in 1906 by Governor Gabriel Angoulvant."

[76] https://en.wikipedia.org/wiki/Ivory_Coast (Supra note 71)P.41.From 1904 to 1958, Ivory Coast was part of the Federation of French West Africa. It was a colony and an overseas territory under the Third Republic. In World War I, France organized regiments from Ivory Coast to fight in France, and colony resources were rationed from 1917–1919.".

This dominant position of Cote d'Ivoire in terms of resources will be reflected during the two world wars when Cote d'Ivoire supplied more than 150.000 men[77] during World War 1 and countless natural and agricultural resources for the war's effort in 1914-18 and 1939-45.

After the second World War, and to show gratitude to Africans who sacrificed blood and material resources during the war, France, starting in 1944, allowed its "subjects" to organize politically. In Cote d'Ivoire, Houphouet-Boigny, rich farmer, and a doctor, created the "Syndicat Agricole Africain" known by its French acronym "SAA" to fight for a fair pricing system for raw materials such as cocoa and coffee.

Houphouet Boigny also spearheaded the creation of the "Rassemblement Democratique Africain" or "RDA" on which he will later build a political party known to this day as the "PDCI-RDA" or "Democratic Party of Cote d'Ivoire" member of the "RDA". He became de facto, the leader of Cote d'Ivoire with whom the French worked regarding Ivorian matters. Houphouet-Boigny will go on to serve in the French government five times and even became the Prime Minister of France for…a few hours.

Exhausted financially and politically by the Second World War but also under pressure from African newly trained elites and Washington, notwithstanding the creation of the French Union in 1958, France but also the United Kingdom handed over the colonies to their rightful owners at the

[77] https://en.wikipedia.org/wiki/Ivory_Coast (Supra note 71)P.41. "France organized regiments from Ivory Coast to fight in France, and colony resources were rationed from 1917–1919. Some 150,000 men from Côte d'Ivoire died in World War I. Until the period following World War II, governmental affairs in French West Africa were administered from Paris. France's policy in West Africa was reflected in its philosophy of "association", meaning that all Africans in Côte d'Ivoire were officially French "subjects", but without rights to representation in Africa or France."

end of the 50s. On August 7th, 1960, Cote d'Ivoire[78] became officially an independent country and Houphouet-Boigny was elected its first President.

Cote d'Ivoire has been a land of immigration before its independence, due in part to the colonial government undertakings and the size of the Ivorian population. In 1900, France imposed a head tax to finance a public works program that was labor-intensive.

To reach its goals, *France*[79] imposed a system of forced labor under which each Ivorian male adult was required to work for ten (10) days each year without compensation as part of his obligation to the colonial state. Due to the small size of the Ivorian population, the French recruited large numbers of workers from Upper Volta (actual Burkina-Faso) to work in Cote d'Ivoire.

This source of labor was so important to the economic life of Cote d'Ivoire that in 1932 the colonial body known by its French acronym AOF or (Afrique Occidentale Francaise) annexed a large part of Upper Volta to Cote d'Ivoire and administered it as a single colony.

[78] https://en.wikipedia.org/wiki/Ivory_Coast (Supra note 71)P.41. "At independence (1960), the country was easily French West Africa's most prosperous, contributing over 40% of the region's total exports. When Houphouet-Boigny became the first president, his government gave farmers good prices for their products to further stimulate production, which was further boosted by a significant immigration of workers from surrounding countries. Coffee production increased significantly, catapulting Côte d'Ivoire into third place in world output, behind Brazil and Colombia. By 1979, the country was the world's leading producer of cocoa. It also became Africa's leading exporter of pineapples and Palm oil. French technicians contributed to the "Ivoirian miracle". In other African nations, the people drove out the Europeans following independence, but in Côte d'Ivoire, they poured in. The French community grew from only 30,000 prior to independence to 60,000 in 1980, most of them teachers, managers, and advisors. For 20 years, the economy maintained an annual growth rate of 10%—the highest of Africa's non-oil-exporting countries".

[79] https://en.wikipedia.org/wiki/History_of_Ivory_Coast (Accessed on 02/07/2020) "France's imposition of a head tax in 1900, aimed at enabling the colony to undertake a public works program, provoked a number of revolts. The public works programs undertaken by the Ivorian colonial government and the exploitation of natural resources required massive commitments of Labor. The French therefore imposed a system of forced labor under which each male adult Ivorian was required to work for ten days each year without compensation as part of his obligation to the state. The system was subject to extreme misuse and was the most hated aspect of French colonial rule. Because the population of Côte d'Ivoire was insufficient to meet the Labor demand on French held plantations and forests, which were among the greatest users of Labor in French West Africa, the French recruited large numbers of workers from Upper Volta to work in Côte d'Ivoire. This source of Labor was so important to the economic life of Ivory Coast that in 1932 the AOF annexed a large part of Upper Volta to Ivory Coast and administered it as a single colony. Many Ivorians viewed the tax as a violation of the terms of the protectorate treaties because France was now demanding the equivalent of a *coutume* from the local kings rather than the reverse. Much of the population, especially in the interior, also considered the tax a humiliating symbol of submission."

Cote d'Ivoire kept welcoming a cheap manpower from Burkina-Faso even after the country became independent. Besides Burkina-Faso, several West-African countries were a source of migration to Cote d'Ivoire (Mali, Guinee, Nigeria, Ghana, Togo, and Benin).

The Ivorian "melting pot" was even more pronounced with the arrival of migrants from Central Africa and from the Middle East, mainly Lebanon. The co-existence between these immigrants and the local population was for the most part harmonious and peaceful which, coupled with the political stability of the country led by its founding father, Houphouet-Boigny, made Cote d'Ivoire a haven of peace and prosperity during the first three decades of its independence.

The political stability of Cote d'Ivoire allowed it to make important inroads in terms of economic development in comparison to other African countries.

In turn, international institutions of financing like the World Bank and the International Monetary Fund or IMF loaned the country the funds it needed to build the public infrastructure.

Cote d'Ivoire became heavily indebted at the end of the 80s compounded by the fall of prices of raw materials like cocoa and coffee. To turn things around, the World Bank and the International Monetary Fund- IMF- "imposed" to the country, what was then dubbed "structural adjustment plans" in 1986.

To top these economic measures decided outside of Africa, a pressure was put on the Ivorian government notably President Houphouet Boigny who was old, to name a Prime Minister who would oversee the government. President Houphouet at first balked at the idea of sharing his power with a Prime Minister before ceding under pressure from the Breton woods Institutions.

In 1989, Mr. Alassane Dramane Ouattara was chosen by President Houphouet to lead a ministerial committee to tackle the economic crisis of Cote d'Ivoire.

The only problem with the nomination of Mr. Alassane Ouattara was that very few Ivorians knew him before his nomination. Rumors quickly swirled around the country that he was not a native Ivorian but a national of Burkina-Faso.

Some people became hostile to the important community of people from Burkina-Faso, some of whom have been in the country for generations going back to the colonial era.

As we will see later, this situation will provoke two civil wars in a country that was known for its legendary stability. Two decades after peacefully acceding to independence, characterized by an economic growth dubbed the "Ivorian miracle", Cote d'Ivoire went through an economic recession at the start of the 80s preceded by two decades of growth thanks to the export of raw materials like cocoa and coffee.

As Jean-Claude Berthelemy and Francois Bourguignon[80] (1996) noted, throughout the 1960s and 1970s the gross domestic product (GDP) of Cote d'Ivoire increased at an average annual rate of about 7.5 percent, which was close to the record of the top-performing developing countries. The combination of a cheap labor from surrounding countries and a fertile soil in the South and Western part of the country allowed Cote d'Ivoire to quickly catch and outperform its rival Ghana.

Another reason for the rapid agricultural development of Cote d'Ivoire can be attributed to the fact that the father of the country, Felix Houphouet Boigny was himself a farmer well before becoming a national leader during colonial times.

[80] J.C Berthelemy, F. Bourguignon. "Growth and Crisis in Cote d'Ivoire." May 1996. World Bank. Comparative Macroeconomic Studies.

However, as pointed out by Robert Handloff[81], the worldwide economic recession at the beginning of the 1980s caused the prices of cocoa and coffee, Côte d'Ivoire's principal exports, to drop sharply, resulting in a significant economic slowdown.

The economic crisis that started at the beginning of the 80s continued through the mid-90s which made Jean-Claude Berthelemy and Francois Bourguignon[82] ask if instead of an economic "cycle", Cote d'Ivoire was not entering a downturn that would persist in the long run.

Ironically, the year of publication of their work, 1996, was the beginning of a new economic growth under the second President of Cote d'Ivoire, Henri Konan Bedie that abruptly ended at the end of the year 1999 through the first military coup in the history of Cote d'Ivoire. The economic crises of the 80s and 90s were the precursors to the xenophobic atmosphere of the 90s that led to two civil wars in the first decade of the 21st century breaking the consensus held by outside observers that Cote d'Ivoire was different from the rest of Africa in the words of Robert Handloff[83].

[81] Robert E. Handloff, ed. *Côte d'Ivoire: A Country Study*. Washington: GPO for the Library of Congress, 1988. http://countrystudies.us/ivory-coast/3.htm "Meanwhile, foreign borrowing to finance massive investments in infrastructure and public enterprises (that lost money) raised Côte d'Ivoire's foreign debt beyond its ability to meet its obligations. Budget reductions and a structural adjustment program forced much of the population to lower its expectations, which in turn contributed to, among other social ills, heightened frustrations, and a sharp increase in violent crime. By the end of the 1980s, Côte d'Ivoire was confronting the same problems of political and economic development as other African countries and having to respond with many of the same difficult and often inadequate solutions."

[82] Berthelemy, Bourguignon. "Growth and Crisis in Cote d'Ivoire." (Supra note 80) P.47.", Cote d'lvoire is not unique in this reversal of fortune. Many countries have experienced a succession of favourable and adverse events in their development yet have been able to grow at a satisfactory average rate eventually. What makes the case of C6te d'lvoire unusual is the magnitude and the length of the present "'cycle," if it is indeed a cycle and not a downturn that will continue into the long run. Furthermore, since there has been little institutional or policy change over the past thirty years, the present sustained recession can only be seen as the result of new and lasting constraints from abroad and the incapacity of C6te d'lvoire's institutions to cope with these forces".

[83]Handloff, ed. *Côte d'Ivoire: A Country Study*. (Supra note 81) P.48. "Observers of Africa have often characterized Côte d'Ivoire as different from the rest of Africa. Borrowing the metaphor of Félix Houphouet-Boigny, president of Côte d'Ivoire, they have described it as an oasis of political stability and economic prosperity--in short, the "Ivoirian miracle." Indeed, if judged on the basis of political stability and economic performance during its first twenty years of independence, Côte d'Ivoire does appear unique: it has had only one president and no coups since gaining independence, and between 1960 and 1979 the gross national product (GNP) grew by almost 8 percent per year, compared with minimal or negative growth rates elsewhere in Africa."

No Ivorian personifies more the “civil war decade” of the 21st century in Cote d’Ivoire than the current President of Cote d’Ivoire, Alhassane Dramane Ouattara, a.k.a A.D.O for his diehard partisans who are mostly from the northern Muslim part of Cote d’Ivoire and Immigrants from West-Africa and beyond.

Mr. Ouattara’s international connections are deep and varied thanks to his career at the International Monetary Fund (IMF) in Washington. Cote d’Ivoire during the first 30+ years of its independence, was a haven of peace, stability, and prosperity by African standards.

Then after the passing of its founding father, Felix Houphouet Boigny in 1993, political instability took hold with the heirs apparent to the “throne” squabbling for power. These heirs apparent were Henry Konan Bedie who was President of the National Assembly at the death of President Houphouet Boigny and the designated successor by article 11 of the constitution of Cote d’Ivoire.

However, the arrival of Mr. Alhassane Ouattara from the International Monetary Fund (IMF) where he was an economist, to take on the recession Cote d’Ivoire was going through in the 90s created a de facto rivalry between him and the designated successor, Mr. Bedie. The Parti Democratique de Cote d’Ivoire (Democratic Party of Cote d’Ivoire) (PDCI) at the helm of the country since independence was then divided between supporters of Mr. Bedie and Mr. Ouattara, both groups jockeying for power.

In the first act of their confrontation, Mr. Bedie prevailed by acceding to power through the Constitution in 1993.

Mr. Ouattara, far from renouncing his ultimate ambition to lead Cote d’Ivoire, made a tactical retreat to Washington D.C at the IMF with the help of his international connections. One year later,

supporters of Mr. Ouattara inside the PDCI left the party to found a new one called the Rally of the Republicans (Rassemblement des Republicains) or RDR.

The following year, during the presidential elections of 1995, the RDR and the other opposition party, the Front Populaire Ivoirien (Ivorian Popular Front) or FPI decided to boycott the election due to the refusal of the Ivorian authorities to allow the candidacy of Mr. Ouattara who was still living and working in Washington.

In the end, President Bedie was the sole serious candidate who as expected, won the controversial elections. The seeds of a permanent instability in the public discourse were sowed and what was to happen usually in Africa, happened.

In December of 1999, President Bedie was victim of a military coup, the first in the history of Cote d'Ivoire. The Ivorian miracle expressed for 3 decades in stability and prosperity was gone. The chaos that followed this "coup d'état" will lead the country of Houphouet Boigny to go through two (2) civil wars in less than a decade.

Following the first "Coup d'état" in December 1999 led by the army chief of staff, Robert Guei and under pressure from the "international community", a presidential election was held in October 2000.

Once again, Mr. Ouattara was excluded from running by the Constitutional Court, which validated the candidacy of the leader of the junta, Robert Guei, and the historic opponent Laurent Gbagbo.

Unfortunately for Robert Guei, Gbagbo Laurent prevailed at the polls, but it took street demonstrations to force the junta leader to relinquish power.

To make matters worse, supporters of Mr. Ouattara saw the humiliating departure of Robert Guei as an opportunity to hold new elections and therefore, took to the streets to demonstrate. That did not go well with the newly elected President and his supporters.

Chaos ensued and the security forces with the backing of the President-elect went hard at the protesters which occasioned dozens of fatalities in their ranks. A few months into the presidency of Mr. Gbagbo, an attempted coup by soldiers loyal to Mr. Ouattara was foiled by the security forces and on September 19th, 2002, a new attempted coup was partially foiled in Abidjan but not in the northern half of the country.

Cote d'Ivoire became at this point a divided country with the wealthy south under the control of the Ivorian national armed forces and the North of the country under rebel forces loyal to Mr. Ouattara.

In 2005 and after multiple regional mediations, a unity government was formed led by the rebel leader Soro Guillaume. A relative calm reigned until the end of 2010 when a new presidential election was set to take place. It will unfortunately lead to the second Civil War the country has known. For years, the Gbagbo administration had refused to organize any elections if half of the country was occupied by rebel forces.

In fact, the Ivorian Constitution forbids such polls if the integrity of the Ivorian territory is threatened. However, under intense pressures from the so-called "International Community" to hold elections despite the de facto division of the territory, President Gbagbo acceded to their demands.

The chaotic polls especially in the northern part of the country where Mr. Ouattara's forces dominated led to voters suspected of being in favor of President Gbagbo being brutalized and killed by the forces of Mr. Ouattara.

There were widespread frauds in the North and what was to be expected, happened. For four days, the Electoral Commission was unable to declare a winner at the polls, instead hiding behind an untenable silence.

In the end, the President of the Electoral Commission was allegedly taken by foreign diplomats to the Golf Hotel[84], where Mr. Ouattara and his men were headquartered, protected by French and United Nations forces. Before journalists from the Associated Press (AP) and the Agence France Presse (AFP), he declared Mr. Ouattara the winner of the election.

The breaking news heard around the world before being known to Ivorian Authorities and the Ivorian people led to a stalemate with President Gbagbo refusing to recognize the solo and suspicious declaration of the President of the Electoral Commission in a private setting surrounded by forces and people favorable to Mr. Ouattara.

The rest is history: thousands of civilians died in the ensuing confrontation between rebel forces loyal to Mr. Ouattara, backed by the United Nations forces and French troops, and the Ivorian national army.

[84] Laurent Bigot. as cited in "Ivory Coast: in fact, who won the presidential election of 2010?". Le Monde Afrique. May 27th, 2016. https://www.lemonde.fr/afrique/article/2016/05/27/cote-d-ivoire-mais-qui-a-gagne-la-presidentielle-de-2010_4927642_3212.html (Accessed on 06/23/2020). The announcement is made at the Hôtel du golf, the HQ of Alassane Ouattara, the UN mission in Côte d'Ivoire (Onuci), having refused to allow this to take place at her home. Alassane Ouattara is declared the winner with a lead of 376,000 votes.

President Gbagbo who took refuge in the presidential residence and bunker was ultimately taken alive by French forces and handed to Mr. Ouattara's forces.

Those two civil wars were the prelude to the explosion of cybercrimes in Cote d'Ivoire for a simple reason: most of the rebels and their leaders were involved in organized traffics of precious minerals, cocoa, coffee, and even human trafficking[85].

The result has been the flaunting of riches by former rebels all over the country, especially in the south where the commercial hub of Abidjan is located.

Young men who have not had the opportunity to get rich fast began searching for ways to get rich like the former rebels. The easiest route they found was to use the internet to scam people all over the world and especially Europe./.

[85] Voanews.com. Africa. "Rights Group Decry Trafficking of Nigerian Women in Ivory Coast". August 26,2010. https://www.voanews.com/africa/rights-group-decrys-trafficking-nigerian-women-ivory-coast "Civil war split Ivory Coast in half in 2002, and the country continues to struggle to hold long-delayed presidential elections that could bring an end to nearly a decade of political instability and internal conflict.
Wells said Ivory Coast provides fertile ground for impunity in human rights violations, like the trafficking of Nigerian women for sex work. "In fact, a lot of the severe human rights abuses going on in Cote d'Ivoire right now are taking a back seat to simply getting to elections, which I think is a major concern," said the researcher. "A lot of these things are getting thrown under the rug and the average Ivorian, or in this case, the Nigerians who are being trafficked in, are those that are suffering as result." Among its recommendations, Human Rights Watch has called on Nigerian and Ivorian authorities to investigate and prosecute traffickers taking women to Ivory Coast. HRW has also called on Nigerian authorities to educate Nigerian women about the existence and methods of these rings and offer assistance and protection to repatriated victims of trafficking. HRW says the Nigerian women are brought to Ivory Coast through countries like Benin, Togo, Ghana, and Burkina Faso. On a regional level, HRW is calling on the Economic Community of West African States to work with countries to protect women and girls from trafficking and bring perpetrators to justice."

3-2: The Regional Influence

When it comes to cybercrimes around the world, the west-African region is one of the first cited by experts in cybersecurity.

In fact, West-Africa is so ill-perceived when it comes to cybercrimes that an email originating from that part of the world is seen as suspicious even when emanating from legitimate sources. One must go back to the 70s to understand how this region easily became a hotbed of cybercrimes. The United Nations Office on Drugs and Crime (UNODC) pointed out in a *report*[86], that since the "oil shocks" of the 70s, the West-African region has been a staple of transnational crimes and must be regarded as an issue of growing concern.

The report cites illegal activities such as drug trafficking, advanced fee and Internet fraud, human trafficking, diamond smuggling, forgery, cigarette smuggling, illegal manufacture of firearms, trafficking in firearms, armed robbery and the theft and smuggling of oil.

Today, the region is being poised to become an underground market when it comes to cybercrimes. Many factors, among them the transnational movement of people and goods help spread the scourge of cybercrimes among west-African nations.

As early as 2012, *Ryan Flores et al*[87] predicted that we would see a cybercriminal underground market emerge from the region. Cybercrimes in the 80s used to be a one country-issue, Nigeria, but today it has spread to most of West-Africa. Known in the 80s as the "Nigerian letter", cybercrime is nowadays known as the "African letter".

[86] United Nations Office on Drugs and Crime. "Transnational Organized Crime in the West African Region." United Nations, New York. 2005.

[87] Ryan Flores, Bakuei Matsukawa et. al. *"Cybercrime in West-Africa: poised for an underground market."* Trend Micro, Interpol joint research paper. 2017. www.trendmicro.com , www.interpol.int .

A sizeable number of West-African nations harbor cyber criminals with Nigeria, Ghana and Cote d'Ivoire being the "tete de Pont" or bridgeheads of cybercrimes in West-Africa.

Our research has touched upon the historical background, the enumeration of traditional crimes to cybercrimes and the battery of legislations taken by member-states to fight cybercrimes in West-Africa.

To understand the easiness with which West-Africa became known as one of the underground markets in cybercrimes, one must understand how most African countries came to be in the 60s in terms of political, social, and economic governance.

Most West-African states to the exception of Liberia have been colonized by European powers, mainly France, Great-Britain, and Portugal. Liberia on the other hand was a creation of slave Abolitionists.

These West-African colonies gained independence in the second half of the twentieth century beginning with Ghana in 1957. The timing could not be better because as the United Nations Office on Drugs and Crime (UNODC) noted, the first decade of independence occurred at the height of the long economic boom—the longest and most widespread in history—that was transforming the world in the third quarter of the twentieth century.

One would think that with their newly gained political independence, these African states would easily ride the same wave of economic growth as the rest of the world, which could have solidified the political stability of the new nations.

Unfortunately, this was not the case as countries like Ghana, Nigeria, Niger, Mali, Sierra Leone, Togo, and Benin all went through a military coup within a few years of independence. The fact of the matter was that organized crime existed in some corners of West-Africa even before these colonies gained independence.

As *Stephen Ellis*[88] interviews with law enforcement officers in Abidjan showed, in Côte d'Ivoire, even before independence in 1960, there were Corsican gangs specializing in cigarette-smuggling as well as the recruitment of women for prostitution in France.

On top of the political chaos observed in some West-African countries right after gaining independence, some countries like Sierra-Leone overtly accused Nigeria of having spread the scourge of organized crime in their country.

The *report*[89] by UNODC alleged a Nigerian connection, by citing a Sierra Leonean police official, who connects the rise of organized crime in his country to the creation of the Economic Community of West African States (ECOWAS) in 1975, which facilitated movement between member States. In the French-speaking countries, Côte d'Ivoire offered a similar allure to Nigeria's in the Anglophone world.

According to *Alain Sissoko*[90], cited by the report, organized crime is regarded as having started in Côte d'Ivoire too in the 1970s, when the country attracted large numbers of immigrants in search of work. A problem of armed robbery emerged, as bands composed of immigrants were formed, later joined by Ivorians.

Moreover, he argued, wars in Liberia and Sierra Leone in the 90s, have facilitated the import of firearms by armed groups, including armed robbers, to Côte d'Ivoire. One thing most experts agree on is that organized crime began before the 70s in Nigeria.

One of those experts, *Etannibi E.O. Alemika*[91], noted that elements of organized crime may be identified before 1975 in the form of organized groups involved in falsifying imports to transfer

[88] Stephen Ellis interviews with law enforcement officers in Abidjan, 1997.
[89] Morie Lengor, as cited in "United Nations Transnational Organized Crime Assessment Form: Sierra Leone," April 2004.
[90] Alain Sissoko as cited in, "United Nations Transnational Organized Crime Assessment Form: Côte d'Ivoire," April 2004.
[91] Etannibi E.O. Alemika, as cited in "United Nations Transnational Organized Crime Assessment Form: Nigeria," April 2004.

funds outside the country, normally in contravention of currency regulations. He added that this process involved over-invoicing, or importing sub-standard goods for delivery to government departments, in return for kickbacks paid to government officials.

This practice was alluded to by the executors of the country's first coup in 1966.

This is an interesting observation in that, as will be analyzed in a subsequent section, it may be regarded as a pioneering form of the widespread frauds that were to become a trademark of West African criminal networks in later years. *Etannibi E.O. Alemika*[92] did not stop there as he pointed out that from the late 1980s, transnational advance-fee fraud became a public issue in Nigeria for the first time, apparently developing from the prior existence of corrupt dealings in foreign exchange and the transfer of stolen funds through foreign businesses and entrepreneurs.

Moreover, *Etannibi*[93] blamed the flourishing of organized crime in Nigeria to the introduction of a structural adjustment program in 1986, resulting in greater poverty and unemployment and a consequent increase in emigration.

Finally, the rapid and ill-prepared liberalization of the financial sector, including the establishment of poorly regulated finance businesses and banks, provided new opportunities for money laundering, fraud, and illegal foreign exchange transactions.

According to the *report*[94] by the United Nations Office on Drugs and Crime (UNODC), in Ghana too, organized crime appears to have emerged in the 1980s, connected to the problems and the opportunities offered by international migration.

Ghanaians, the report pointed out, were among the first West Africans in modern times to migrate widely, particularly with the onset of major economic problems in the 1970s, benefiting from the

[92] Etannibi E.O. Alemika, (Supra note 91)P.56.
[93] Ibid.
[94]Ibid.

country's generally high standard of education, the large number of people speaking good English, enabling them to compete in international labor markets, and a tradition of migration by young men especially in search of economic and social advancement.

The deportation of more than a million Ghanaians from Nigeria in 1982 and the tightening of the international labor market may have contributed according to the *report*[95] to young people turning in big numbers to organized crimes back home.

The existence of organized crime in the three major economies (Nigeria, Ghana, Cote d'Ivoire) of West-Africa well before independence in the case of Nigeria and Cote d'Ivoire, may help explain why the region is known today as a hotbed of Cybercrimes to the outside world. The other culprit might be the digitalization of daily activities in Africa.

After missing out on the agricultural and the industrial revolution of past centuries, the African continent like one man, has decided not to miss out on the digital revolution of the 21st century.

The term digitalization should not be confused with the term digitization. According to *Gartner's IT Glossary*[96], digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities, whereas digitization is the process of changing from analog to digital form.

Everywhere on the continent, governments and the private sector are teaming up to bring new technologies to the local populations. In West-Africa, according to the 2019 *GSMA Intelligence report*[97], by the end of 2018, there were 185 million unique subscribers, an increase of nearly 10 million over the previous year.

[95] Etannibi E.O. Alemika (Supra note 91) P.56.
[96] http://www.gartner.com/it-glossary/
[97] The Mobile Economy West-Africa 2019. www.gsmaintelligence.com/research .

Future growth will largely be driven by young consumers owning a mobile phone for the first-time and more than 40% of the sub-region's population are under 18 years old. A considerable proportion will become young adults over the next decade.

By 2025, the number of unique subscribers will reach 248 million, taking the subscriber penetration rate to 54%, compared to 48% at the end of 2018. These numbers show how important the connectivity in Africa is, although uneven from one place to the other.

The economic contribution of the mobile revolution in African economies is also substantial. The *report*[98] pointed out that in 2018, mobile technologies and services generated $52 billion of economic value (8.7% of GDP) in West-Africa-a figure that will reach almost $70 billion (9.5% of GDP) by 2023 as countries increasingly benefit from the improvements in productivity and efficiency brought about by increased take-up of mobile services.

Africa is also the global leader in mobile money, which has become an important component of Africa's financial services landscape. In an article published recently, *Mutsa Chironga et al* [99]noted that the Mobile Network Operators (MNOs) have dominated mobile money services in Africa for the past decade. All these trends show that the digitalization of the world economy is having a positive impact in Africa.

The continent does not just consume foreign-based models of development but is taking the lead to change the local culture and investors are taking notes. In 2016, African tech firms raised a record US$ 367 million according to media reports. Africa needs technology and people who

[98] The Mobile Economy West-Africa 2019.(Supra note).58. www.gsmaintelligence.com/research
[99] Mutsa Chironga, Hilary De Grandis, Yassir Zouaoui. *Mobile financial services in Africa: Winning the battle for the customer*. September 2017. Article. https://www.mckinsey.com/industries/financial-services/our-insights/mobile-financial-services-in-africa-winning-the-battle-for-the-customer (Accessed on 07/05/19).

deliver it. It needs food, and people who know how to grow it. Now the two are coming together, presenting a new down and a new culture firmly rooted in tradition, argued the Think-Tank.

Despite these positive changes in the African digital landscape, one must also grapple with the fact that this digitalization though in its infancy is being used to perpetrate cybercrimes. Some Africans use the internet to commit illegal activities like spamming, also known as the 'Advanced Fee Fraud'.

Spamming[100] was said to be one the most prevalent activities on the Nigerian Internet landscape accounting for the 18% of all online activities amongst others in 2008.

The use of digital means to perpetrate cybercrimes is not just a West-African issue, far from it: it is an worldwide issue. The "Nigerian Prince" who send you an email saying that he wants to share his 'wealth' with you may be a Nigerian national, but he may also be a South-African or a citizen of Ghana; in fact, he may even be a US citizen living in New Orleans and is white.

As the former Secretary-General of the International Telecommunications Union (ITU), Hamadoun Touré put it, "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity".

In 2013, a *Symantec report*[101] noted that cybercrime was increasing in Africa at a faster rate than any other region in the world. As *Nir Kshetri*[102] noted recently, some economies in the continent

[100] Longe, O. B., Chiemeke, S. C, Onifade, O. F. W., Balogun, F. M., Longe, F. A. & Otti, V. U. (2007). Exposure of children and teenagers to Internet pornography In Southwestern Nigeria: Concerns, trends & implications. Journal of Information Technology Impact, 7(3), 195-212. Retrieved from http://www.jiti.net/v07/jiti.v7n3.195-212.pdf
[101] https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (Accessed on 12/23/19)
[102] Kshetri, Nir (2010) "The economics of click fraud", IEEE Security & Privacy, 8 (3), May/June, 45-53.

are becoming attractive to cybercriminals, thanks to the high degree of digitization of economic activities.

For instance, 86% of South Africans extensively use online banking services. This proportion is higher than many countries in the Middle East and Turkey.

The more people in Africa, use the internet for their daily activities like banking, entertainment etc., the more exposed to cybercriminals they become. One of the main reasons for the upsurge in cybercrimes in Africa is the fact that the internet is poorly secured in most countries. It is paramount for developing countries, including African ones to put in place a robust cybersecurity architecture to protect online users.

African countries must also train more people in the field of cybersecurity to help both the private and the public sectors in the fight against cybercrimes.

Tens of thousands of jobs if not hundreds of thousands could be created on the continent in the field of cybersecurity. The lack of expertise in the fight against cybercriminals compounds the issue of cybercriminality in Africa and especially in West-Africa.

West-Africa has been over the past couple of years an underground market for cybercrimes that make headlines around the world. Although sixteen countries comprise the West-African region, only three of them are the epicenters of cybercrimes, namely Nigeria, Ghana, and Cote d'Ivoire.

Since the latter country is the target of this dissertation, we are going to dissect empirically cybercrimes in the other two (2) regional hubs, Nigeria, and Ghana. As the saying goes, give to Caesar what is Caesar's, meaning we are going to first analyze cybercrimes in Nigeria./.

* NIGERIA

The Republic of Nigeria is certainly the most well-known West-African country in the world both in good and bad things. Nigeria is in West Africa along the Atlantic Ocean's Gulf of Guinea. Its land borders are with Benin to the west, Cameroon and Chad to the east, and Niger to the north.

The country gained its independence from Great Britain in 1960 and as of 2017, has a population of 190.9 million people. There are three major languages spoken in Nigeria besides English: Hausa, Igbo, and Yoruba.

The country went through a horrific civil war in the 70s with more than a million casualties. Nigeria is rich in oil and gas but has never really taken advantage of it to build a middle class; in fact, the oil 'curse' was the main reason of the multiple military coups since the country gained its independence.

It has given birth to an endemic corruption at the highest levels of government. Fortunately, the country has become a democracy at the end of the past century, precisely since 1999.

Over the past twenty years, the different administrations of the country have tried to combat the scourge of corruption within the country with mixed results. Nigeria has also a vibrant and entrepreneurial youth both inside and outside the country.

In recent years, Tech giants like Facebook, Google and Microsoft have invested heavily in Nigeria to tap into the creativity of the Nigerian youth.

Unfortunately, few people around the world know these positives developments inside the country. Rather, most people outside Nigeria know the country as the place where e-mails with offers of

giving away “free” money originate. The bulk of cybercriminals who operate in West-Africa are in Nigeria.

These scammers operate under the slogan “I Go Chop Your Dollar” as *Longe et al.*[103] pointed out in a 2009 report.

They also noted that the criminals take great pride in how much they can exploit victims (usually from the western world) with some even claiming it is a payback for what the “Whiteman” has done to Africa.

Most Cybercriminals operating in Nigeria do so through email scam and phishing. They usually send you an email saying that they are the children of a rich personality in government, banking or the military who have inherited millions of dollars sitting in a bank; they want your help to transfer the money out of the country for a small percentage of the total amount which always amounts to millions of US Dollars. The practice has gone global to the point that the label “Nigerian Prince” is widely known to refer to these scammers.

As we have talked about previously, the issue of cybercrimes in Nigeria was preceded by the appearance of organized crime syndicates since the independence of the country in 1960, if not earlier.

These organized crime groups specialized in human trafficking, arms smuggling, illegal drugs smuggling and later will introduce what was then called the “Nigerian letter”, ancestor of the modern “advanced fee fraud” which consists of promising something of value to get the victims to pay some negligible amount of money.

[103] Longe, O. B., Chiemeke, S. C, Exposure of children and teenagers to Internet pornography. (Supra note 100) P.60.

Today, these practices have spread all over Africa and sometimes outside of the African continent. As we also previously noted, the "Nigerian prince" could be someone in Nigeria, but also someone in Accra, Ghana or in Johannesburg, South Africa or even a native of the United States or Russia.

Apparently, many people want a piece of the "pie" by acting like a scammer from Nigeria. It is important to note that the Nigerian authorities have been aggressively combatting the scourge of cybercrimes through a plethora of both legal and enforcement measures although with mixed results.

The country also is collaborating with international partners like the Federal Bureau of Investigation (FBI), the United States Justice Department etc. to more proactively go after these criminals whose actions give a bad name to the most populous nation in Africa.

Beside these governmental efforts, we think that the Nigerian government should invest more money in Law enforcement readiness, combatting corruption at all levels of society beginning with members of the administration.

One thing young people either in Nigeria or elsewhere in Africa, always use as an excuse to justify their criminal behavior, is that those in power are getting rich through corruption on the back of the people.

We also think that the only investment that will curb cybercrimes and other forms of illegal activities in Nigeria in the long term is an investment in education. Young Nigerians lucky enough to get an education excel wherever they are.

The Nigerian community in the United States holds more PhDs than any other group in the country. Educated Africans are rarely involved in crimes, including cybercrimes no matter which part of Africa they are from./.

* GHANA

The Republic of Ghana[104], is a country located along the Gulf of Guinea and Atlantic Ocean, in the subregion of West-Africa. Spanning a land mass of 238,535 km^2 (92,099 sq. mi), Ghana is bordered by the Ivory Coast in the west, Burkina Faso in the north, Togo in the east and the Gulf of Guinea and Atlantic Ocean in the south. *Ghana* means "Warrior King" in the Soninke language.

Ghana became independent from Great Britain in 1957. As of 2017, Ghana had almost 30 million people. The country went through political instability after the independence; it became a democracy some twenty years ago. The Ghanaian youth is one of the most mobile in Africa in terms of emigration inside and outside of Africa.

The spread of organized crime in Ghana can be traced back to an event that occurred in the 80s, the deportation of more than one million citizens of Ghana from Nigeria. Some unemployed youths who came back home to find no work, became involved in illegal activities, among them, the infamous 'advanced fee fraud' that originated in Nigeria.

As Longe and Chiemeke[105] noted, the frauds take the form of victims being approached by letter, faxes or, recently, electronic mail, without prior contact. Victims' addresses are obtained from telephone and email directories, business journals, magazines, newspapers or through web e-mail address harvesters.

[104] https://en.wikipedia.org/wiki/Ghana (Accessed on 1/9/2020)
[105] Longe & Chiemeke, S. (2006). The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. In Proceedings of the 1st International Conference of the International Institute of Mathematics and Computer Sciences, June Covenant University, Ota, Nigeria, 1 - 7.

Today, cybercriminals only harvest e-mail addresses since telephone directories are no longer in use in most countries.

Cybercrimes or "Sakawa" in Ghana are on par with cybercrimes in Nigeria and Cote d'Ivoire. In fact, while working on this dissertation, two cases of online romance scam involving Nigerians and Ghanaians made headlines here in the United States. In one case[106], a 76-year-old New Jersey woman was tricked into giving $125,000 to a man who pretended to be in a romantic relationship with her.

The perpetrator happened to be a national of Ghana and was working with accomplices back in Ghana. He was arrested and charged with 2nd-degree theft and 2nd-degree money laundering, but his accomplices were not.

In the other case[107] involving citizens of Nigeria, the FBI in collaboration with Nigerian authorities, arrested 80 cybercriminals both in the US-California- and in Nigeria.

To fight cybercrimes, the Government of Ghana has taken several measures, including the Electronic Transaction Act (ETA) of 2008 which has specific legislation on cybercrimes and prescribes punishment for cybercrime perpetrators.

On top of the ETA, the Parliament of Ghana passed the Data Protection *Act (DPA)* of 2012 to protect the privacy and personal data of individuals. Ghana also put in place a National Cybersecurity Centre[108] whose main goal is to be responsible for Ghana's cybersecurity

[106] https://www.nbcbayarea.com/news/national-international/76-year-old-new-jersey-woman-tricked-into-giving-away-125000-to-online-boyfriend/1961429/ (Accessed on 1/12/20).
[107] https://abc7.com/fbi-serves-arrest-search-warrants-in-south-bay-connected-to-international-scams/5485625/ (Accessed on 1/12/20).
[108] https://cybersecurity.gov.gh/ (Accessed on 1/14/20)

development including cybersecurity incidents response coordination within government and with the private sector.

Despite these encouraging measures, there is an urgent need for the Ghanaian authorities to better educate the public on the damage to its international image, cybercrimes or “Sakawa” causes the country.

We also think, just like in the case of Nigeria, that there is also an urgent need to invest in the youth through education. Again, an educated man or woman is less tempted by committing crimes in general and cybercrimes especially.

While the benefits of investing in education take time, it is important to keep in mind that there is a youth ready and able to launch small businesses; thus, the need to create the conditions for the development of entrepreneurship among the youth.

On the legal front, we think it is paramount for the state to be able to go after cybercriminals, to prosecute and sentence them as a deterrent for other people with ill-intent. In other words, the fight against cybercrimes in Ghana as in the rest of Africa, requires a combination of social, economic, and legal measures for a more effective success in this endeavor.

The republic of Ghana should also train both Law enforcement and civilians to be capable of dealing with the scourge of cybercriminality spreading at the speed of an Australian wildfire all over Africa.

At last, it is paramount for Ghana to intensify its cooperation within ECOWAS, but also with international partners better equipped to deal with cybercrimes.

One such ideal partner would be the Federal Bureau of Investigation (FBI) if there is not already some form of cooperation between them./.

3-3: Typology of Cybercrimes in Cote d'Ivoire

3-3-1: Phishing

Phishing[109] is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card numbers, or other sensitive details by impersonating oneself as a trustworthy entity in a digital communication. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an *Advanced Persistent Threat (APT)*[110] event. In this latter scenario, employees are compromised to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

According to the cybersecurity[111] firm, *Security Boulevard*, 22% of all data breaches in 2020 involved phishing attacks.

[109] Wikipedia contributors. (2021, March 29). *Phishing*. Wikipedia. https://en.wikipedia.org/wiki/Phishing
[110] G Urbas and KR Choo, Resource materials on technology-enabled crime, AIC, Canberra, 2008, p.85.
[111] Meharchandani, D. (2020, December 7). *Staggering Phishing Statistics in 2020*. Security Boulevard.

Some of the biggest phishing attacks of 2020 involved big companies like Nintendo and Twitter[112]. In Cote d'Ivoire, cybercriminals too use phishing as a technique to trick their potential targets to steal important data like credit card information, personal information etc. A google report[113] dating back to 2014, showed that phishing is the main way manual hijackers steal user credentials. The report found that phishing requests target victims' email (35%) and banking institutions (21%) accounts, as well as their app stores and social networking credentials. Of the hijacking case samples analysed, it was found that most of the hijackers appear to originate from five main countries: China, Côte d'Ivoire, Malaysia, Nigeria, and South Africa.

This report confirmed our assumptions that cybercriminals in Cote d'Ivoire usually target French-speaking countries while Nigerian cybercriminals target English-speaking countries like the United State or the United Kingdom; per the report[114], "two major groups of hijackers emerge: the Nigerian one (NG) and Côte d'Ivoire (CI) one.

---

[112] Sari, O. (2021, March 10). *The Biggest Data Breaches in the first half of 2020 - Keepnet Labs*. Anti-Phishing Solution and Security Awareness Training - Keepnet Labs. https://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020/

[113] Google Inc. (2014). *Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild*. http://intellivoire.net/wp-content/uploads/2014/11/google_hijacking_study_2014.pdf (Accessed on 03/29/2021). Excerpt of the report: "Injecting decoy credentials in phishing pages targeting Google users reveals that criminals' response time is surprisingly fast. We found that criminals attempted to access 20% of the accounts within 30 minutes. Looking at real hijacking cases, we observed that, once logged in, manual hijackers' profile the victim's account and spend an average of 3 minutes to assess the value of the account before exploiting it or abandoning the process. This step entails searching through the victim's email history for banking details or messages that the victim had previously flagged as important. We also see attackers scanning through email contacts which are then either solicited for funds or targeted with a salvo of targeted phishing emails. Restoring a victim's account access is a non-trivial problem. We found that SMS is the most dependable out-of-band channel, where users that provided a phone number recover their account 81% of the time. Providing a secondary email address is also fruitful, succeeding 75% of the time. Absent these two mechanisms, we must rely on secret questions or manual review where our success rate falls to 14%."

[114]Ibid. In terms of defence strategies, the report suggests "Using a second authentication factor, such as a phone, has proven the best client-side defense against hijacking. While second factor authentication has some drawbacks, we believe that it is the best way to curb hijacking long term. The main issue with second factor authentication is that it is incompatible with legacy applications, such as mail clients. We work around this by authorizing our users to generate an application-specific password for those type of apps. However, this is far from ideal since those passwords can be phished. Consequently, we also collaborate with vendors to move their apps to a better authentication technology, such as OAuth. An additional drawback of second factor authentication is usability. While phones provide a good user experience, we are exploring alternatives [7] for people who do not have a smartphone (e.g., emerging countries) or want a separated physical device. We hope to see more research done in this space as there is a clear need of innovation in term of usability and accessibility."

We believe those two groups to be different as their native language differs, French vs English, and they are 2000km apart. Anecdotal evidence suggest that Côte d'Ivoire specialize in scamming French speaking countries whereas Nigeria focuses on English speaking countries. The volume of phone numbers involved in this type of attack is small enough to corroborate our hypothesis that it is manual work and large enough to point to organized groups that are dedicated to monetizing hijacked accounts.

Finally, we note that South Africa (ZA) account for 10% of both datasets which suggest that South Africa is also one of the largest home of hijackers".

This report shows that Cote d'Ivoire for at least the past decade has been known internationally to be a hotspot of cybercrimes.

In fact, phishing is the first step in the process of stealing from unsuspecting online users; once the target opens the message received, a virus takes hold of the computer system allowing the criminals to steal personal information, credits card and sometimes other valuable information. As the site "Webroot"[115] explains further, cybercriminals "use spam, fake websites constructed to look identical to real sites, email and instant messages to trick you into divulging sensitive information, like bank account passwords and credit card numbers."

In Cote d'Ivoire, cybercriminals in recent years, have changed their tactics by moving to social medias like Facebook, Instagram, Twitter etc. to target lonely souls looking for love.

That is why, in the Ivorian media, most of the public stories focus on romance scams while phishing scams are less talked about.

[115] Webroot. *What Email Phishing Scams Do and How to*. (2020).www.webroot.com.

One reason for the popularity of romance scams in the public psyche, is that it targets everyone who is on social medias while email phishing for example targets companies and a very few individuals as far as Cote d'Ivoire is concerned. Nevertheless, it must be noticed that individuals are targeted on their mobile phones to steal money stored digitally which we will be talking about later.

One last thing to signal is the existence of Phishing Kits on the dark market known as Phishing-as-a-Service (PaaS). The security website wow.intsights.com[116], defines Phishing Kits as software packages that streamline the process of copying a site design and uploading it to another web server as a phishing site.

They come with simple instructions on how to use them to duplicate a site and upload it to a web server added wow.intsights.com. This makes becoming a phishing guru without the skills needed, even easier.

Recommendations

We will never say it loud enough, online users need to be careful when dealing with emails in their inbox or even text messages on their smartphones because criminals are always trying to trick you into opening this message that seems coming from a familiar source. Most of the time, they play onto this sensation of familiarity or even knowledge of the source of the email to encourage you to open it without any care.

[116] *Banking & Financial Services Cyber Threat Landscape Report*. (2019). https://wow.intsights.com/rs/071-ZWD-900/images/Banking%20%26%20Financial%20Services%20Cyber%20Threat%20Landscape%20Report.pdf (Accessed on 04/09/2021). Here is how Phishing Kits work in the real-world: "After the copied site is up, the hacker starts sending phishing emails to target users, attempting to trick them into visiting the site. Phishing kits have increased the quantity and velocity of phishing attacks around the world by lowering the hacker barrier to entry, enabling novices to run campaigns with limited technical knowledge. While this is not a new development or trend, phishing attacks still remain one of the most common methods cybercriminals use to target organizations."

I have to admit that even myself, falls time to time for these phishing emails. The point is to reduce to the minimum, the number of times one falls for these tricks. Here are a few tips provided by Webroot[117] to protect yourself against phishing emails:

How will I know if I have been phished?

Phishers often pretend to be legitimate companies. Their messages may sound genuine, and their sites can look remarkably like the real thing. It can be hard to tell the difference, but you may be dealing with a phishing scam if you see the following:

- Requests for confidential information via email or instant message
- Emotional language using scare tactics or urgent requests to respond.
- Misspelled URLs, spelling mistakes or the use of sub-domains
- Links within the body of a message
- Lack of a personal greeting or customized information within a message. Legitimate emails from banks and credit card companies will often include partial account numbers, username, or password.

How can I protect myself from phishing?

When you arm yourself with information and resources, you are wiser about computer security threats, and less vulnerable to phishing scam tactics. Take these steps to fortify your computer security and get better phishing protection right away:

- Do not provide personal information to any unsolicited requests for information.
- Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser.

[117] Webroot. *What Email Phishing Scams Do and How to*. (2020).(Supra note 115) P.71.

- If you suspect you have received phishing bait, contact the company that is the subject of the email by phone to check that the message is legitimate.
- Type in a trusted URL for a company's site into the address bar of your browser to bypass the link in a suspected phishing message.
- Use varied and complex passwords for all your accounts.
- Continually check the accuracy of personal accounts and deal with any discrepancies right away
- Avoid questionable websites.
- Practice safe email protocol:
    - Do not open messages from unknown senders.
    - Immediately delete messages you suspect to be spam.

We should also encourage the Ivorian Authorities to recruit more volunteers for a national awareness campaign which will be repeated at least twice a year./.

3-3-1: Romance scam

Cote d'Ivoire is one of the epicentres of romance scams in West-Africa, behind Nigeria and ahead of Ghana. The issue is such that some foreign embassies in Abidjan, the economic capital of Cote d'Ivoire, have issued warnings to their nationals on their local websites.

This is the case of the US embassy[118]and the French embassy which advise their citizens through the description of a romance scam and other types of scams plus several tips on how to detect them.

The obvious question to ask is what is a romance scam? According to the FBI's website[119], romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

In the United States, the last three (3) years have seen an exponential growth in romance scams losses for the victims. As Emma Fletcher pointed out in an article[120] on the Federal Trade

[118]U.S. Embassy in Cote d'Ivoire. (2015, December 7). *419 Scams.* https://ci.usembassy.gov/embassy/embassy/sections-offices/419-scams/?_ga=2.105688195.122874908.1583284762-452227721.1583284762

[119] *Federal Bureau of Investigation*. Romance Scams. (2020, April 16). https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams (Accessed on 03/22/2021).
See description here: "The criminals who conduct romance scams are experts at what they do and will seem genuine, caring, and believable. Con artists are present on most dating and social media sites. The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money. Scam artists often say they are in the building and construction industry and are engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they ask for money for a medical emergency or unexpected legal fee. If someone you meet online needs your bank account information to deposit money, they are using your account to conduct other theft and fraud schemes."

[120] Federal Trade Commission. *Romance scams take record dollars in 2020*. (2021, February 10). https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020 (Accessed on 03/22/2021). Why 2020 saw so many losses for romance scams victims?
Read here: "It is reasonable to wonder: what happened in 2020 to make these dollars losses continue to spike? An obvious reason may be the pandemic limiting our ability to meet in person. But outside the pandemic, the share of people who have ever used an online dating site or app has also been rising.[3] And romance scammers are primed to take advantage. Scammers fabricate attractive online profiles to draw people in, often lifting pictures from the web and using made up names. Some go a step further and assume the identities of real people. Once they make online

Commission website, "for three years running, people have reported losing more money on romance scams than on any other fraud type identified."

In 2020, romance scams losses in the United States amounted to a whopping $ $304 million, up about 50% from 2019 per the article.

To explain the record amount of romance scam losses in 2020, the author argued that Covid-19 and its multiple confinements may have had an impact on this situation. Many people confined to their homes, tended to use dating apps to find a soulmate.

So how does a romance scam work? Cybercriminals operating for the most part from West-Africa and in our case, from Abidjan, create fakes profiles on dating sites and apps or through social media platforms like Facebook, Instagram, or Google Hangouts with stolen pictures from the internet and present themselves as either a lonely woman or man looking for love. According to the Federal Trade Commission[121] (FTC), the scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money. Some of the lies romance scammers tell their potential victims per the FTC, are as follow: they often tell their victims that they:

- Work on an oil rig,
- In the military,
- A doctor with an international organization.

Romance Scammers also tend to ask their targets for money to:

contact, they make up reasons not to meet in person. The pandemic has both made that easier and inspired new twists to their stories, with many people reporting that their so-called suitor claimed to be unable to travel because of the pandemic. Some scammers have even cancelled first date plans due to a positive COVID-19 evaluate".

[121] Consumer Information. *What You Need to Know About Romance Scams*. (2021, March 4). https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams (Accessed on 03/22/2021)

- Pay for a plane ticket or other travel expenses,
- Pay for surgery or other medical expenses,
- Pay custom fees to retrieve something,
- Pay off gambling debts,
- Pay for a visa or other official travel documents.

As for the methods of payment, these scammers ask their victims to pay:

- By wiring money,
- With reload cards like MoneyPak or gift cards from vendors like Amazon, Google Play, iTunes, or Steam. (Source: Consumer.ftc.gov)[122].

Three countries out of West-Africa, are the main hubs of romance scams targeting Westerners: Nigeria, Ghana, and Cote d'Ivoire. In the latter country, romance scammers due to language barriers, tend to target French-Speaking Europeans (France, Switzerland, Belgium) and Francophones in Canada and elsewhere. Here is the testimony[123] of a victim of romance scam living in Canada who is Francophone.

[122] Consumer Information. *What You Need to Know About Romance Scams*. (Supra note 121) P.76.

[123] *Testimonial: 3 months of love and dirty water*. (2017, April 2). Romance Scams. https://arnaqueinternet.com/racontez-votre-histoire/arnaques-aux-sentiments/3-mois-d-amour-et-d-eau-sale/
Hello, I have never been raped, (all my respects and sympathies for those who have been), but I can tell you that I exactly felt a rape following the love scam that I have suffered recently. Widowed for almost 2 years, after 27 years of happiness with a remarkable partner, I accompanied him in his fight against cancer for 8 years. I know what empathy is and the importance of helping. A network of scammers on the Badoo dating site horrified me and abused my vulnerability. After hearing about this site, I decided to create a profile in September 2012. My big mistake was to agree to correspond with a man from another country. He calls himself a businessperson, his name is ADRIAN POLVSEN, well-off, widowed and whose wife, he met at the university, died during the delivery of their second child, a son. He has a daughter WANITA POVLSEN who lives in Malaysia where his wife was originally, and whom her mother-in-law wanted to take care of since she was her only granddaughter. Him being a businessperson from London said he saw her once or twice a year. He even put me in touch with her via email. He sent me a picture of her. She looked like him. It was all so coherent and felt so true. He had great values, charming, attentive, really, I believed in everything that he said to me. Yes, I had doubts I expressed to him, but not 2 seconds later, he was leading me back to where he wanted. He called me every day and yes, in my vulnerability I fell for it. Very few times have I had doubts and he would ask me to talk to him every day via Skype, Yahoo Messenger or on the phone. He told me he wanted to come to Canada and settle down with his daughter. He told me that he had entered into a contract for the sale of Honda vehicles that were en route by boat to Kharkov in Ukraine. This is where the horror began. The morning before his

In some cases, arrests are made like this one that took place both in Quebec and Abidjan, Cote d'Ivoire. This particular romance scam caused the loss of $2.3 million to the victims who are elderly from Quebec, Canada. During our research, I was able to connect with cybercriminals posing as Ivorian women looking for love on Facebook. They use beautiful pictures of women on google that can be accessed by typing "girl" in google search. My "date" whose last name was "Yao" sent me a picture when I asked "her" to take a picture of "herself" right away and send it to me. I must point out that her last name "Yao" is for males in Cote d'Ivoire. As the picture showed, "she" did not seem happy to take a headshot for me. The picture can be found in google by simply right clicking it and select search on google. Sometimes, some cybercriminals specialized in romance scams, "play" the role of both a "man" and a "woman" depending on who they are talking to online.

departure he phoned me before leaving for the airport and as soon as he arrived in Ukraine, he started asking me for money for customs clearance and sales certificates to deliver the vehicles to the buyer. I sent him the requested money, a considerable sum and after customs clearance, he put me in touch with his customs broker Francis Adigwe to explain to me that everything was true. A few days before he left Ukraine to see me, he called me to tell me that during the delivery of the vehicles, drugs were found in one of the last cars in the warehouse and that the police were coming to look into it. He told me to phone his broker who was the only one who spoke English to help him. There I was very scared since I had sent some money for customs clearance and could have been involved in this criminal situation. He would phone me regularly to ask for CAD180,000 to give to the corrupt police in Ukraine so he would not go to jail, and he would cry every time he called me. I told him I did not want to be involved in this story and all I asked for was my loaned money. He told me he would reimburse me as soon as the vehicle buyers were there to pay him but until the case was settled with the corrupt police, he would not be paid. His broker called me regularly to tell me that he would protect me and that my name would not be disclosed to the Ukrainian police. I finally came out of my vulnerability; naivety and the doubts rose again. I called a criminal lawyer to make sure I would not be involved, and he confirmed it was a fraud and to go to the police. What I did, I went to file a complaint. I have also opened a case of fraud with the RCMP (Royal Canadian Mounted Police) who take these frauds very seriously. My bank has been informed and with the international security department are still seeing what can be done for the protection of their clients. The RCMP told me that there are thousands of people who have been defrauded for romance./.

Recommendations

We will never say it enough, people in search of a soulmate should be careful when using dating sites. You should make sure that you are dealing with the right person both on social media and on dating sites. You should never send money to people you have never met in person./.

3-3-2: Advance-Fee Fraud

The FBI[124] defines Advance-Fee Fraud as when the victim pays money to someone in anticipation of receiving something of greater value- such as a loan, contract, investment, or gift- and then receives little or nothing in return.

Advance-fee fraud, also known as "419"-in reference to the fraud designation in the Nigerian criminal code- in fact dates back right after the French revolution[125].

It was known as the "Spanish Prisoner' a century later. According to Finn Brunton's article[126] in the Boston globe, the first recognizable version of the Spanish Prisoner cropped up in the aftermath of the French Revolution. It went like this: A letter arrived describing an aristocrat in exile, say, the Marquis de …, who in escaping from revolutionary violence had thrown a chest full of jewels into a lake.

His faithful servant, now writing this heartfelt letter, had come back to retrieve it, and unfortunately ended up in prison. With just a little help from you, a fellow Frenchman, to aid in the servant's bail or escape, you would earn a portion of the loot. The scheme worked: "Of a

[124] Federal Bureau of Investigation. "Scams and Frauds from A to Z." San Bernardino, CA. August 4th, 2017.
[125] Finn Brunton. "The long, weird history of the Nigerian e-mail scam." Globe Correspondent, May 19, 2013, 12:00 a.m. https://www.bostonglobe.com/ideas/2013/05/18/the-long-weird-history-nigerian-mail-scam/C8bIhwQSVoygYtrlxsJTlJ/story.html (Accessed on 09/09/2020).
[126] Ibid.

hundred such letters" sent by French confidence tricksters, "twenty were always answered," wrote Eugène Vidocq, the French criminal turned detective.

The Spanish Prisoner[127] was popularized in the United States during the Spanish-American War. Havana and Madrid offered the perfect setting for the letter's promises—remote but not inaccessible, exotic but recognizable, and full of mercenaries, adventurers, and corrupt officers. A detailed, daily presence in the pages of Pulitzer's and Hearst's newspapers, the war provided an ideal context for the story of a military man imprisoned in Spain with money concealed in the United States (say, a shipment of Cuban gold) that he could recover—with your help. Bolstered by current events folded into the story—I was captured at the battle of X, I was friends with famous dead soldier Y—the scam proliferated, and Spanish Prisoner syndicates on the East Coast did a brisk business. Beginning in the 80s, millions of "letters" originating from Nigeria were sent all over the world "promising" millions of dollars to unknown people if they were willing to contribute a small fee to get the money out of the country. One common theme between the geographical places where advance-fee fraud proliferated over the past 200 years was the instability following social and political upheaval: the French revolution, the Spanish-American war, and the multiple coup d'états in Nigeria in the 80s.

As Finn Brunton[128] put it, far from being a testament to the rise of the internet, advance-fee fraud is a window into much deeper human impulses and fears. "The scam tends to arise wherever we assume corruption and confusion are greatest, and its long and twisting story offers a kind of negative portrait of world history—the places over the last few centuries where those fears have most firmly taken root", he added.

[127] Finn Brunton. "The long, weird history of the Nigerian e-mail scam" (Supra note 125) P.79.
[128] Ibid.

Today, advance-fee fraud is present in most West-African countries, including Cote d'Ivoire. The issue is so serious that the US Embassy[129] in Abidjan, has dedicated a page on its website to describe the scam and how to avoid being a victim.

[129] US Embassy in Cote d'Ivoire. 419 Scams. https://ci.usembassy.gov/embassy/embassy/sections-offices/419-scams/ (Accessed on 09/23/2020).

The Standard Scam:

Send me money, so that I can give you millions in return. This is an old con known as the "advance fee scam" and it dates to the early 1900's through the United States Postal Service. The principal lure is that someone has a large sum of money hidden somewhere (a secret bank account, a trunk held in storage house or in a foreign customs) and that they cannot get the money out of the country safely. However, if you provide them some small "advance fee", the "attorney" will arrange to transfer a percentage of the money (usually in the millions of US dollars) to you if you pay certain "advance" fees to cover the expenses.

The American Embassy in Cote d'Ivoire receives many inquiries a week about such scams. These victims have wired large sums of money to these "fraud baiters" posing as heirs (usually widows or orphaned children) to some lost fortune, whom they corresponded with through an unsolicited e-mail. The "orphaned children" will soon start to call victims "Uncle" or "Aunt", and then soon move up to calling them "Dady" or "Momy" to create an emotional bond to use the "adoption" or "marriage" ruse to lure you into their web with the promise of this hidden money.

The Strategy of the Scams:

They will send you photographs, documents, files, court agreements, or anything you ask for to prove their legitimacy. They will pose as attorneys, government officials, embassy officials, religious figures, and sympathetic characters to further support this illusion. The bottom line is everything is likely false. Every person is likely fictitious and probably the same person acting all roles. All documents provided are usually no more than worthless computer-generated paper. Whatever proof you ask for, they will generate it on the computer, but in the end it normally will all be counterfeit. All photographs provided can be of anyone – a stolen photo, or out of a magazine. The photographs are all untraceable and anonymous. It is often true that it is not the real people behind these scams.

All addresses provided are likely illegitimate, fictitious, or non-existent. They will provide you fake websites or Yahoo! E-mail addresses (most preferred). They have created very authentic looking websites through domains located in other countries to protect their trail. They have even assumed the identities of real persons, attorneys, government officials, and even members of the clergy. This impersonation of real persons (identity theft) allows them to create further illusions to their bona fides should someone attempt to conduct a due diligence on them. In the end, they are all invisible, faceless people hiding behind the Internet anonymously in a West African country where the odds of them ever being identified, caught, or prosecuted are almost non-existent.

All telephone numbers provided will be cell phones. In Cote d'Ivoire, all cell phone numbers start with 01, 02, 03, 04, 05, 06, 07, 08, 09, 40, 60, 65, 66, 67. They do not generally provide landline telephone numbers, since these numbers can be easily traced to a physical location. Anyone in Cote d'Ivoire can easily purchase an inexpensive cell phone on a street corner and then purchase anonymously a pre-paid SIM card to operate their "business" out of this cell phone number, without ever having to provide any subscriber information. If they believe that they are being traced, identified, or near arrest, they can abandon their fake identities by tossing these pre-paid cell phone and any tools of their trade into a public trashcan and walk away, thus protecting their true identities.

For faxes, they will provide hard-line numbers to public Internet or Cybernet Cafes to further hide their clandestine operations and anonymity (and where they operate their e-mails and fake websites too). Over the Internet, they are "pretenders" and can assume the identity of anyone whom they want to be, and they can provide you any fake document or photo you want as proof. Since many names, stories, and modus operandi are like other scams here, it is suspected that the same ring is running several scams at once.

Many victims refuse to believe that they have become a target or a victim, or that they can "out con" these professional scam artists. Whenever a victim instructs the "attorney" or "heir" to contact the US Embassy, they will always provide the victim reasons why they cannot do this. The victim must realize that if these people have cell phones, have access to their e-mail and the Internet, and travel freely to a bank or Western Union / MoneyGram to retrieve wired funds, then they certainly are capable of contacting or visiting the US Embassy. It is usually at this time that the scam artists know the scam has been recognized and will quickly abandon the scam and break off communications with the victim,

The victims of advance-fee scams in Cote d'Ivoire used to be Europeans (mostly French but also Belgian, Swiss and citizens from Luxemburg). The reason being that French is spoken in these countries.

Today, thanks to the collaboration between the Ivorian Authorities and the European Union, less Europeans are victims of scams coming from Cote d'Ivoire. Instead, Ivorian cybercriminals have turned their attention to Ivorian citizens.

---

or then pose as law enforcement officials to "assist" them further with retrieving their lost funds. Of course, there will be new additional "advance fees" to do this.
Any money wired to them will be forever lost and irretrievable. If they hook a victim, they will always insist money be wired through WesternUnion or MoneyGram. They prefer WesternUnion and MoneyGram because these funds can be easily retrieved at any branch (thousands of them) throughout the country using their false ID. The branch location where they retrieve the wired funds are virtually impossible to identify or locate in Cote d'Ivoire. And, without a subpoena, WesternUnion and MoneyGram (in the US) will not provide any information to the victim or law enforcement agency.
The 419 artists will seldom provide legitimate bank account numbers as these can be traced back to tangible locations. If they provide a specific account to a specific bank, successful surveillances have been made to arrest the "fraud baiters." They learn from their mistakes, and their share "lessons learned" within their sub-cultured network. These 419 "fraud baiters" are smart, devious, and heartless. They are also dangerous and ruthless. They have lured victims to West Africa where they have kidnapped them for ransom, killed them, or both. They will not hesitate to bribe judges, officials, or witnesses, and they will not hesitate to kill anyone who interferes with their organized crime operations, or anyone who cooperates with the police investigating them. They operate invisibly and are nearly impossible to identify, locate, arrest, and prosecute. Therefore 419 scams are the fourth largest industry in West Africa. They prey upon the greed, gullibility, loneliness, and the sympathies of their intended victims, many of whom are quite educated. Most 419 "fraud baiters" are Nigerian Muslim males who often pose on singles websites (Matchmaker or Christian singles websites) posing as Christian women or men. These are also known as 419 "Lonely Hearts" scams and have successfully duped many trusting and lonely Christians out of large sums of money.
They have posed as priests, ministers, evangelists, missionaries and even nuns being persecuted in Muslim countries, and they are trying to find ways to get the tithes of their church out of the country. Of course, these riches they promise will require you to provide them some "advance fee" for the attorney, licenses, and new unforeseen bureaucratic requirements that will be never ending.
The first fees will be small, but one bureaucratic problem leads to another requiring just "one more" payment to create the illusion that you are almost there. This dangle or "carrot" of just one more payment to receive all these millions will eventually add up to thousands of dollars. By then, it is too late.
If such money did exist, they will not share it with a stranger they met over the Internet in exchange for assisting them. If such money existed, they would have family, friends, and political contacts who would gladly help them. Remember; if you send any money to these people consider it lost forever.
Regretfully, some have contacted us too late after losing their entire life's savings (hundreds of thousands of dollars) expecting to receive these millions in return, to adopt an orphaned refugee, or find a new love, spouse, or companion they met over the Internet./.

The immediate consequence of that shift is that cybercriminals who used to be “heroes” for ordinary people for making the “white man pay back what he stole during colonial times” are now seen as thugs, thieves etc. for stealing from the locals.

They are now more often being denounced by their Ivorian victims, arrested, and prosecuted by the Ivorian Authorities. Some of the types of advance-fee fraud originating from Cote d’Ivoire are “Stranded traveler” (1), Inheritance (2) and Lottery (3).

1- Stranded traveler:

In the case of the “stranded traveler”, Ivorian cybercriminals through phishing(e-mail), contact their victims and pretend to be “Law enforcement” who have in their “custody” the victim’s relative “stranded” due to the loss of their documents, while on vacation or for work, and without money to purchase a plane ticket back to Europe. The goal being to convince the victim to send virtual money through for example Orange Money.

2- Inheritance:

In this case, the cybercriminals tell their victims about an inheritance left to them by a rich dad or mom that they would like to transfer outside the country (Cote d’Ivoire) if only their victims are willing to pay a small fee for administrative and bureaucratic papers. The intent being to let their victims know that they will receive a big chunk of the inheritance once the money is out of the country.

3- Lottery:

The lottery scam is straightforward: the scammers inform their victims that they had won a lottery they have not participated in. To get the lumpsum payment, they often ask the victims to pay small "administrative fees" by sending their credit card information or their biographic information.

As the saying goes, if it is too good to be true, then it is not true. All the scam techniques enumerated above are old as mankind itself, but unsuspecting people always fall for them. The losses to the victims are in the millions of dollars each year.

Recommendations

Once again, it is important for the public to be skeptical of those "wonderful" offers they received in their mailboxes or through their email addresses. People should also take a deep breath when they receive such offers: how is it possible to win for example a lottery to which you have not participated in?

A little bit of questioning will save you money and your sanity, if not your life, because many victims of these scams end up taking their own lives. Public awareness campaigns should be constantly held to inform the public regarding online scams of all types.

Here in the United States, there are no formal awareness campaigns held regularly but only warnings on public websites (FBI, Justice Department etc.) for the most part. The media gets involved when there is a case where a substantial financial loss or even a loss of life occurs and is newsworthy.

It is obviously not enough since most people do not always pay attention to the news. Non-profits organizations should dedicate time and resources to informing through small workshops, the most vulnerable who are the elderly and people living alone. I have started such workshops[130] here in San Francisco earlier this year./.

[130] www.aducademy.com

3-3-3: Malware

The *Oxford dictionary*[131] defines Malware as a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Short for "malicious software," malware can be found in viruses, worms, trojan horses, and spyware.

Country	Rank	Percentage within Africa	Incident Count
South-Africa	1	20%	1,716,308
Tunisia	2	14&	1,166,774
Kenya	3	8%	668,194
Nigeria	4	6%	469,018
Cote d'Ivoire	5	5%	407,112
Ghana	6	5%	405,805
Egypt	7	5%	400,679
Algeria	8	4%	304,114
Ethiopia	9	3%	245,172
Cameroon	10	3%	224,546

Figure1: Top 10 Source African Countries for Malware—2016. Source: Symantec. / African Union.(Source: Symantec)

According to a report by *Symantec*[132] in collaboration with the African Union, the global percentage of malware originating from Africa is 1.5%. Of the top 10 African countries for malware activities, Cote d'Ivoire is number 5 with 407,112 incident count in 2016. Nigeria was number 4 and Ghana at number 6. South Africa and Tunisia are respectively number 1 and number 2.

Overall, the percentage of malware coming from African countries is relatively small compared to the rest of the world. Nevertheless, Cote d'Ivoire, target of this dissertation is among the top 10 African countries where malware originates.

[131] https://www.lexico.com/en/definition/malware (Accessed on 02/13/2020).
[132] See Cybercrime and Cybersecurity: Trends in Africa. 2016. Symantec/African Union.

As the figure showed, the three biggest economies of West-Africa, meaning Nigeria, Ghana, and Cote d'Ivoire account for 16% of malware originating from Africa.

Even here, it is safe to say that the numbers are not that big compared to South-Africa with 20% of malware source. It is important to note that African countries are also victims of malware attacks from various places around the world.

For example, in 2019, *Symantec*[133] reported a wave of malware attacks against African financial institutions in Cote d'Ivoire, Ghana, Cameroon, Democratic Republic of Congo (DRC) and Equatorial Guinea. According to the cybersecurity company Infocyte[134], Africa now has one of the highest global mobile malware infection rates. Infocyte explains this situation by the fact that some African nations were able to entirely skip the stages of bricks and mortar bank branches and landline telephones and move directly into online banking and mobile telephone apps.

[133] Symantec. Report (2019).https://www.symantec.com/blogs/threat-intelligence/african-financial-attacks (Accessed on 03/12/2019). The four types of attacks as described by Symantec: "Symantec has observed four distinct attack campaigns directed against financial targets in Africa. The first has been underway since at least mid-2017 and has targeted organizations in Ivory Coast and Equatorial Guinea. The attackers infected victims with commodity malware known as NanoCore (Trojan.Nancrat) and were also observed using PsExec, a Microsoft Sysinternals tool used for executing processes on other systems, on infected computers. Lure documents used by the attackers referred to a West African bank which has operations in several countries in the region. Some tools used in these attacks are like tools mentioned in a 2017 SWIFT alert, indicating the attackers may have been attempting to perform financial fraud.
The second type of attack began in late 2017 and targeted organizations in Ivory Coast, Ghana, Congo (DR), and Cameroon. The attackers used malicious PowerShell scripts to infect their targets and also used the credential-stealing tool Mimikatz (Hacktool.Mimikatz). They also made use of UltraVNC, an open-source remote administration tool for Microsoft Windows. The attackers then infected computers with the commodity malware known as Cobalt Strike (Trojan.Agentemis) which is capable of opening a backdoor on the computer, communicating with a command and control (C&C) server, and downloading additional payloads. Communication with the C&C server was handled by dynamic DNS infrastructure, which helped shield the location of the attackers.
The third type of attack was directed against an organization in Ivory Coast. This organization had also been targeted by the second campaign. This second attack also involved the use of commodity malware, in this case the Remote Manipulator System RAT (Backdoor.Gussdoor), alongside Mimikatz and two custom Remote Desktop Protocol (RDP) tools. Since Mimikatz can be used to harvest credentials and RDP allows for remote connections to computers, it's likely the attackers wanted additional remote access capability and were interested in moving laterally across the victim's network.
The fourth type of attack began in December 2018 and was directed against organizations in Ivory Coast. The attackers used off-the-shelf malware known as Imminent Monitor RAT (Infostealer.Hawket)".

[134] Infocyte (2018). *The Threat of Malware in Africa*. https://www.infocyte.com/wp-content/uploads/security_brief-malware_in_africa.pdf (Accessed on 04/12/2021).

Such rapid growth does not allow the time necessary to progressively establish proper security procedures. According to the same cybersecurity firm, the IT Infrastructure infections rate is 81% in Cote d'Ivoire. Another issue with malware in Africa and Cote d'Ivoire is the proliferation of fake dating mobile applications, source of malware.

According to Trend Micro,[135] more than 7000 attacks affecting mobile users on the continent, have been detected. How does it work? Trend Micro says that to boost their authenticity, the malicious replica applications usually copied the names and designs of popular legitimate dating applications such as Tinder, Bumble, and Zooks.

The fake apps were used as a lure for propagating malware or for collecting personally identifiable information (PII), which can then be sold or used in phishing scams, according to Trend Micro which added that the threat does not end with fake dating applications because even legitimate dating applications can be abused by cybercriminals. Another area where malware proliferates in Africa as a whole, including in Cote d'Ivoire is the sale of smartphones with malware already pre-installed.

In a report published in 2020, the mobile company Upstream Systems[136] exposed the use of the malware Triada on smartphones sold to low-income African consumers in a dozen countries.

---

[135] Trend Micro. *Fake Dating Apps Found as Top Source of Malware in Africa - Security News - Trend Micro ZA-EN*. (2020). https://www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/fake-dating-apps-found-as-top-source-of-malware-in-africa (Accessed on 04/14/2021). "The research disclosed, the sheer amount of information many people share without second thought (full name, contact details, and sometimes, even home and office addresses) make users vulnerable to threats such as identity theft and frauds. Malware can also be propagated through the apps' messaging feature, as most of the apps do not flag messages with malicious content. As personal phones are also often used for work-related purposes, these threats can easily transcend to the enterprise.

[136] Pcmag.com. *Thousands of Cheap Android Phones in Africa Were Pre-Installed with Malware*. (2020). https://www.pcmag.com/news/thousands-of-cheap-android-phones-in-africa-were-pre-installed-with-malware (Accessed on 04/12/2021). Here is how Upstream Systems discovered the pre-installed malware on smartphones sold in Africa: "Usually malware ends up on an Android device after the owner installs a fake third-party app that contains malicious code. However, upstream noticed the Triada malware was getting preinstalled on thousands of Tecno W2 handsets from a Chinese company called Transsion before getting sold to local consumers in countries such as

Recommendations

It is unfortunate to know that most African countries are unwilling or unable to safeguard their IT Infrastructure more seriously. According to the cybersecurity website scidev.net[137], countries like Kenya, Nigeria, and South Africa, have experienced millions of malwares and other attacks last year. "There were 3.8 million malware attacks and 16.8 million PUA detections," says Kaspersky. "In South Africa, there were almost ten million malware attacks and a staggering 43 million PUA detections. Kenyan users faced even more malware attacks — around 14 million and 41 million PUA appearances", Scidev.net added quoting the secretive cybersecurity firm Kaspersky.

In Cote d'Ivoire, we believe the Ivorian Authorities who have done an excellent job at creating the necessary agencies to deal with cybersecurity issues, will once again take the security more

Ethiopia, Cameroon, and Egypt. According to BuzzFeed, the W2 was being sold for as little as $30 but could end up looting funds from unsuspecting victims. This is because the phone would download additional malware called helper, which can proceed to subscribe the owner to costly digital services. "Had the subscription attempts been successful, the data services involved would have consumed each user's pre-paid airtime —the only way to pay for digital products in many emerging markets," Upstream said. In addition, helper will engage "click fraud," by clicking the ads that hang in the background of the device. "All of these actions happened completely in the background and were invisible to device owners," it added. Upstream, which sells an anti-fraud system to mobile carriers, began noticing the suspicious activity in March 2019. Since then, the company has blocked over 19.2 million transactions tied to the malware that tried to secretly sign-up users to subscription services without their permission. The activity was traced back to more than 200,000 unique devices. Upstream decided to investigate further and acquired some Techno W2 products and found the malware would reinstall itself even after a factory reboot. Attempts to remove the malware by uninstalling certain applications also did nothing but cause them to reappear five minutes later. So how did the malware get on the phones? Transsion told BuzzFeed it sourced the infections to an unidentified "vendor in the supply chain process," meaning the hackers infiltrated a third-party firm charged with managing the phones' software. The findings match what other security research from Google has found: The authors behind Triada deliver it by hacking into computers from device manufacturers and secretly planting the malware inside the Android software. Transsion claims to have fixed the infection problem back in March 2018 when the company's W2 phone was initially flagged for delivering the Triada malware. The Chinese company also delivered an update to address helper late last year, but in both cases the user must download and install the patches. Why the patches did not arrive to affected consumers remains unclear. But upstream says phone vendors need to be on guard against malware infiltrating their systems. "It is common that developers and manufacturers are usually unaware of the malware infection," the company said. "They must be extra careful when choosing third party SDKs (software development kits) and modules, preventing questionable SDKs from sneaking malware into their products. "The Triada malware was not found on other found phones from Transsion", Upstream added.

[137] scidev.net. *Cyberattack surge highlights Africa security risk*. (2020, October 8). Sub-Saharan Africa. https://www.scidev.net/sub-saharan-africa/news/cyberattack-surge-highlights-africa-security-risk/ (Accessed on 04/12/2021).

seriously and robustly because of its national security and privacy implications. Although new laws adapted to the cybersecurity threat exist, one must point out the lack of skilled personnel both at the Ministry of Justice and within the different agencies overseeing the telecommunications sector.

To sums up, more frequent trainings are warranted for the existing personnel but more needs to be done to recruit new and well-trained individuals to join in the fight against cybercriminality in Cote d'Ivoire. One way to get new expertise to deal with security threats in the digital arena faster, is for the Ivorian Authorities to for example, make a financially sound proposition to Ivorian citizens living abroad and who are experts in cybersecurity to return to Cote d'Ivoire to join in the fight.

They should be given the salaries and other benefits these experts earned in developed countries like France, Canada, and the United States etc./.

3-3-3: Sextortion

The FBI[138] defines sextortion as a serious crime that occurs when someone threatens to distribute your private and sensitive material if you do not provide them images of a sexual nature, sexual favours, or money.

In Cote d'Ivoire, cybercriminals engaged in sextortion threaten their victims to distribute their videos if they are not provided with money which seems logical since their victims usually live thousands of miles away in the West. Unfortunately, this particular form of scam can have devastating results on the victims.

The Daily Mirror[139] reports that sextortion gangs extortion teenagers by luring them into webcam sex acts using fake women's profiles. According to the article[140], at least four victims have committed suicide after webcam blackmailers tricked them into performing online sex acts.

One of the victims in this case felt prey to a cybercriminal from Cote d'Ivoire: here is an exchange between the British teenager and the Ivorian blackmailer as the Mirror put it:

> *One teenager stung by an Ivory Coast gang told his blackmailer after being online for just 100 minutes: I'd rather go and shoot myself, you f***ing trash making people do this.*
> *The coldhearted criminal replied: I thank you I want your money more I will share your video bye?*[141].

In his suicide note minutes after his exchange with the Ivorian cybercriminal, the victim wrote:

---

[138] Federal Bureau of Investigation. *What is Sextortion?* (2016, May 23). https://www.fbi.gov/video-repository/newss-what-is-sextortion/view (Accessed on 04/16/2021).
[139] Sommerlad, N. (2017, April 3). "Sextortion" gangs' extortion 30 teenagers a day by luring them into webcam sex acts using fake women's profiles. *Mirror*. https://www.mirror.co.uk/news/uk-news/cyber-sex-gangs-blackmail-30-9972341 (Accessed on 04/16/2021).
[140] Ibid.
[141] Ibid.

I was getting extorted by someone for £800 so they sent a video around of me and ruined my life". I am so sorry … but this is the only way out.[142]

The fact that the victims are from English-speaking countries and the criminals are from Cote d'Ivoire, a francophone country, is intriguing at first. It goes against the accepted idea that cybercriminals from Cote d'Ivoire tend to target people living in French-speaking countries, especially since this is not the only case on record. In fact, another case in which a teenager from Utah took his own life after being tricked into sexually acting on webcam occurred in 2017. Here again, the culprit(s) were from Cote d'Ivoire and in this case, the victim sent money to the criminals who asked for more money until Tevan Tobler[143], the victim, took his own life. The Tevan story

Here is how the Mirror uncovered in the Ivory Coast during their investigation: "The Daily Mirror went to Africa to find how this teenager and another Briton were driven to take their own lives by criminals in the Ivory Coast. We found police there struggling to cope with the rackets operating via a network of scammers, internet cafes and Western Union cash transfers. The National Crime Agency had 1,245 cases of "financially motivated webcam blackmail" reported to their Anti-Kidnap and Extortion Unit in 2016, up more than threefold in 2015. But experts believe the true figure could be 10 times higher. Some are ambushed as they browse social media, some are looking for love on dating sites and others are tricked by pop-up ads on porn websites. Roy Sinclair, from the police unit, said: "There is huge under-reporting of these kinds of offences, often because victims feel ashamed or embarrassed but of course criminals rely on that reaction to succeed." The tragic English teenager had killed himself after being lured into a Skype chat with a "pretty brunette". Police believe the victim, who we agreed not to name, was tricked into sexual activity in front of his webcam. The Ivorian extortionist, who set up the fake Skype profile, sent his victim a picture of the sex act, threatening to post it on YouTube and share it with Facebook friends and family. He also vowed to make the baseless claim that the teenager had been watching child-sex abuse videos at the time. He sent a link for a Western Union account and demanded £800. The youngster tried to send £350. But his bank blocked it, suspecting fraud. The same Ivorian Skype user had targeted another potential victim on Facebook, just five days earlier, posing as a 22-year-old Texan brunette. But pictures of "Daniella" had been stolen. Officers traced the Skype and fake Facebook accounts to the Ivory Coast, as well as two mobile phone numbers linked to a Western Union account used in the extortion bid. Ivorian Cybercrime police found the mobile numbers allegedly belonged to a man called Ouare Yaya. He is on the run but had withdrawn cash from Western Union branches. He was linked to a cashier called Kouadio Eoule, 33, accused of letting Yaya withdraw £164 sent by a victim. But our victim made no payments to the blackmailer, so any withdrawal could not be linked to his suicide. We visited Eoule in Maca jail in the business capital of Abidjan. He said: "If they don't find Yaya, I'll go to jail for 10 years. I am finished. "I had nothing to do with this. Tell his parents I didn't know anything." UK police said inquiries into the suicide were ongoing and they hope to extradite the blackmailer, if caught, to face up to 14 years in jail. But tough cybercrime laws introduced in the Ivory Coast in 2013 mean offenders face up to 20 years and £164,000 fines. The cruel scam is called "chantage" there and police are investigating links to a second British suicide, two in Italy, two in France and one in Canada. But these are deaths recorded in one country. Two other British victims have been linked to other countries. One Ivory Coast victim was a closet bisexual whose male blackmailers threatened to tell his wife. Another was a government minister in Mali. Côte d'Ivoire has overtaken Nigeria as the capital of cybercrime in Africa. Half the population live in poverty and cybercrooks earn thousands of pounds a month."

[143] Reavy, P. (2019, April 10). Utah family sharing sextortion suicide story likely saved some lives, police say. *Deseret News.* https://www.deseret.com/2019/4/10/20670612/utah-family-sharing-sextortion-suicide-story-likely-saved-

went viral in 2019 nationwide which helped uncover other cases in progress or having occurred in silence.

Investigators even learned about the story of a Texas Police Officer[144] who committed suicide after being victim of sextortion. Despite these relatively recent and few cases in which cybercriminals from a Francophone country target people in Anglophone countries, we maintain that most victims of cybercrimes involving criminals in Cote d'Ivoire are French-speaking people who in some cases, may reside in an English-speaking country like the United States.

It will be interesting to dissect the profile of the Ivorian cybercriminal as we will in this dissertation, to see if those who target English-speaking folks from Cote d'Ivoire are Ivorian citizens or Anglophones living in the country on a temporary or permanent basis. It is also critical to know the education background of the average cybercriminal operating from Cote d'Ivoire.

Recommendations

Sextortion is a dangerous scam whose consequences can easily lead to suicide among the victims as seen in the Tevan case in Utah and others. We think the Ivorian authorities should take this threat extremely seriously as it has the potential of snowballing within the cybercriminals' circles.

For now, it seems like sextortion coming out of Cote d'Ivoire and targeting westerners is small in comparison to other types of online scams. We believe that short of action, if this scam becomes a staple of Cote d'Ivoire in the eyes of the world, the country will greatly suffer in terms of reputation but also economically as everything coming out of the country will be seen suspiciously.

some-lives-police-say#davis-county-sheriffs-detective-john-peirce-works-in-his-office-at-the-davis-county-justice-center-in-farmington-on-monday-april-1-2019-peirce-worked-on-the-tevan-tobler-case (Accessed on 04/16/2021).

[144] Ibid.

Since some victims of sextortion commit suicides, each and every case of sextortion leading up to a suicide will automatically go viral around the world and people would want to know the geographic origin of this particular scam. We will even suggest to the authorities to set up a special task force to deal exclusively with these forms of cybercrimes that can provoke a loss of human life.

As we've said above, the urgency of now with regard to sextortion is proven by the unnecessary deaths of Tevan and other teenagers, victims of this inhumane form of cybercrime.

The reputation of Cote d'Ivoire and other African countries for that matter, who may be dealing with cybercrimes, should prompt all the stakeholders to join force and work closely with their western counterparts to stem the tide of the scourge of cybercrimes from Ivorian and African societies.

Far from us, the idea of underestimating the damages of other types of cybercrimes which sometimes lead to victims committing suicide too, the lives of young men, the future of humanity, are at stake. This should be taken seriously at the very top of the Ivorian Government./.

3-3-4: Spam

A spam is according to the Merriam-webster dictionary, an unsolicited usually commercial message (such as e-mails, text messages, or Internet postings) sent to many recipients or posted in many places.

Cote d'Ivoire is one of the top ten African countries were most of the spams such as unsolicited e-mails originate when it comes to the African continent.

Of the top 10 African countries where spam originates, Cote d'Ivoire is at number 7 according to the *Symantec/African Union report*[145] of 2016.

Country	Rank	Percentage within Africa	Incident Count
South-Africa	1	24%	271,700,021
Tunisia	2	14%	160,301,789
Egypt	3	7%	78,429,009
Kenya	4	7%	78,410,109
Nigeria	5	4%	50,491,804
Algeria	6	4%	50,253,534
Cote d'Ivoire	7	4%	47,632,285
Ghana	8	4%	43,938,441
Morocco	9	3%	32,197,294
Cameroon	10	2%	25,478,566

Figure2: Top 10 Source African Countries for Spam—2016. Source: Symantec/African Union.

As figure 2 shows, Cote d'Ivoire, Nigeria, and Ghana are among the top ten countries in Africa when it comes to spam. Once again, South-Africa and Tunisia lead the pack.

Cybercriminals operating in Cote d'Ivoire usually target French-speaking people both locally and abroad mainly in Europe (France, Belgium, Luxemburg, Switzerland).

Nevertheless, a certain percentage of spam e-mails targeting English-speaking countries like the United States originate from Cote d'Ivoire.

[145] Cybercrime and Cybersecurity: Trends in Africa. 2016. Symantec/African Union.

Here are a sample of these e-mails:

Spam E-mail 1:

From: Bahadur Reza Nobakhti bahadur_1i@yahoo.com
Date: Sat, Jan 12, 5:32 PM
Subj: Hello my dear

Hello my dear

May peace of our almighty god be unto you.

Greeting in the name of our almighty god I wish you and your family happy moments of life now and forever more amen.my name is mrs bahadur Reza Nobakhti ,69 years old from Dubai living in in Abidjan, cote d'lvoire, please, I do not have formal relationship with you but because of my present predicament and circumstances I am made to contact you. I have been suffering from cancer and have a short life to leave. I have made up my mind to donate my inheritance of 3.5million usd to the less privileged please help me to fulfill my last wish, please contact me here.

[reza_ba20@yahoo.com]

Please contact me in my personal email. [reza_ba20@yahoo.com]

I wait to hear from you.

Thanks

Mrs. bahadur Reza Nobakhti

Spam E-mail 2:

Date: Fri, 1 Jul 2016
From: Juliana Timothy mrsjulianatimothy@gmail.com
Reply-To: Juliana Timothy juliana_timothy@yahoo.co.jp
Subject: My Dear Beloved in Christ

My Dear Beloved in Christ

Greetings to you and your family. I am Mrs. Juliana Timothy A widow to late Mr. Johnson Timothy of Ivory Coast" I am 58 years old, my late Husband was a Director with the Construction Company here before his Sudden Death in this Country's present political Crisis 2013, but before his death, he Deposited the Sum of˙$4 Million US dollars with one of the Bank here in Ivory Coast with my name and I am suffering from pancreatic cancer, My condition is really bad and it is quite obvious that I won't live more than two months according to my doctors, and I have no Child who is going to take care of this Huge amount of Money, I am willing to donate the sum of $4,Million US dollars for you to help widows and the less privileged ones in the rural and urban

areas and to carry out charity works in your Country and around the World on my Behalf

Waiting for your Urgent Responds.
Remain blessed in the name of the Lord.
Yours in Christ.
Mrs. Juliana Timothy

It remains to be seen if the authors of these spam e-mails in English are Ivorians who speak some English or scammers from English-speaking countries operating from Cote d'Ivoire.

Over the past couple of years, Ivorian scammers have shifted from targeting Europeans to targeting Ivorians.

According to the Authority for the Regulation of Telecommunications in Cote d'Ivoire (ARTCI), 98 % of victims are Ivorians which has turned the once-popular scammers into pariahs.

3-3-5: Bots

The Oxford dictionary defines a bot as an autonomous program on a network (especially the Internet) that can interact with computer systems or users, especially one designed to respond or behave like a player in an adventure game.

The more practical definition of a bot is that it is a software that is designed to automate the kinds of tasks you would usually do on your own, like making a dinner reservation, adding an appointment to your calendar, or fetching and displaying information.

In recent years, malicious bots used to attack network systems like a denial-of-service (DOS) attack by a botnet or to commit click fraud. The use of botnets in denial-of-service (DOS) is well used in Africa including in Cote d'Ivoire.

Here are the top 10 African countries when it comes to malicious bots:

Country	Rank	Percentage within Africa	Incident count
Egypt	1	48%	6,778,893
Algeria	2	15%	2,117,402
Tunisia	3	6%	798,121
South Africa	4	5%	768,800
Morocco	5	4%	601,180
Nigeria	6	3%	488,416
Kenya	7	3%	435,032
Ghana	8	2%	282,776
Sudan	9	2%	258,914
Cote D'Ivoire	10	2%	247,672

Figure 3: Top 10 Source African Countries for Bots—2016 (Source: Symantec).

As the figure 3 shows, Egypt is where most of malicious bots originate in Africa, followed by Algeria. Cote d'Ivoire is number 10 with 2% of the total incident count on the continent. Nigeria and Ghana, the other two hotspots in West-Africa, are number 6 and number 8, respectively.

Once again, the "contribution" of west-African countries in bots attacks although not overwhelming, does however exist. As we will see later, in the case of Command & Control (C&C) servers, which are computers controlled by an attacker or cybercriminal used to send commands to systems compromised by malware and receive stolen data from a target network, Cote d'Ivoire ranks number one in Africa.

Botnets are armies of computers that have been compromised by online criminals, usually without the knowledge of the real owner, and remotely commanded to steal information, send spam, spread malware, or launch Distributed-Denial-of-Service (DDoS) attacks.

The *FBI* testified in 2014 to a U.S. Senate's subcommittee on the sheer scale of the botnet problem which sees 18 computers recruited by the hackers every second of every day:

> *The impact of this global cyber threat has been significant. According to industry estimates, botnets have caused over $9 billion in losses to U.S. victims and over $110 billion in losses globally. Approximately 500 million computers are infected globally each year, translating into 18 victims per second. Source: fbi.gov.*

In Cote d'Ivoire as in the rest of the world, the Botnet master can instruct the hijacked computers to send spam or to distribute malware.

A botnet also provides opportunities for hackers to steal personal and financial information, exfiltrating sensitive documents and monitoring keystrokes with the intention of grabbing passwords and breaking into bank accounts.

African businesses and especially financial institutions lose hundreds of millions of dollars each year to cybercriminals. Sometimes, the victim of Botnets is African while the cybercriminal behind the attack is outside of Africa.

In 2016, between March and April, the West-African nation of Liberia was massively attacked through a Distributed-Denial- of- Service (DDoS) that almost knocked out the entire country offline.

The criminal behind this attack was a British citizen operating in Peyia, Cyprus. According to *news reports*[146], Kaye the cybercriminal began carrying out intermittent Distributed Denial of Service (DDoS) attacks on the Liberian telecommunications provider Lonestar MTN in October 2015 using rented botnets and stressors./.

[146]Rogers, P. (2019, April 19). *British cybercriminal sentenced for disrupting Liberian telecoms provider*. Intelligent CIO Africa. https://www.intelligentcio.com/africa/2019/01/22/british-cybercriminal-sentenced-for-disrupting-liberian-telecoms-provider/ (Accessed on 1/23/2020). Details: "The 30-year-old expert hacker was hired by a senior official at Cellcom, a rival Liberian network provider, and paid a monthly retainer. From September 2016, Kaye used his own Mirai botnet, made up of a network of infected Dahua security cameras, to carry out consistent attacks on Lonestar. In November 2016, the traffic from Kaye's botnet was so high in volume that it disabled Internet access across Liberia. The attacks had a direct and significant impact on Lonestar's ability to provide services to its customers, resulting in revenue loss of tens of millions in US dollars as customers left the network. Remedial action taken by Lonestar to prevent the attacks incurred at around US$600,000. He has been sentenced to two years and eight months."

3-3-6: Cyber-Terrorism?

In Cote d'Ivoire, article 3 of the Ivorian penal code[147] speaks of the consequences of committing terrorist acts but does not define what is terrorism. To conceptualize "Cyberterrorism", it is essential to define terrorism in the real-world.

Unfortunately, there is no universal definition of terrorism both here in the United States and internationally; the many attempts by the United Nations to define terrorism have been so far unsuccessful due to the Organization of the Islamic Conference (OIC) which repeatedly vetoed the inclusion of the phrase *"arm struggle for liberation"* and *"self-determination"*[148].

Here in the States, we have three different definitions of terrorism depending on which organization does the work of defining it.

For the FBI, terrorism is "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives"[149].

[147] Article 3 of the Ivorian Penal Code states: "Is punished (...), anyone with the intention of cause a situation of terror or to intimidate the population, or to promote a religious political cause or ideological, or to force the government, organization or institution to initiate an initiative or act according to certain principles, commits or threatens to commit an act that: carries injury to life; cause of violence serious to people; causes serious damage to property, natural resources, to the environment or cultural heritage; put in danger the life of one or more people; creates a serious risk to health or safety of the public or any other party public ; exposes the public to a dangerous, radioactive or novice, a toxic product or an agent microbiological or other agent or toxin organic; interrupts, disrupts, damages, or destroys a system IT or service provision directly linked to an infrastructure of communication, banking and financial, transport systems public or key infrastructure; disrupts the provision of services emergency services such as the police, civil protection and medical services; endangers public safety or national security; creates or is likely to create a crisis situation within populations or insurgency general".

[148] Human Rights Voices. UN 101: There is no UN definition of terrorism. http://www.eyeontheun.org/facts.asp?1=1&p=61 (Accessed on 10/14/19).

[149] National Institute of Justice (2017). Terrorism. https://www.nij.gov/topics/crime/terrorism/Pages/welcome.aspx (Accessed on 10/12/2019)

The CIA defines terrorism under Title 22 of the US Code, Section 2656f(d) this way: "The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents".[150]

On the other hand, the Department of Defense (DOD), defines terrorism as: "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological"[151].

This divergence in the definition of terrorism within the intelligence community proves that defining Cyberterrorism is harder if not impossible to do.

The term "Cyberterrorism" was first coined by Barry Collin while working at Palo Alto's Institute for Security and Intelligence in the 1980s who defined it as *"the convergence of terror and cyberspace"*[152].

This simple definition lacks specifics as to what kind of terror takes place in Cyberspace. Does the "*threat of unlawful violence*" as defined in the D.O.D definition of terrorism applies to the virtual world? Practically, it will be difficult to instill fear in the general (or a particular segment) of the population through a 'virtual threat' as noted by Janine Kremling and Amanda Parker in their book *"Cyberspace, Cybersecurity and Cybercrime".*[153]

In the academic world, some experts like Marjie T. Britz, Professor of criminal justice at Clemson University tentatively defines "cyberterrorism" as "the premeditated, methodological, and ideologically motivated dissemination of information, facilitation of communication, or attack

[150] 22 U.S Code Sec 2656f.
[151] Terrorism [definition]. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=5407
[152] Janine Kremling, Amanda M. Sharp Parker. "Cyberspace, Cybersecurity and Cybercrime." Los Angeles, USA: SAGE Publications Inc. 2017 P. 128.
[153] Ibid.

against digital information, computer systems, and/or computer programs which requires advanced planning and is intended to result in social, financial, physical, or psychological harm to noncombatant targets and audiences; or any dissemination of information which is designed to facilitate such actions"[154].

The issue with such definition of "Cyberterrorism" is that no known terrorist groups have the infrastructure, technical know-how and the manpower to undertake such actions in Cyberspace. On the other hand, this definition of "Cyberterrorism" could easily be applied to "Cyberwarfare" undertaken by either Nation-States or State-Sponsored Groups (SSG).

Most known terrorist groups use the internet more as a Public Relations (PR) stunt and recruitment tool than to attack critical infrastructures. Even the web defacement done by ISIS on the Central Command (CentCom) does not meet the criteria of "Cyberterror".

Moreover, hacker groups do deface websites for "fun" as seen in the case of the *Swedish Hacker Group*[155] which defaced the CIA website in 1996.

The Sony attack of 2014 by the "Guardians of Peace" (GOP) from North Korea is an example of Cyberwarfare by a Nation-State. It clearly shows that Nation-States can have two arms to perpetrate Cyberattacks on hostile nations:

a- <u>State arm</u>:

"Just as nuclear was the strategic warfare of the industrial era, cyberwarfare has become the strategic war of the information era," says U.S. Secretary of Defense Leon Panetta.

[154] Marjie T. Britz. "Computer Forensics and Cybercrime: An Introduction." Pearson. Third Edition.
[155] Grabosky, P. (2015). *Cybercrime (Keynotes Criminology Criminal Justice)* (1st ed.). Oxford University Press.

The formation of the *General Reconnaissance Bureau*[156] (GRB) with *Cyberunits 91* and *121* in North Korea is one such example of an official state arm for Cyberwarfare. In practice, these official arm units do not directly do the attacks. They are left to a state-sponsored actor like the *Guardians of Peace* (GOP).

b- **State-Sponsored Groups**:

The Sony Attack revealed for the first time the existence of the "Guardians of Peace" or GOP to the world. They released documents from the Sony Computer Network over several weeks which raised the issue of foreign obstruction of *First Amendment rights in the United States*[157].

The Cyberattacks against Estonia in April 2007 by a Kremlin-backed group *Nashi e* proves once again that Nation-States like North Korea, Russia, Iran prefers to lean on "subsidiaries" for some Cyberattacks.

The legal conundrum in this case is to be able to trace these attacks back to the state that sponsored them.

These states can always deny any wrongdoing. To sum up, we believe there is no such thing as Cyberterrorism but rather Cyberwarfare with many tentacles.

Terrorism is a foreign notion to most Ivorians until recently when terrorist groups perpetrated a number of attacks on Ivorian soil. The perpetrators were all foreigners from neighboring countries, Mali, and Burkina-Faso.

It is thus unlikely to have cybercriminals engage in "cyber-terrorism" either domestically or internationally./.

[156] Haggard, S., & Lindsey, J. R. (2015). North Korea and the Sony hack: Exporting instability through Cyberspace. *Asia Pacific Issues from the East-West Center, 117, 1-8*

[157] Janine Kremling, Amanda M. Sharp Parker. "Cyberspace, Cybersecurity and Cybercrime." (Supra note 83).

2.3: Cybercrimes and the Routine Activity Theory

In order to compare Cybercrimes to the Routine Activity Theory (RAT) developed by Cohen and Felson in 1979, it is important to define Cybercrimes. Although there is no legal definition of Cybercrimes, a working definition was offered by *Thomas and Loader*[158], who conceptualize cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.'

Although this definition is helpful in centering Cybercrimes around computers or 'virtual space', it does not consider the necessary distinction between crimes committed online. Wall[159] tried a legal definition of Cybercrimes by subdividing them in four categories:

1- *Cyber-Trespass*: crossing boundaries into other people's property and/or causing damage, e.g., hacking, defacement, viruses.
2- *Cyber-Deceptions and thefts*: stealing (money, property), e.g., credit card fraud, intellectual property violations (a.k.a. 'piracy').
3- *Cyber-Pornography*: activities that breach laws on obscenity and decency.
4- *Cyber-Violence*: doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, e.g., hate speech, stalking.

Not everyone agrees with that classification either; this is the case with Majid Yar[160] who argued that it does little in the way of isolating what might be qualitatively *different* or *new* about such

[158] Thomas, D. and Loader, B. (two thousand). Introduction – Cybercrime: Law enforcement, security, and surveillance in the information age. In D. Thomas and B. Loader (eds) Cybercrime: Law enforcement, security, and surveillance in the information age. London: Routledge
[159]Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) Crime and the internet. London: Routledge.
[160] Majid Yar. The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology 2005; two; 407. http://euc.sagepub.com/cgi/content/abstract/2/4/407 (Accessed on 11/1/19).

offences and their commission when considered from a perspective that looks beyond a limited legalistic framework.

For some criminologists, the novelty of cybercrimes resides in the *structure* in which the crime takes place or shape which is known as "Cyberspace".

For Majid Yar[161] it is the supposedly novel socio-interactional features of the cyberspace environment (primarily the collapse of spatial–temporal barriers, many-to-many connectivity, and the anonymity and plasticity of online identity) that make possible new forms and patterns of illicit activity. This tentative definition by Majid is at best partial, for it does not consider the use of cyberspace to further "terrestrial crimes" in the virtual world.

Thus, the need to define cybercrimes as all-encompassing of "old" and "new" types of crimes. In other words, cyberspace is both a tool to commit 'terrestrial crimes' by enhancing its means, but also to commit 'new' crimes specific to the nature of cyberspace.

This double possibility of the virtual environment is what makes cybercrimes a novelty. One important question is to ask if the novelty of cybercrimes, as defined above allows its comparison to the Routine Activity Theory (RAT) which involves having motivated offenders, suitable targets, and the absence of a capable guardian.

[161] Majid Yar. The Novelty of 'Cybercrime'.(Supra note 160) P.105.

2.3.1: Motivated Offenders

The advent of cyberspace has seen the migration of everyday activities into the "Cybersphere". Businesses, Governments, and non-profit organizations have gradually migrated their activities online to enhance productivity, save money and make life "easier" for their personnel. Individuals too, have followed suit either to communicate with each other, shop, or for entertainment purposes.

According to one estimate, there are as of July 2019, *4.33 billion*[162] internet users around the world. Most of them use the internet for their daily activities (email, shopping, learning, entertaining etc.).

The obvious consequence of such number of online users is to have potential offenders in their midst.

As *Peter Grabosky*[163] argued, the supply of motivated offenders is in part a reflection of the number of individuals with access to the tools of cybercrime. Having more internet users increases the risk of having motivated offenders roaming cyberspace looking for their next "fresh meat" to steal from.

The irony here is that places like Africa that have less than 20 percent internet users, harbor more motivated offenders than places like the West when compared to the online population of these places. The types of Cybercrimes committed are as varied as the number of Cybercriminals.

At first, we had script kiddies (hacking) who hacked computer systems for the thrill of it or to make a statement about their prowess. Today, we have sexual predators roaming internet to prey on young internet users (cyber-pornography); some criminals are after your credit card details for

[162] https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed on 11/05/19).
[163] Grabosky, P. (2015). *Cybercrime*. (Supra note 155) P.103.

financial gain, while others deface websites of institutions they abhor for political, social, and environmental reasons.

In that sense, one can argue that the first condition-motivated offenders- of the Routine Activity Theory is met.

2.3.2: Suitable Targets

The presence of suitable targets in cyberspace is as Professor *Grabosky*[164] put it, a function of the take up of digital technology. In other words, the more people use the internet, the more suitable targets become available.

From a Routine Activity Theory perspective, we are going to analyze what Professor *Majid Yar*[165] called its four-fold constituent properties – value, inertia, visibility and accessibility, or VIVA.

a- Value:

In cyberspace, the value given to potential suitable targets varies according to the aim of who is doing the targeting. It is as Professor *Majid*[166] argued, a function of the various purposes the offender may have in mind for the target once appropriated – whether it is for personal pleasure, for sale, for use in the commission of a further offence or other non-criminal activity, and so on.

An offender who is interested by a financial gain will be targeting the personal and credit card information of online shoppers that he values more than anything else. A sexual predator will be looking for young people who venture online without paying attention to whom they are talking to; for this sexual predator, online pornography has more value than anything else.

[164] Grabosky, P. (2015). *Cybercrime*. (Supra note 155) P.103.
[165] Majid Yar. The Novelty of 'Cybercrime'. (Supra note 160) P.105.
[166] Ibid.

On the other hand, a spy will attach more value to state secrets on computer systems. Equally, the target will vary according to the shifting valuations attached socially and economically to particular goods at particular times – factors such as scarcity and fashion will play a role in setting the value placed upon the target by offenders and others, according to *Marcus Felson*[167]. The availability of valuable targets in cyberspace derives from the fact that we depend more and more on computers.

As *Grabosky*[168] noted, institutions of critical infrastructure such as electric power, water supply, telecommunications, air traffic control and banking are all networked.

Nowadays, we are constantly using social medias like Facebook to send and receive photos, Twitter, or YouTube to watch videos or ATMs to withdraw money electronically.

This *"digital dependency"* creates opportunities for offenders everywhere.

b- Inertia

The term inertia as proposed by *Marcus Felson*[169] refers to the physical properties of objects or persons that might offer varying degrees of resistance to effective predation: a large and heavy object is relatively difficult to remove, and a large and heavy person is relatively difficult to assault.

If that assertation is true for "terrestrial objects", the opposite is true in cyberspace because digitized information in cyberspace is 'weightless' as Majid Yar correctly pointed it out.

The obvious consequence is that 'terrestrial objects' due to their physical properties can offer some form of resistance to predation while digital information cannot offer a resistance based on

[167] Felson, M. (1998). Crime and everyday life, 2nd edn. Thousand Oaks, CA: Pine Forge Press.
[168] Grabosky, P. (2015). *Cybercrime.* (Supra note 155) P.103.
[169] Felson, M. (1998). Crime and everyday life. (Supra note 167).109.

its weight. The data can be downloaded many times over or even replicated infinitely in the case of media 'piracy' as noted by *Grabosky and Smith*[170].

That being said, the digital information is not 100% devoid of 'weight' as argued by *Majid Yar*[171] who thinks that even informational goods retain inertial properties to some degree.

He demonstrates his assertion by noting that the volume of data (e.g., file size) impacts upon the portability of the target; also, the technological specification of the tools (the computer system) used by the 'information thief' will place limits upon the appropriation of large informational targets. The obvious conclusion is that informational goods are not absolutely weightless.

c- Visibility

Visibility refers to the visibility of the objects an offender wishes to steal. For example, a wallet left unattended in a public place is visible to enough people including those who may wish to steal it. Thus, the obvious question is to know how online targets offer some form of visibility to potential predators.

RAT postulates a positive correlation between target visibility and suitability. For *Majid Yar*[172], conceptualizing visibility in cyberspace presents a difficult issue, given that the social raison d'etre of technologies such as the Internet is to invite and facilitate communication and interaction, making visibility a ubiquitous feature of virtually present entities.

The structure of cyberspace is such that users and 'informational goods' are visible to anyone who wish to establish a "virtual contact", to the exception of closed networks like the intranet or Virtual

[170] Grabosky, P. and Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies.
[171] Majid Yar. The Novelty of 'Cybercrime'. (Supra note 160) P.105.
[172] Ibid.

Private Networks (VPN). In the terrestrial world, physical barriers prevent an outsider to pierce the veil of what is going on inside the physical structure.

For example, a warehouse offers little visibility to the outside world regarding the goods it contains.

On the other hand, a website, a social media page or un email can easily be visible to anyone who is interested in them. In the end, the visibility in cyberspace is ubiquitous while the visibility in the terrestrial world is limited by the distances.

Entities and human beings present in cyberspace present a visibility that makes them suitable targets for potential cyber-offenders.

d- Accessibility

Marcus Felson[173] defines accessibility as the 'ability of an offender to get to the target and then get away from the scene of a crime'. One would assume that the easier the accessibility, the greater the suitability of the target. Are online targets easily accessible?

In response to *Beavon et al. (1994)*[174] who identify the number of physical routes through which a target is accessible as a significant variable in the distribution of property crimes, *Majid Yar*[175] noted that, given that traversal of cyberspace is 'non-linear', and it is possible to jump from any one point to any other point within the space, it is difficult to conceive targets as differentiated according to the likelihood of accessibility to a potential offender in this manner. He added that

[173] Felson, M. (1998). Crime and everyday life. (Supra note 167) P.109.
[174] Beavon, D., Brantingham, P. L. and Brantingham, P. J. (1994). The influence of street networks on the patterning of property offenses. In R. V. Clarke (ed.) Crime prevention studies, Vol II, 149–63. New York: Willow Tree Press.
[175] Majid Yar. The Novelty of 'Cybercrime'. (Supra note 160) P.105.

similarly, the availability of egress from the 'scene of the crime' is difficult to operationalize as a discriminating variable when applied to cyberspace.

The accessibility in cyberspace is contingent upon the "cyber-guardrails" put in place to make it harder for potential cyber-offenders to access a website for example, as in the real world.

As *Grabosky*[176] correctly pointed out, Institutions of critical infrastructure such as electric power, water supply, telecommunications, air traffic control and banking are all networked. These online networks use tools such as firewalls, antivirus software, blocking and filtering technologies, encryption, to reduce accessibility to potential offenders and can be conceived as the virtual counterparts of lock-picks, glasscutters, and crowbars.

In sum, the suitable targets defined for the terrestrial world can be transpose in the virtual world as the value, the inertia, the visibility, and the accessibility of the target proven in the real world, do exist in the virtual world.

2.3.3: Absence of a Capable Guardian

The last requirement of the Routine Activity Theory is the absence of a capable guardian. In the terrestrial world, a guardian can be anybody who as *Grabosky*[177] noted, "mind the store". A security guard, parents, people walking on the street or something like a burglar alarm or CCTV Cameras in offices and stores.

In cyberspace we have private and informal social guardians: these range from in-house network administrators and systems security staff who watch over their electronic charges, through trade organizations oriented to self-regulation, to 'ordinary online citizens' who exercise a range of

[176] Grabosky, P. (2015). *Cybercrime*. (Supra note 155) P.103.
[177] Ibid.

informal social controls over each other's behavior (such as the practice of 'flaming' those who breach social norms on offensive behavior in chat rooms as pointed out by *Smith et al*[178].

Cohen and Felson[179] put an emphasis on 'ordinary citizens' going about their routine activities. Guardianship after all refers to 'the capability of persons and objects to prevent crime from occurring' said *Tseloni et al*[180].

The basic function of a guardian as added by Grabosky is to exercise surveillance over people or places for the purpose of preventing crime or to enable a prompt response in the event that a crime is committed. As in the terrestrial world, the presence of a capable guardian during the commission of a crime in cyberspace is at best illusory. *Felson*[181] noted that the police 'are very unlikely to be on the spot when a crime occurs'.

Majid Yar[182] agrees by stating that in terms of formal social guardianship, maintaining such co-presence is well-nigh impossible, given the ease of offender mobility and the temporal irregularity of cyber-spatial activities (it would require a ubiquitous, round-the-clock police presence on the Internet). *Grabosky* goes a step further by stating this:

> *Of course, would-be guardians do not always function the way they should. Parents may be lacking in computer literacy or may be careless in supervising their children. Computer users may be nonchalant about the sites they visit and about the e-mail attachments that they open. They may use passwords that are easy to guess, or they may even leave them in plain view. They may fail to install or to update their virus detection software.*

---

[178] Smith, C., McLaughlin, M. and Osborne, K. (1997). Conduct control on Usenet. Journal of Computer-Mediated Communication 2; URL (consulted 13 May 2005): http://www.ascusc.org/jcmc/vol2/issue4/smith.html.
[179] Cohen, L. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review 44, 588–608.
[180] Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004). Burglary victimization in England and Wales, the Unites States and The Netherlands: A cross-national comparative test of routine activities and lifestyle theories. British Journal of Criminology 44, 66–91.
[181] Felson, M. (1998). Crime and everyday life. (Supra note 167) P.109.
[182] Majid Yar. The Novelty of 'Cybercrime'. (Supra note 160) P.105.

In sum, the Routine Activity Theory's concept of capable guardianship is transposable to cyberspace, even if the nature of cyberspace restricts its implementation as in the guardianship in the terrestrial world.

In the end, cybercrimes like crimes committed in the terrestrial world can be conceptualized through the Routine Activity Theory (RAT) because both type of crimes follow similar patterns./.

3-4: Profile of the Ivorian cybercriminal

The Ivorian population is incredibly young with a median age of 18.9 years[183], according to the United Nations data. 51.3 % of the Ivorian population lives in urban area with a population density of 215 people per mi2 and a life expectancy of 58.75 years, according to the United Nations.

The total population is roughly 27.000.000 people. The literacy rate in Cote d'Ivoire, according to the United Nations Educational, Scientific and Cultural Organization or UNESCO[184], is 47.17 %. With such a young population, no one is surprised or should be surprised by the rapid development of cybercriminality in Cote d'Ivoire.

In the country, cybercriminals are known as "Brouteurs." The term "Brouteurs"[185] is an Ivorian expression for crooks who do not have to try hard to make easy money, they only have to stoop like sheep to "graze on green grass."

[183] United Nations. (2021). *Côte d'Ivoire Population (2021) - Worldometer*. https://www.worldometers.info/world-population/cote-d-ivoire-population/ (Accessed on 04/20/2021).
[184]UNESCO uis. *Côte d'Ivoire* (2020). http://uis.unesco.org/en/country/ci (Accessed on 04/20/2021).
[185] Net Offensive. Who are the Internet grazers and crooks? (2020, July 27). https://www.netoffensive.blog/e-reputation/donnees-personnelles/sextorsion/arnaque-webcam/les-brouteurs/ (Accessed on 04/22/2021).

According to Professor and Researcher Anon N'Guessan[186] of the Felix Houphouet Boigny University in Abidjan, the scourge of cybercriminality is present among Ivorian students, both in high school and in college.

His report[187] revealed that the techniques used are those usually practiced by most cybercriminals: inheritance scams, extortion, feelings scams, the use of false documents (bank cards, checks ...).

As for the explanatory factors behind this phenomenon, Professor Anon cited "at the foreground financial problems and at the background graduate unemployment, lack of parental authority, and the proliferation of cybercafés. It is noted as major impacts, deficient performance in class, dropping out, and adoption of behaviours that could lead to committing murder to satisfy their material greed."

In Cote d'Ivoire, young people are easily swayed by what is called "La mode" or the trend irrespective of what that trend is. A few decades ago, a deadly trend took place among students which consisted of crossing the street, boulevard by closing your eyes. De facto, these students would cross streets blindly.

As one could expect, many students died from this so-called trend. The scourge of cybercriminality wreaking havoc among the Ivorian youth, can be traced back to the consequences of the civil wars that occurred in 2002 and 2011. Those civil wars have created a new class of rich young people who joined the rebellion earlier on and engaged in all kinds of traffics (cocoa, coffee, diamond, gold etc.).

[186]N'Guessan, A. (2014, November 28). The practice of Cybercrime in schools and University in Cote d'Ivoire. Case of pupils and students in the District of Abidjan. https://paperity.org/p/59114531/la-pratique-de-la-cybercriminalite-en-milieux-scolaire-et-universitaire-de-cote-divoire (Accessed on 04/22/2021).

[187] Ibid.

Seeing these young people showing off their riches in towns and cities, other young people who according to Professor Anon, come from underprivileged backgrounds of the Ivorian economic capital, decided to become rich here and now.

"We find among them students, pupils, unemployed, and even some young workers who want to supplement their end of the month"[188], he added. The easiest route these youths found, was scamming the "white man."

Here[189] is the description of the Ivorian cybercriminal done by an Ivorian journalist on his personal blog, translated and reproduced…verbatim:

With these findings, it is fair to say that the perpetrators of sextortion in Cote d'Ivoire are highly likely Ivorian nationals with a certain degree of education since English is taught from high school to the University.

---

[188] N'Guessan, A. (2014, November 28). The practice of Cybercrime in schools and University in Cote d'Ivoire. Case of pupils and students in the District of Abidjan. (Supra note 117).115.

[189] Idriss, F. B. (2017, October 14). Cyber-fraud, the 501 blows of Ivorian grazers. https://visavis.mondoblog.org/cyber-delinquance-les-501-coups-des-brouteurs-ivoiriens/ (Accessed on 04/22/2021). Cyber-scam, the 501 shots of Ivorian grazers the scam, in a new form of cybercrime in Ivory Coast. A danger for young people who abandon training in favor of delinquency. My investigation ...

Face wrapped in a solar pair, the shimmering wrist of a luxury watch, the 3G cell phone taped to the ear, a diamond buckle on the left ear, shiny jewels on the neck, brand new clothes out of the box. 'a shop of claws of the Plateau (Abidjan)' 'massages" the body of Alfred S. This Saturday, sitting in a sparkling "Mercedes E-Class" with an iPad on board, the barely 17-year-old is considered a formidable "savvy" internet con artist. He has nothing to envy of successful businessmen. Even less to be regretted as his schoolmates he abandoned, three years in third grade, continue their studies. He surfs in supermarkets in the economic capital of Abidjan. Alfred S. exposes his way of "living his life". A life to fiddle with all day long on the keyboard of his computer. "I decided to take charge of myself. I no longer depend on my parents. Through the internet, I own a car, an internet cafe and two arcades. Besides, I live in my apartment, "rejoices the grazer whom his" admirers "affectionately call" the billionaire "in the group. A nickname that sticks to his skin. For this barely 17-year-old boy, school is just a steppingstone to success in life. Because "you don't need to do a letter class to eat a white man," Alfred S. had, he reveals, his first million CFA francs at the age of 17. Today, it employs around ten people who work daily in its small businesses called "training schools". In his stable, he teaches adolescents of his age the worst and most malicious methods to cheat honest people on the web. These "schoolchildren" are known as "RL" "Launcher Robot" while he is the "Chairman". Crazy launchers, they can transfer more than 10,000 messages every day to the mailboxes of European individuals who, it seems, are the most profitable targets. From 8 a.m. to 10 p.m., these "children" who have dropped out of school storm the chairman's apartment in the Cocody-Les Vallons sub-district. There, a space has been created. These crooks commonly known as "grazers" are at the feet of the master who teaches them the basics of the scam.

The involvement of native English speakers does not have to be dismissed. Either way, Cote d'Ivoire is unfortunately a hub of cybercrimes in West-Africa.

We will later analyze the legal apparatus put in place by the Ivorian Authorities to fight this disturbing scourge enveloping the Ivorian youth, educated or otherwise.

Recommendations

The first recommendation one can give to the stakeholders of the cybercrime scourge in Cote d'Ivoire, would be to take it seriously because it has worldwide implications. This is not a matter whose impact lies solely within the borders of Cote d'Ivoire.

The Tevan story and many others that happened in foreign countries means that the entire world has a stake in what is taking place in Cote d'Ivoire with regard to cybercrimes.

As many investigations by local researchers have demonstrated, the issue of cybercriminality within the Ivorian youth is a multi-prong issue that touch the social, economic, and the prospects of the youth.

The Ivorian government must redouble its efforts in terms of awareness campaigns on campuses across the nation to discourage those who are committing crimes in cyberspace and those young people who want to join in.

One thing that will certainly get the attention of all the stakeholders would be for the government to inform the nation and especially the youth that they could be extradited to foreign countries to face justice if they commit crimes online that lead to deaths abroad like in the case of Tevan in Utah, here in the United States. We believe that the prospect of facing the harsh conditions of a justice system like the one we have here in the states would make those kids think twice before committing cybercrimes.

The problem with this recommendation is that Cote d'Ivoire does not have extradition treaties with most countries and also, one must acknowledge the recent trends in cybercrimes that come from the fact the vast majority of the victims are now Ivorian citizens. One way to resolve those aspects would be to focus the awareness campaigns by talking about victims like Tevan with pictures, testimonies of those who knew him etc.

We think that such campaigns showing the faces of the victims of cybercrimes will certainly make an impact on the youth but also their parents and the country at large./.

3-5: Targets of cybercrimes

The victims of cybercrimes committed from Cote d'Ivoire are usually unsuspecting people who are either looking for companionship, or to make money quickly who can be classified as greedy.

A cybercriminal who anonymously testified[190] about their methods said: "we create several e-mail addresses on different browsers: Facebook, Yahoo, Google, AOL, Windows live, Msn Messenger… With these boxes, we go looking for e-mail addresses that will allow us to correspond with whites or any other person outside of Côte d'Ivoire." The fact that targets of cybercriminals are "white men or women" is not fortuitous.

The first and most important reason is that cybercriminals believe that white people are all rich. The second reason which can be seen as their "moral justification" is that they consider the white man as having "exploited" or continue to exploit African countries.

They see themselves as the modern-day robin hoods who are out to "avenge" the victims of colonization. The irony with that "moral" justification is that most cybercriminals who make it big indulge in pleasures and luxury[191].

According to net offensive[192], the modus operandi of cybercriminals operating either from Cote d'Ivoire or Nigeria for that matter, is simple: "the scammer begins by spotting a target on social networks: a person who has experienced one or more love disappointments and who can easily be seduced."

Here is a brief description of the modus operandi as described by Net Offensive:

[190] Idriss, F. B. (2017, October 14). Cyber-fraud, the 501 blows of Ivorian grazers. (Supra note 189) P.116.
[191] Ibid.
[192] Net Offensive. Who are the Internet grazers and crooks? (Supra note 185) P.115.

> *Once the victim is identified, the grazer sends a friend request via a fake profile. The profile picture has it all: a sexy young woman, smiling and… single! The victim bites on the hook and the new contact, behind which the grazer is hiding, soon initiates the discussion. The speech is broken: the young woman says she lives in France and is looking for love. To appear more believable, photos of family or friends are sometimes sent. It is understood that in most cases these are photomontages. The profile is usually created by collecting photos of an attractive but totally unknown person on Instagram or other social networks like Facebook./.*

In recent years, the vast majority of victims are Ivorian citizens due to the tight cooperation between Cote d'Ivoire and Europe, France.

This turnaround has made the Ivorian public leary of those who were seen not long ago as "stars" and "heroes." In fact, a hostility has developed against these cybercriminals. The public outcry also pushed the government to go after them more harshly which had the effect to send some criminals running for cover in neighbouring countries like Benin and Togo.

Nevertheless, according to mondoblog[193], the Ivorian Police are complicit of cybercrimes committed by Ivorian cybercriminals. In fact, mondoblog based on its investigations, affirms that some elements of the cyber-police are themselves complicit in cybercrimes and tend to encourage it through networks of cybercriminals.

A pupil cybercriminal ("Papi dollar") told the investigator that he no longer withdraws his money from money transfer companies because Forensic officers roam their places very often and are quick to arrest you when they catch you.

And once in their hands, you have the choice between giving them a share of your loot or ending up with the judicial police. Sometimes these agents take all your money. Recently, a police officer

[193] Idriss, F. B. (2017, October 14). Cyber-fraud, the 501 blows of Ivorian grazers. (Supra note 189) P.116.

snatched 2,500 euros (around 1,637,500 FCFA) from me while I was leaving a Western Union agency in Cocody[194].

Another link in this ecosystem of criminals preying on unsuspecting victims both locally and abroad, are the parents of those cybercriminals who directly benefit from the loot of their children. In his testimony[195], "papi dollar" affirms that his father withdraws the money from money transfer agencies.

It is also important to note that there are accomplices within the money transfer and the banking systems./.

Recommendations

The fact that many Ivorian citizens are victims of cybercrimes on top of westerners, is a wake-up call for the Ivorian government to strengthen its fight against cybercrimes.

In order to efficiently prosecute and win this fight, it is of utmost importance to making sure that those who are leading the fight inside the government are dedicated civil servants and Law enforcement officers.

Corruption at every level of society is such that, it would be illusory to envision a quick turnaround in the fight against the scourge of cybercrimes in Cote d'Ivoire. So, once again, the Ivorian government should put a maximum pressure on the national agencies leading the fight to stamp out the most corrupt elements.

On the other hand, money transfer companies and the banking system should also be asked to investigate and remove those employees who are complicit of cybercrimes in Cote d'Ivoire. The

[194]Idriss, F. B. (2017, October 14). Cyber-fraud, the 501 blows of Ivorian grazers .(Supra note 189) P.116.
[195] Ibid.

legal apparatus put in place by the government to fight cybercriminality should be enforced effectively by the Ivorian Authorities through the justice system.

Cote d'Ivoire should also request assistance from countries and Institutions that are a step ahead in the fight against cybercrimes, to fund and train more skilled cybersecurity specialists. To potential victims everywhere, when it seems too good to be true, then it is.

Never trust anyone you met online who is asking you money in an emergency situation. Under no circumstances, should anyone perform sexual acts on webcam for someone they do not know personally even if she pretends to be Miss Universe./.

3-6: Impact of cybercrimes in Cote d'Ivoire

3-6-1: Economic impact

One of the severe impacts of cybercrimes in Cote d'Ivoire, is the economic development of the country. According to J.J. Bogui[196], around the year 2008, many Internet Service Providers (ISPs) noticed the vast number of spams originating from Cote d'Ivoire which even prompted many African countries to ask the Ivorian Authorities to solve the issue or else.

Cote d'Ivoire is now "blacklisted" by most European countries, the United and India as being one of the epicentres of cybercrimes in West-Africa. Many Ivorian businesspeople have complained of not being able to do business digitally once their partners locate them as being from Cote d'Ivoire, according to J. Bogui[197].

The issue at hand here is the lack of trust by international partners regarding proposals made digitally from Cote d'Ivoire. Some businesspeople revealed that they are sometimes "insulted"[198] by their correspondents when they discover that the message had originated from Cote d'Ivoire. This situation has led major international fintech companies like PayPal Inc and Stripe Inc to forbid any transactions from all African countries including Cote d'Ivoire.

Fortunately, going forward, Flutterwave, a Nigerian and US-based fintech company has announced in March 2021 that it has partnered with PayPal to enable African merchants to easily accept payments from PayPal users globally through Flutter wave's platform.

[196] Bogui, J. (2010). Cybercrime, a threat to development: Internet frauds in Côte d'Ivoire. Contemporary Africa, 2 (2), 155-170. https://doi.org/10.3917/afco.234.0155 (Accessed on 04/29/2021).
[197] Ibid.
[198] Ibid.

The reputation of Cote d'Ivoire around the world has been badly hit by the scourge of cybercriminality and it will take years of arduous public relations stunt from the Ivorian government to restore the good name of the country abroad. In order to do that, the fight against cybercrimes must be strong and merciless./.

3-6-2: Social impact

The social impact of cybercrimes is varied according to the place where it is happening. The social impact of cybercrimes in the West is different from the impact it has on developing countries such as African countries.

While cybercrimes in the news can encourage people to "protect" themselves online with security tools in the former, the situation is completely different in the latter; most third world countries have little or no security measures for people using computers.

The immediate consequence of such situation is to deter some people from using the internet all together for their everyday activities in developing countries. Cybercrimes both in the West and in developing countries can have *cultural, psychological, and interpersonal impacts*[199].

Aiken et al[200]. argued that cybercrime explodes the notion of social impact, because, quite frankly, of the nature of the environment in which it occurs. A *Symantec* report reveals that nearly two thirds of adults globally have been a victim of some kind of cybercrime (65%).

Cybercrime hotspots where adults have experienced cybercrime include China (83%) Brazil/India (76%) USA (73%). Even though people are paralyzed by powerlessness and frozen by fear, most people in the West still use the internet for their daily activities as the report revealed.

This attitude vis-à-vis the threat of cybercrime to online users in most developed countries is described by associate professor of psychology at Loyola Marymount University, Joseph LaBrie PhD, as '*learned helplessness*'.

[199] Mary Aiken, Ciaran Mc Mahon, Ciaran Haughton, Laura O'Neill & Edward O'Carroll (2015): A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online, Contemporary Social Science, DOI: 10.1080/21582041.2015.1117648. http://dx.doi.org/10.1080/21582041.2015.1117648.
[200] Ibid.

He argued that "Learned helplessness" happens when people do not know enough about a problem or do not know how to resolve it. It is like getting ripped off at a garage – if you do not know enough about cars, you do not argue with the mechanic. People just accept situations, even if it feels bad.

In reality, not everyone accepts this learned helplessness as argued by Professor LaBrie. A cross-section of the population is terrified of the internet due to publicized cyberattacks like the one on Target in 2013 or Sony in 2014.

Thus, some internet users avoid shopping online or downloading movies, music for entertainment purposes. They go to the mall to get these things, just like some people avoid traveling by air for fear of plane crash; a cybercrime case that makes it into the news is like a plane accident: it is spoken of in such dramatic fashion that it captures the public imagination.

In turn, a tendency to demonize the internet for every crime that takes hold is growing at an alarming rate.

As *David Wall*[201] pointed out, when politicians, police, interest groups, policymakers and others are pressed for comments about dramatic crimes or events that have captured the public imagination, their immediate response nowadays, seems to be to point to the internet as a causal factor. The reality can be tricky. Sometimes, the internet links are found to be *circumstantial, secondary*[202].

[201] David S. Wall. Cybercrime and The Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime (Revised Feb. 2011). Criminology, SASS, Durham University, 32 Old Elvet, Durham.
[202] Ibid.

The issue here is that the first allegations made by public officials are rarely retracted. Another impact of cybercrimes is to create a digital panopticon as argued by *Paul Day*[203]. He notes that internet users live in a goldfish bowl where every movement is watched by anyone who is interested. The idea of the panopticon was put forth by the philosopher Jeremy Bentham in 1786.

The goal was to be able to watch every inmate at any time by the guards, but nobody knew they were being watched.

The philosophy behind the panopticon was straightforward: if no inmate knew they were being watched at any time, all the inmates will assume that they were being watched all the time, thus will behave properly.

In this sense, cybercrime is used as a scapegoat by governments around the world to 'spy' on anyone venturing in cyberspace, which create a sense that we live in a digital world where everyone is being watched all the time.

This digital panopticon negatively impacts the purpose of the internet in the eyes of many users; instead of being this free and open highway of information and knowledge accessible to everyone, the internet has become a place where the government plays the undercover detective in the name of combating cybercrimes.

All these social impacts enumerated above affect and deter online users in developing countries like Cote d'Ivoire.

[203] Paul, Day. *Cyber Attack*: *The truth about digital crime, cyber warfare, and government snooping.* London, UK: Carlton Publishing Group, 2014.

Unfortunately, the world at large is moving toward a digital economy at every level of society. Thenceforth, it is an imperative for the government of Cote d'Ivoire to get its priorities straight if it does not want to run the risk of being excluded from the global digital economy./.

CHAPTER 3: Laws against Cybercrimes in Cote d'Ivoire

To uproot cybercrimes from society, countries the world over have or are enacting cyberlaws in order to give the necessary legal tools to law enforcement agencies in this fight.

The republic of Cote d'Ivoire has done exactly that, starting in 2013 with the Law against cybercrimes. In fact, under the push of the regional organization, ECOWAS which stands for the Economic Community of West-African States, most countries in the region have enacted laws against cybercrimes, data protection and electronic commerce.

The African Union (AU) through a legal template, urged and advised African countries to enact cyberlaws to fight cybercriminality on the African continent. Outside of Africa, important regional organizations like the European Union (EU) have taken the lead by adopting the Budapest Convention and the General Data Protection Regulation or G.D.P.R.

We are going to dissect the regional (ECOWAS) and the continental (AU) initiatives and their impact on the cyberlaws enacted in Cote d'Ivoire. We will also examine the influence of international treaties like the Budapest Convention and the G.D.P.R. on the way African countries, especially Cote d'Ivoire are fighting cybercrimes with all the necessary help they can get.

3-1: The Ecowas Directive

The Directive on Fighting Cybercrime was adopted on January 8th, 2011, in Abuja, the political capital of the Federal Republic of Nigeria, by the Council of Ministers of ECOWAS. The Council of Ministers agreed that the use of the internet has generated an upsurge of reprehensible acts in the region.

They also noted that cybercrime requires the definition of specific offences that must be linked with conventional offences such as theft, swindling, the receipt of stolen goods, blackmail and damages caused by the internet.

The Member States were also conscious that criminal acts committed through the internet, require the identification of a legal regime and a suitable punishment due to the extent of the damages they cause. Last but not least, they were desirous to effectively fight against cybercrime and provide for an efficient and reliable international cooperation.

The framers of the Directive dedicated an entire chapter (II), enumerating the type of offences related to the information and communication technologies or ICTs. Such offences encompass the fraudulent access to computer systems (Art. 4) to the fraudulent interception of computer data (Art. 8) or anything related to child pornography (Art.16).

The Directive encourages member states to incorporate traditional offences into digital offences (chapter III). In other words, they recognize the fact that old crimes in the real world can be committed through digital means such as the internet.

The Directive also enumerates major penalties for entities other than the public authorities who violate these rules. Certainly, the most important article (art 33) in the whole Directive is dedicated to judicial cooperation between the members of ECOWAS.

The Directive highly encourages member states to cooperate with each other whenever the occasion arises and to do so in line with relevant international instruments and mechanisms on international cooperation in criminal matters.

In practice, there is not a strong cooperation among West-African nations when it comes to combating cybercrimes. Multiple issues prevent a more effective cooperation between member states of ECOWAS, among them, the nature of Internet, the financial costs, and the lack of technical expertise in most West-African countries. These factors are not exhaustive, but they wreak havoc across Africa and the world.

As Ajayi[204] pointed out, one of the biggest impediments in the fight against cybercriminals is the anonymous nature of the Internet. The localization of cybercriminals is not an easy task, especially in West-Africa, where most criminals use cybercafes to commit scams and frauds. Nowadays, cybercriminals can even buy Internet tools to hide online while committing illegal acts, Ajayi[205] added.

[204] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12. https://doi.org/10.5897/jiis2015.0089 (Accessed on 05/18/21).

[205] Ibid. "the unfettered freedom of information and communication enables the cybercriminals to hide their identity using different telecommunications gadgets so as to make it impossible to trace the online Internet Protocol (IP) address of any user. Further, if the IP address of a cybercriminal were traced to a particular location, the next hurdle cannot be scaled as the identity of a cybercriminal is undisclosed to the owner or operator of Internet service provider. Several telecommunications gadgets such as Psiphon, The Onion Router (Tor) etc. are used to shield the identity of Internet users and communication are often routed via many servers which further compounds the possibility of cybercriminals being traced. In effect, if the identities of criminals are incapable of being traced, how can the laws enacted to address cybercrimes work? The dictum of law Lord Denning in a celebrated case to the effect that, it is a cardinal principle of Law that "You cannot put something on nothing and expect it to stand" The point being emphasized here is that, in so far as the identities of cybercriminals remains elusive, no law, however well-crafted nor intended can work because the law does not work in vacuum; stated in another way, cybercrime laws were principally

Indeed, cybercriminals can buy tools like The Onion Router (Tor) to shield their online presence making it extremely unlikely to trace them effectively. The Onion Router (Tor) is a system, developed with the support of the U.S. Naval Research Laboratory, with the specific purpose of insuring the anonymity of communications over the Internet.

The issue of online anonymity used by cybercriminals is not specific to West-Africa but rather, a worldwide issue. The lack of appropriate training and resources of most West-African Law enforcement agencies, make it even more difficult to win this aspect of the battle against cybercriminals. As Luke Irwin[206] argued on his blog, the police have "historically relied on primitive methods for catching cybercriminals".

The "dark web and assumed names are all but impenetrable, meaning crooks can operate with almost total impunity" he pointed out. Besides the issue related to the nature of the Internet, which is a rather worldwide issue, the cooperation among ECOWAS member states is also in practice, difficult to implement due to the lack of technical expertise in most West-African nations.

3-2: The African Union Convention on Cybersecurity and Personal Data Protection

The Information and Communication Technologies or ICTs following their liberalization on the African continent have seen exponential growth not seen anywhere else in the world. According to GSMA Intelligence[207]:

> *By the end of 2018, there were 456 million unique mobile subscribers in Sub-Saharan Africa – an increase of 20 million over the previous year and representing a subscriber*

enacted to apprehend and prosecute cybercriminals, so, if the criminals are not identifiable, any law(s) put in place, is nothing but a nullity".

[206] Irwin, L. *Online anonymity has allowed cybercrime to thrive*. (2018, July 16). https://www.itgovernance.eu/blog/en/online-anonymity-has-allowed-cyber-crime-to-thrive (Accessed on 05/18/21).

[207] GSMA Intelligence. *The Mobile Economy Sub-Saharan Africa 2019*. https://data.gsmaintelligence.com/research/research/research-2019/the-mobile-economy-sub-saharan-africa-2019

> *penetration rate of 44%. Around 239 million people, equivalent to 23% of the population, also use the mobile internet on a regular basis.*

GSMA[208] Intelligence also predicted that:

> *Sub-Saharan Africa will remain the fastest growing region, with a CAGR of 4.6% and an additional 167 million subscribers over the period to 2025. This will take the total subscriber base to just over 600 million, representing around half the population.*

Facing such a sudden and rapid growth in the digital sphere, the African continent had to collectively come up with ways to ensure the smooth transition to the cyber economy era.

What better way to do that than, by making sure the 54 members of the African Union had the legal, policy and social tools to not only safeguard Cyber-Africa but to also be a part of the solutions posed by the burgeoning cybercriminality taking place on the continent.

A uniform regulation of cyber-activities on the continent was in order.

Thus, The African Union Convention on Cybersecurity and Personal Data Protection was adopted on June 27th, 2014, in Malabo, Equatorial Guinea. The adoption of the Convention was preceded by some hiccups regarding the original draft that was criticized mainly by Kenya. The Kenyan Strathmore University's Centre for Intellectual Property and Information Technology Law (CIPIT) claimed that the original version, which was drafted in 2011, would have limited freedom of speech and the right to privacy while giving governments too much power, producing a "legislative overkill", according to Joel Macharia, a Kenyan Tech Entrepreneur.

The regulations in the draft were also concerning for private companies when it comes to the development of e-commerce in Africa.

[208] GSMA Intelligence. *The Mobile Economy Sub-Saharan Africa 2019*. (Supra note 207) P.132.

Three years after the adoption of the Convention, the African Union, launched its Internet Security Infrastructure Guidelines with the aim to facilitate the implementation of the African Union Convention on Cybersecurity and Personal Data Protection.

The guidelines while non-binding, nevertheless, recommends actions necessary to successfully implement the Convention in the African Cybersecurity context, namely the lack of public awareness and the human capital to deal with the growing threat of cybercrimes on the continent.

A year before the adoption of the African Union Convention on Cybersecurity and Personal Data Protection, Richard Medugno[209] was predicting that Africa was going to become a safe harbor for cybercriminals because only 5 of Africa's 54 countries had cybercrimes laws.

As Eric Tamarkin[210] from the Institute for Security Studies (I.S.S) remarked right after the adoption of the Convention, it is a positive start, but substantial challenges are ahead. He pointed out that the portion of the draft related to free speech raised by Kenya ended up remaining unchanged in the definitive version:

> *In particular, free speech critics of the AU's approach cite the provision that requires the criminalization of the computerized creation and dissemination of 'writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature'. Additionally, free speech critics object to the required criminalization of using a computer system to 'insult … persons for the reason that they belong to a group distinguished by race, color, descent, national or ethnic origin, or religion or political opinion'. Finally, they question the required criminalization of using a computer system to*

[209] Medugno, R. (2014, March 28). *Africa: A New Safe Harbor for Cybercriminals?* Trend Micro, Inc. https://blog.trendmicro.com/africa-a-new-safe-harbor-for-cybercriminals/ *"As expected, the most connected African countries, and those with the biggest user bases, are also those with the most malware: Algeria, Egypt, Nigeria, and South Africa. Of these, only South Africa has a cybercrime law in place, though Kenya is in the process of creating one. So given the situation, we think it is safe to say that the number of cybercrime activities targeting or originating from Africa will increase—and dramatically—in the next few years. As the world becomes more digital, so does the need to stay diligent with IT security."*

[210] ISS Africa. *The AU's cybercrime response: A positive start, but substantial challenges ahead*. (2015, January 20). https://issafrica.org/research/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead

> *'deliberately deny, approve or justify acts constituting genocide or crimes against humanity'*[211].

The convention is overly ambitious and too cumbersome, as it deals with many areas of electronic activity beyond cybercrime[212], he added.

In effect, the few African countries that had a cybercrime legislation in place like Cameroon, Cote d'Ivoire had an arduous task to readjust their legislation to conform to the Convention. In his conclusion[213], countries coalescing around a common instrument have a chance to successfully fight cybercrime.

One of the goals of the convention was to reach cyber stability[214], defined as:

> *a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels.*

[211] ISS Africa. *The AU's cybercrime response: A positive start, but substantial challenges ahead*. (Supra note 210) P.134.
[212] Ibid.
[213] Ibid. "Despite the substantial hurdles and shortcomings of the international treaty approach, states that coalesce around a common instrument will have a stronger position in the global fight against cybercrime. So long as there remains a weak link in the cybersecurity chain, cybercriminals will seek to exploit it. Unless and until there is broad global agreement on criminalizing cybercrime and robust international cooperation to enforce those laws, cybercriminals operating in cybercrime safe havens will continue to target individuals, businesses, and governments with impunity. If Africa becomes known as a cybercrime safe harbor, this could have devastating consequences for the continent's potential growth. Furthermore, if an African state becomes known as a hospitable environment for cybercriminals, it will not only damage that country but will also have a negatively impact on the reputation of the continent as a whole. The AU's convention is a positive step toward prodding African states into taking proactive domestic measures to help curb the scourge of cybercrime. The Budapest convention remains the best available instrument to unite the international community under a common framework to fight cybercrime, but African states should not wait for the international cybercrime treaty process to unfold, as ratification is not a panacea to the cybercrime problem. They should instead focus on shoring up their cybersecurity and enhancing their capacity to fight cybercrime without delay."
[214] Marco, G. (2009) Understanding Cybercrime: A Guide for Developing Countries. Geneva: ITU, p. 84.

This definition creates a basis from which to discern-when stability is the goal-what is potentially relevant, useful, and strategic information about an activity in the cyber domain from what is not. It can also serve as a basis for determining what resources and activities can be directed purposefully towards that end, added Lisa Rudnick and Derek Miller[215].

To reach cyber stability, they have developed a user's-centred tool for policymakers the world over. The goal is:

> *To contribute towards the achievement of international cyber stability by improving the capacity of diplomats and policymakers to participate in a more informed and effective manner in dialogue and decision-making processes pertaining to stability in the cyber sphere[216].*

As catchy as the concept of cyber stability sounds, one must recognize that it is a new concept which aims to arm states and regional organizations with the proper tools to guard against the scourge of cybercrimes of all kinds.

In this regard, the idea behind the African Union convention on cybersecurity and personal data protection is exactly to reach some form of cyber stability on the African continent, a haven for cybercriminals as Loucif Kharouni[217] posited back in 2013. As U.J Orji[218] explained, the idea of cyber stability is, the concept to promote the exercise of state responsibilities to address the security challenges of the information society.

This requires states to establish appropriate legal, policy and regulatory measures to protect cyber users and cyber infrastructure within their authority, and also ensure that cyber activities which are

[215] Rudnick, L. et al. (2015) Towards Cyber Stability: A User-Centred Tool for Policy Makers. Geneva: United Nations Institute for Disarmament Research, p. 7.
[216] Ibid.
[217] Trend Micro, & Kharouni, L. (2013). *Africa, a new safe harbor for cybercriminals?* https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf
[218] Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? Masaryk University Journal of Law and Technology. https://journals.muni.cz/mujlt/article/view/8666/9255

conducted within their authority do not cause harm to other individuals or infrastructure in another authority.

He also pointed out, the slow pace of ratification by member states and the absence of effective regional coordination as some of the major reasons why the Convention has not been effectively applied as a framework for promoting regional cyber stability.

In order to reach its lofty goals in the realm of cybersecurity in Africa, Uchenna[219] makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve the regional harmonization of cybersecurity governance frameworks and harness the application of the Convention as a framework for promoting regional cyber stability, in line with Article 32 of the African Union Convention on Cybersecurity and personal data protection which provides for the establishment of a monitoring and operational mechanism for the purpose of implementing the Convention.

The content of Article 32 as to the responsibilities of the Convention's operational mechanism is as follow:

> *(a) promoting the adoption and implementation of measures to strengthen cybersecurity in electronic services and combating cybercrime and human right violations in cyberspace; and*
>
> *(b) advising African governments on measures to promote cybersecurity and combat cybercrime and human right violations in cyberspace at the national level*[220].

Before we dive into the content of the convention itself, it is important to describe the chronological steps taken by the African Union (AU) before arriving at the proper adoption of a convention on cybersecurity and personal data protection in Malabo, Equatorial Guinea in 2014.

[219] Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity. (Supra note 218) P.136.
[220] See Article 32 AU Convention on Cybersecurity and Personal Data Protection.

The AU signaled the need of a continental harmonization of cybersecurity policies in 2008 in the Draft Report in a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation[221].

Unlike its European counterpart, the Council of Europe, which had taken steps at the end of the 90s, the African Union waited so long because in the words of U.J Orji[222], a major factor that might have impeded the development of regional cybersecurity initiatives can be traced to the low penetration of ICTs in Africa prior to the widespread availability of wireless technologies within the first decade of the 21st century.

The following year, exactly on November 5th, 2009, the African Union members at the ministerial level, convened an Extraordinary Session in Johannesburg, South Africa, where they adopted a set of declarations known as the *Oliver Tambo Declaration*[223]. The Declaration directed the AU to:

> *Jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection*[224].

The Oliver Tambo Declaration was adopted to keep in line with the decision of the 13th Ordinary Session of the Executive Council in Sharm El-Sheik, Egypt in 2008, calling on the African Union Commission and Member States:

> *To take the necessary measures to speed up the implementation of the Reference Framework for Harmonization for Telecommunication ICT Policy and Regulation, the Strategies and Action Plans for the development of a Postal Sector in Africa, and the*

[221] See African Union (2008) Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report. Addis Ababa, Ethiopia: African Union.
[222] Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity. (Supra note 218) P.136.
[223] See Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) Oliver Tambo Declaration. Johannesburg, South Africa: African Union.
[224] See Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) Oliver Tambo Declaration. Johannesburg, South Africa: African Union.

ARAPKE with a view to develop a strong, integrated and the viable communications sector in the continent[225].

In that declaration[226], member states of the AU, vowed to establish the Reference Framework for Harmonization for Telecommunication ICT and Policy Regulatory, the Strategies and Action Plans for the development of the Postal Sector in Africa; they also wanted to ensure that ICT policies are mainstreamed in other sectors at national, regional, and continental levels. Last but not least, the member states wanted to prioritize the integration of ICTs into National Imperative Programmes including Education Training Systems and the public administration with a view to produce a critical mass and increase skilled human capital and promote access and use of ICTs at 10% growth rate per annum while promoting the transition of Broadcasting from Analog to digital and to promote a South-South cooperation.

The Convention that resulted from the Oliver Tambo Declaration was far from the lofty goals set in the declaration.

In fact, many stakeholders turned against the first draft of the convention.

In effect, the issue raised by some participants, especially from Kenya revolved around what Kaitlin Ball[227] termed the *"juxtaposition of personal liberty and national security concerns."* The concept of personal liberty involves the freedom of speech, civil opposition, freedom of association and assembly, which are most of the time in conflict with the national security apparatus of developing countries where democracy has not taken solid roots.

[225] See *Oliver Tambo Declaration*. (2009, November). https://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf
[226] Ibid.
[227] Ball, K. M. (2017). Introductory Note to African Union Convention on Cyber Security and Personal Data Protection. *International Legal Materials*, *56*(1), 164–192. https://www.jstor.org/stable/90020562

This is the case of most African nations to the notable exception of countries like South-Africa, Mauritius, Botswana, and a few others. There is, therefore, a huge risk that most African countries will strip away at individual freedoms in the name of fighting cybercriminality.

The one thing we are sure of is that, less democratic governments always manage to violate individual liberties, irrespective of what is deemed appropriate to safeguard national security. One thing the "conflict" about the draft of the convention made clear was that the national security concerns weighed heavily on the draft, thus raising the legitimate concerns of advocate groups the continent over.

This turn of events was not surprising since the representatives of member states wrote the convention. In its preamble, the convention acknowledged the challenges posed by the protection of personal data and private life in the information and communication era not only to governments but also to other stakeholders.

Thus, the convention suggested a balance[228] between the use of information and communication technologies and the protection of the privacy of citizens while guaranteeing the free flow of information.

That being said, in the next line, the convention reminds everyone that the protection under criminal law of the system of values of ICTs is a necessity prompted by security considerations.

The Convention also signaled the need to define a strategy for the repression of cybercrimes in member states by modernizing the old instruments of repression and considering crimes that are specifics to the Information and Communication Technologies (ICTs).

[228] See AU Convention on Cybersecurity and Personal Data Protection. Part I – Objectives.

The Convention (Article 11) requires all states to establish an independent administrative authority tasked with protecting personal data[229]. Article 12 calls on member states to establish limits on the processing and storage of data, although it allows for exceptions in the public interest like in the case of a scientific need.

The Convention grants states, the right to discontinue data processing or even temporally or permanently prohibit data processing in emergency situations endangering fundament rights and freedoms.

The Convention in its Chapter III promoting Cyber Security and combating cybercrime[230], encourages member states to adopt a national strategy to implement a national cybersecurity policy in the area of legislative reform and development, sensitization and capacity-building, public-private partnership, and international cooperation.

Article 25 encourages member states to confer specific responsibilities on institutions either newly created or pre-existing. In other words, just like for the personal data protection aspect of the Convention, the cybersecurity aspect of the Convention requires member states to establish a specific institution to deal with the promotion of cybersecurity and the repression of cybercrime.

Article 25 al.3 requires member states to ensure that measures adopted in the area of cybersecurity will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, especially the African Charter on Human and People's Rights[231].

[229] Ball, K. M. (2017). Introductory Note to African Union Convention on Cyber Security and Personal Data Protection. (Supra note 227) P.139.
[230] See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art.25. al.2
[231] See AU Convention on Cybersecurity and Personal Data Protection. Chapter III.25 al.3.

Among the measures the Convention deemed important to foster a culture of cybersecurity in member states, are the sensitization, education and training, and the dissemination of information to the public.

Article 28 related to international cooperation, ask states parties to ensure that their legislative measures and/or regulations to fight against cybercrime will help strengthen regional harmonization while respecting *the principle of double criminal liability*[232].

The Convention in article 32, also encourages member states to adopt a regimen of mutual assistance among them in the fight against cybercrime. Other measures to enforce the laws against cybercrime at the national level were included in the Convention[233].

At the African Union's level, the Convention asked the Chairperson of the Commission to report to the Assembly about the establishment and monitoring of the operational mechanism of the Convention.

The monitoring mechanism shall among other things, promote and encourage the Continent to adopt and implement measures to strengthen cybersecurity in electronic services and in combatting cybercrime and human rights violations in cyberspace.

For Uchenna J. Orji[234], the AU Cybersecurity Convention holds several prospects towards promoting regional cyber stability in Africa. Such prospects, he argued, arise from the fact that the establishment of the Convention increases policy and regulatory awareness on cybersecurity governance, while also improving the harmonization of national cybersecurity regimes in AU member states.

[232] See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art. 28 al.1
[233] See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art.32.
[234] Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity. (Supra note 218) P.136.

He cited other prospects[235] that include the imposition of a range of positive obligations on AU member states to establish national cybersecurity regimes, and also increases the possibility of imposing AU sanctions on non-compliant member states.

Unfortunately, as Landry and Kevin Signe[236] pointed out in March 2021, as of June 2020, the Convention has only been ratified by 8 out of 55 members (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda, and Senegal), while 14 countries have signed but not ratified it.

Cote d'Ivoire, which had adopted the Fight Against Cybercriminality Act before the adoption of the AU Convention on Cybersecurity and Personal Data Protection, has yet to sign, let alone to ratify the Convention.

The question is to wonder if The Fight Against Cybercriminality Act adopted by Cote d'Ivoire's Parliament in June 2013 is enough to help the country in the repression of cybercrimes? Let us find out.

[235] Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity. (Supra note 218) P.136.
[236] Signé, L., & Signé, K. (2021, April 6). *How African states can improve their cybersecurity*. Brookings. https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/

3-3: The Fight against Cybercriminality Act

Cote d'Ivoire is one of the countries in West-Africa plagued with cybercrimes since the dawn of the Information and Communication Technologies (ICTs), especially the world wide web or internet.

To its credit, Cote d'Ivoire was one of the first few African countries to tackle the scourge of cybercrimes with a number of legislative initiatives: The Fight Against Cybercriminality Act, adopted on June 19, 2013, a year before the adoption of the African Union Convention on Cybersecurity and Personal Data Protection in Malabo, Equatorial Guinea.

The sense of urgency in adopting those legislations was made acute by the fact that in the earlier 2010's, Cote d'Ivoire was the number one hub in West-Africa when it came to the commission of cybercrimes, surpassing Nigeria, and Ghana.

This sad record had its explanation in the fact that the country is a mini-ECOWAS, meaning that Cote d'Ivoire is traditionally at the receiving end of mass migration from most countries in West-Africa.

The earlier days of cybercrimes in Cote d'Ivoire were dominated by immigrants from Nigeria, but also from Ghana and smaller communities from Benin, Togo, and Sierra Leone. The involvement of native Ivorians was negligeable. That being said, by 2013, most cybercriminals operating in Cote d'Ivoire were Ivorian nationals.

The repression of cybercrimes by the Ivorian authorities against the foreign connections made up of Nigerian nationals and to a lesser degree, citizens from neighbouring Ghana had pushed them into "exile" back to their home country.

Their legacy, however, endures thanks to the rapid ascension of native Ivorians in the commission of cybercrimes of all kinds.

The Ivorian government through its parliament, adopted a number of cyber laws to combat the rising number of cybercrimes committed by Ivorian citizens against French-speaking victims from Cote d'Ivoire to Switzerland, France, Belgium and all the way to Quebec, Canada.

The Fight Against Cybercriminality Act (No 451) was adopted in conjunction with The Law No. 2013-450 dated June 19, 2013, on The Protection of Personal Data.

The first article (Art.1) of The Fight Against Cybercriminality Act explicitly said that:

> *Definitions of legal instruments of ECOWAS, the African Union or the International Telecommunication Union prevail for terms not defined in this Act*[237].

This first article is important as it allows the implementation of the African Union Convention on Cybersecurity and Personal Data Protection that will be adopted a year later by the African Union in Malabo, Equatorial Guinea in 2014.

Article 2 of the Law defines the purpose of the Law as being a tool to fight against cybercriminality and Criminal offenses the discovery of which requires the collection of electronic evidence.

The Act contains 8 chapters going from the commission of crimes specifics to the Information and Communications Technologies (chapter3) to the penal procedure in cybercriminality (Chapter 8).

In between these chapters, we have chapters regarding offenses to intellectual property (chapter4), illegal acts on electronic communication networks (chapter 5) to the Internet Service Providers'(ISPs) obligations (chapter 6) and the adaptation of classical offenses to the Information and Communication Technologies (ICTs) (chapter 7). We begin with the chapter 3 of the Act

[237] See Art.1 of the Fight against cybercriminality Act (Law No 2013- 451.)

which defines the penalties for the commission of crimes specific to information systems and the Internet in general.

The fraudulent access or attempt to access an information system (Art. 4)[238] is punished by jail of no more than 2 years and a fine of $10.000 to $20.000 as a result of the fraud. The fraudulent interception of computer data or its attempt (Art. 8)[239] is severely punished with a jail term of no more than 10 years and a fine between $80.000 and $120.000 which is substantial for the average cybercriminal operating in Cote d'Ivoire.

The alteration, modification, or suppression of computer data (Art.9)[240] is heavily punished by 10 years imprisonment and $120.000 fine. It is important to note that the Chapter 3 of the Fight Against Cybercriminality Act is the heart of the Act and contains thirty articles.

It is also crucial for the sake of this review to focus more on the parts that deal with universal crimes that are specifics to the Internet or Information Systems used not just in Cote d'Ivoire, but all around the world. Article[241] 13 of the Act prohibits intentionally and knowingly, the production, sale, diffusion of a computer program, a password, access code or similar computer data by a jail time of no more than two years and a fine of up to $100.000.

Here, it is obvious that the Ivorian Lawmakers intended to fight the illegal hacking of computer systems and that include financial institutions like the banking system.

We denote that the punishment by imprisonment is quite light with respect to the seriousness of the offense.

[238] See Art. 4 of the Act. (Law No 2013- 451.)
[239] See Art. 8 of the Act. (Law No 2013- 451.)
[240] See Art. 9 of the Act. (Law No 2013- 451.)
[241] See Art. 13 of the Act. (Law No 2013- 451.)

In comparison, 18 U.S. Code[242] § 1029 regarding fraud and related activity in connection with access devices is punished by imprisonment between 10 and 15 years.

On the other hand, the law severely punishes financially whoever engages in the production, storage, dissemination of child pornographic images through information systems or computer data (Art. 15) with a jail sentence of no more than 5 years and a fine of up to $200.000.

For comparison, Art.23 of the Cybercrime prevention and prohibition Act[243] of 2015 in Nigeria punishes anyone who engages in the production and distribution of child pornography to a jail term of no more than 15 years, which is 3 times greater than the jail term in the Ivorian legislation, although the fine in the Nigerian legislation is a mere $49.000.

While Cote d'Ivoire has a harsh financial punishment ($200.000), with a mere jail term of 5 years, Nigeria harshly punishes the guilty party in a case of child pornography of up to 15 years, but with a fine of just $49.000.

What could explain the difference in terms of punishment type between Cote d'Ivoire and Nigeria. Why is that the Ivorian Lawmaker put the focus on the fine while the Nigerian Lawmaker put the focus on the jail term?

Although, it is difficult to gauge the intent of the Lawmakers of each country from the same geographical space, here Cote d'Ivoire and Nigeria are both in West-Africa, one probable reason

[242] *18 U.S. Code § 1029 - Fraud and related activity in connection with access devices*. (2020). LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1029
[243] Nigeria Cert. *ngcert*. (2018). https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

for the differences may have to do with the financial strength of cybercriminals in Cote d'Ivoire and in Nigeria.

It is officially known that criminal gangs in Nigeria, including cybercriminals are well organized financially. In fact, due to the rampant corruption in most African countries and especially in Nigeria, putting the focus in terms of punishment of child pornography on the fine with a reduced jail term would make it easier for the accused to be quickly released since no matter how high is the fine, he can afford it through obscure connections and corruption.

It was wise for the Nigerian Lawmakers to put a harsh jail term in place with a "small" fine because 15 years behind bars means he is out of sight for an exceptionally long time.

On the other hand, in the case of Cote d'Ivoire, the Lawmakers put their focus on the financial punishment because, you do not have these powerful criminal enterprises in the country, capable of paying massive amounts of money to get their man set free from prison.

So, it is understandable for the Ivorian Lawmakers to put the onus on the financial penalty rather than the jail term. The crime of child pornography is so serious that Lawmakers dedicated four (4) articles (Art. 15, 16, 17, 18) to the subject. The theme of child exploitation in general and for prostitution and pornography is overly sensitive in Africa.

As John Mbaku[244], pointed out, the abuse and exploitation of children is a major public policy priority for all African countries. Throughout the continent, children are routinely abused and exploited as sex objects; tools in the production of various goods, including cocoa, gold, and

[244] John Mukum Mbaku, *The Rule of Law and the Exploitation of Children in Africa*, 42 Hastings Int'l & Comp. L. Rev. 287 (2019). Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol42/iss2/2

various minerals, as well as, services, such as pornography and prostitution; and, as child soldiers to fight in sectarian conflicts and civil wars.

He went on to identify the perpetrators[245] of such crimes by revealing that children in Africa are exploited and abused by both domestic and external or foreign actors and these include, but are not limited to, family members and community leaders, foreign tourists who seek the continent's children for sex, and international criminal gangs who are engaged in the production of child pornography, sex trafficking and the illegal harvesting and sale of organs. The Fight Against Cybercriminality Act also deals with identity theft in its article 19. Three (3) types of offenses are identified in article 19 but the penalties are the same for all three offenses: (a) The illegal use of someone else's identity, (b) The sale, distribution of someone else's identity and (c) The production of false identification.

In each case, the author is guilty of identity theft and is jailed for a term of no more than 5 years and a fine of no more than $20.000. The processing of personal data (Art. 24) through illegal means is punished less harshly in terms of jail time (no more than 5 years) but more harshly in terms of fine ($200.000).

The remaining articles of chapter 3 deals with the fraudulent impersonation to deceive victims and collect information from them and the theft of information with or without the use of violence (Art. 25 through Art. 32).

The penalties are harsh on the financial side and less so on the physical restriction of those guilty of the offenses. We must note that the Ivorian Lawmakers emphasize the financial punishment over the physical restriction one to discourage the commission of crimes specifics to the

[245] John Mukum Mbaku, *The Rule of Law and the Exploitation of Children in Africa*. (Supra note 244) P.148.

Information and Communication Technologies (ICTs) unlike their Nigerian counterparts as we saw in the case of child pornography.

The real question is if focusing more on one form of punishment over the other is enough to dissuade the African youth from venturing into the obscure world of cybercriminality. Secondly, it is doubtful that those guilty of said offenses are strictly punished by the justice system in West-Africa in general and in Cote d'Ivoire in particular.

These are questions that we will try to find answers to later in the chapters specifically dedicated to them. The chapter 4 of the Fight Against Cybercriminality Act is dedicated to intellectual property crimes.

Here, the Ivorian legislator once again as in past chapters, severely punishes intellectual property theft in terms of financial penalty ($200.000) over the jail time which is no more than 10 years (Art.33). The issue of intellectual property protections is seen as far removed from the everyday concerns of the average as noted in the online publication Lawteacher[246], as opposed to feeding themselves or being physically safe from political strife.

On the paper, laws are enacted but seldom enforced even though African countries lose billions of dollars each year due to intellectual property theft. As Lawteacher[247] noted, for instance Nigeria, which has a booming video and film industry, known as Nollywood, and the third largest movie industry in the world, is faced with an enormous piracy. Nollywood movies are being duplicated

[246] Teacher, Law. (November 2013). Patent and Intellectual Property Issues in Africa. Retrieved from https://www.lawteacher.net/free-law-essays/international-law/patent-and-intellectual-property-issues-in-africa-international-law-essay.php?vref=1 .
[247] Ibid.

in China and sold in several other African countries. The lack of Intellectual Property creates an unstable market and risk on investments in the industry.

Article[248] 33 of the Act also enumerates the types of intellectual property crimes, while article[249] 34 details those circumstances in which the use of intellectual property assets is not illegal. For example, copies or reproductions of intellectual works for strictly private use. Article[250] 35 of the Act recognize the right of the copyright owner to prevent the use of the intellectual works even when legal if and when such use is detrimental to the interests of the copyright owner. The last article[251] (Art. 36) of chapter 4 warns Internet Service Providers of legal consequences if they do not prevent the use of their materials by patrons to illegally copy or reproduce the intellectual works of copyright owners.

The chapter 5 of the Act focuses on unlawful acts on electronic communication networks. Here, the Ivorian legislator is specifically targeting illegal online gambling by unauthorized persons or entities.

One can be prosecuted for organizing or taking part in illegal online gambling; if caught there are various penalties depending on what role the guilty party played in the act. One thing to note with regard to the Fight Against Cybercriminality Act of Cote d'Ivoire as compared to the Cybercrime Prohibition and Prevention Act[252] of Nigeria, is that while the Ivorian Cyber Law dedicates a chapter for intellectual property protection and another one for illegal online gambling, the Nigerian Cyber Law of 2015 does not.

[248] See Art.33 of the Act
[249] See Art.34 of the Act
[250] See Art.35 of the Act
[251] See Art.36 of the Act
[252] Nigeria Cert. (2018). (Supra note 243) P.147.

On the other hand, both legislations cite cyber terrorism without explaining its meaning though the Nigerian Law refers to the Terrorism Prevention Act of 2011 to find the meaning of the word "cyber terrorism".

As we have said before, the definition of the word "cyber terrorism" is tricky because in most African countries and even at the African Union (AU), there is not a uniform view as to what the word terrorism means in the African context. The chapter 6 of the Act is dedicated to the obligations of operators of Cybercafes.

This part of the law is critical in successfully fighting cybercriminality in Africa, since most of cybercriminals on the continent use cybercafes to commit those online scams, we hear about oftentimes in the news.

The prior identification of cybercafes patrons is now mandatory as article 42 of the Act prescribes. A minor who is less than 10 years old is not allowed inside a cybercafe, while a minor who is less than 18 years old has a limited access to a cybercafe (art.43).

In the case of a minor who is less than 18 years old, article 43 forbids him or her to have access to pornographic, violent, or racist websites. Many African countries have tried to tackle the use of cybercafes to commit cybercrimes by introducing a number of legal prescriptions to deter this phenomenon.

The Nigerian cyber law of 2015 does the same through article 7 of the law by mandating the registration of all cybercafes in the country as business entities whose activities shall be made available to Law enforcement when needed. The registration of cybercafes in Cote d'Ivoire is also mandatory per the law. But unlike the Nigerian Act of 2015 which does not spell out too much with regard to cybercafes, the Fight Against Cybercriminality Act of Cote d'Ivoire is more detailed

when it comes to the management of a cybercafe in terms of duties and responsibilities of the owners of cybercafes.

Hence, where the Nigerian law dedicates only one article to the registration of cybercafes in Nigeria, the Ivoirian law dedicates an entire chapter made up of 16 articles to the duties and responsibilities of cybercafes in Cote d'Ivoire.

For example, articles 46 and 47 detail when a cybercafe's owner can or cannot be held liable for the data stored on their computers.

The impact of cybercafes in the commission of cybercrimes in Africa is substantial in that, those cybercafes are cheap, convenient for the majority of folks addicted to internet in poor countries and even in some parts of well-developed countries in Asia as reported by Li, Zhang, Lu, Zhang, & Wang[253]. Another survey by Gencer and Koc[254] reveals that for up to 25% of students in Turkey, cybercafé was the dominant place for accessing the internet.

In Cote d'Ivoire, the vast majority of cybercriminals use cybercafes also called Internet cafes to commit cybercrimes due to the anonymous nature of a cybercafe.

That being said, it is increasingly challenging to use a cybercafe to commit crimes thanks to the law, except when there is collusion between the criminals and cybercafe owners and even some law enforcement officers.

The chapter 7 of the Act deals with offences related to violence, racism, xenophobia (articles 58 through 66) but also has a national security aspect, in that it severely punishes with a life

[253] Y. Li, X. Zhang, F. Lu, Q. Zhang, and Y. Wang, "Internet addiction among elementary and middle school students in China: a nationally representative sample study," Cyberpsychology Behav Soc Netw Another, vol. 17, no. 2, pp. 111–116, 2014.
[254] S. L. Gencer and M. Koc, "Internet Abuse among Teenagers and Its Relations to Internet Usage Patterns and Demographics," Educ. Technol. Soc., vol. 15, no. 2, pp. 25–36, 2012.

imprisonment, any Ivorian national(art.67) or a foreigner(art.68) who use a computer system to spy on behalf of a foreign country.

The last chapter (8) of the Act deals with the criminal procedure as it relates to cybercriminality in Cote d'Ivoire. The Personal Data Protection Act was adopted the same day the Fight Against Cybercriminality was adopted by the Ivorian Parliament.

The same Parliament would go on to adopt one month later, the Electronic Transactions Act, making Cote d'Ivoire one of the few African countries with a complete set of cyber laws covering the Information and Communication Technologies in the country.

We are now going to dissect the law related to the protection of personal data in Cote d'Ivoire by trying to pierce the veil on the intent of the Ivorian legislator when it comes to the protection of personal data which as we will see can lapses with matters of national security.

The intersection of the need to protect one's personal data and the necessity to protect the national security of any nation, including African countries, have nearly derailed the African Union Convention on Cybersecurity and Personal Data Protection a year after the adoption of the Ivorian law.

3-4: The Personal Data Protection Act

The protection of personal data in Africa is trending toward the adoption of data protection laws over the past couple of years. South Africa adopted the Protection of Personal Information Act (POPI Act) in June 2020 making the industrial giant, the latest African country to enact a law protecting personal data.

A year before that (2019), the first economy of the African continent, Nigeria, adopted the Nigeria Data Protection Regulation (NDPR). That same year, Uganda passed the Data Protection and Privacy Act (DPPA, 2019).

As Cathy-Eitel Nzume[255] pointed out in her contribution to the site of the International Association of Privacy Professionals (IAPP), the enactment of data protection legislation across Africa bodes well for the future. She argued that, since the passage of the General Data Protection Regulation Act[256] in 2016 in Europe, countries all over the world have been enacting privacy laws including in Africa.

Cote d'Ivoire unlike the two economic giants of the continent (Nigeria and South-Africa), passed the Personal Data Protection Act back in 2013. To be fair to South-Africa, one must note that the process to enact the POPI Act started in 2013 with some sections of the Act becoming applicable as soon as 2014.

[255] Cathy-Eitel Nzume, CIPP/US. *Slowly but surely, data protection regulations expand throughout Africa*. (2021, April). IAPP. https://iapp.org/news/a/slowly-but-surely-data-protection-regulations-expand-throughout-africa/
[256] Ibid.

That being said, Cote d'Ivoire in the words of Cathy-Eitel Nzume[257], is one of the trailblazers, with Benin, Senegal, Kenya, Ghana, and South Africa, which have enacted general data protection laws and are spearheading efforts to sensitize citizens.

In a speech[258] at the Annual Conference of the African Bar Association Port-Harcourt, Nigeria on privacy and data protection law, João Luís Traça hailed the Ivorian Data Protection Law in that it makes it possible to avoid the necessity of compliance with formalities with the national regulator, the "Authorité de Régulation des Télécommunications" ("ARTCI"), with the appointment of a Data Protection Officer:

> *In order for natural or legal persons to fulfil the role of a Data Protection Officer in Côte d'Ivoire, they must meet certain criteria. Said rules are laid down in Order No. 511/MPTIC/CAB of 11 November 2014, which defines the relevant profile and lays down the relevant employment conditions. Among other conditions, Data Protection Officers must have completed a certain level of studies in legal sciences or computer sciences or Telecommunications/ICT networks and must be Ivorian citizens*[259].

The Personal Data Protection Act comprises 8 chapters, totaling 54 articles. The first chapter is about the definition of terms while recognizing that:

> *Definitions of legal instruments of ECOWAS, the African Union or the International Telecommunication Union prevail for terms not defined in this Act.*

In that first chapter, the Protection Authority is defined as:

---

[257] Cathy-Eitel Nzume, CIPP/US. *Slowly but surely, data protection regulations expand throughout Africa*. (Supra note 255) P.155.

[258] Joao, T. Privacy / Data protection Law: How much disclosure does growth need? Africa 2.0: A brave new (digital) world. Annual Conference, African Bar Association. Port-Harcourt, Nigeria. 2017. https://www.afribar.org/portHarcourt2017/papers/JoaoTracaPaperPrivacyABAfinal.pdf "As an additional note and to demonstrate the importance of regulators as an effective part of the application of law, reference can also be made to the Ivory Coast and its data protection internal legal landscape (enacted by means of Law No. 2013-450, of 19 of June). In Côte d'Ivoire, we are able to find the same general principles and rules as in the aforementioned examples. Regardless, this authority has gone a step further and it is possible to avoid the necessity of compliance with formalities with the national regulator, the "Authorité de Régulation des Télécommunications" ("ARTCI"), with the appointment of a Data Protection Officer. More to the point, should a person qualify as a Data Protection Officer, under local regulations10, the same can act as a sort-of representative of ARTCI within their own entities (or at least as an independent gatekeeper of the values and rules set in the law) and, as such, audit themselves the application of the law without the need to make filings with the regulator. This exemption to comply with formalities is only voided in specific circumstances, such as special operations of processing of data are involved (e.g., sensitive data)."

[259] Ibid.

The independent administrative body to ensure that the processing of personal data is implemented in accordance with the provisions of this Law.

It is important to note that in Cote d'Ivoire, the agency in charge of the regulation of telecommunications (ARTCI) is also the one in charge of implementing the law regarding the protection of personal data.

In other words, the protection of personal data is not in the hands of a specialized entity uniquely dedicated to protecting the personal data of Ivorians, rather, the implementation of the law on personal data protection is given to an all-powerful agency with multiple other duties.

We think that to implement data protection more efficiently in Cote d'Ivoire as in the rest of Africa, an independent agency whose purpose is centered only around the protection of personal data should be in charge.

That being said, one powerful reason to explain the concentration of many tasks by the "Authorité de Régulation des Télécommunications" ("ARTCI"), is the lack of skilled personnel in the field of cybersecurity in general.

The chapter 2 in its articles 3 and 4 enumerates what the law considers as data collection or exclude from the provisions of the law. Thus, according to article 3 of provisions subject to this law are:

- *Any collection, treatment, transmission, storage, and any use of personal data by a natural person, the state, local authorities, and public or private corporations;*
- *Any automated processing or not of data included or intended to be included in a file;*
- *Any data processing implemented on the national territory;*
- *All processing of data concerning public security, defense, investigation and prosecution of criminal offenses or the state security, subject to the exceptions defined by the specific provisions set by other legislation in force.*

Article 4 of the Act exclude from the scope of the law:

> *Data processing implemented by an individual in the exclusive context of personal or household activity, provided that the data are not intended for systematic communication to third parties or dissemination;*
>
> *Temporary copies made in the course of technical transfer of activities and access to a digital network supply for automatic, intermediate, and transient data and the sole purpose of allowing other recipients of the service the best access possible to the transmitted information.*

Here, the Ivorian legislator is applying the same general principles and rules as in most other countries around the world and especially on the African continent. Joao T pointed it out when he said in his speech that:

> *In Ivory Coast, we are able to find the same general principles and rules as in the aforementioned examples (Mozambique, Angola, and Cabo Verde)*[260].

Article 4 recognize that the regulation of data protection must strike an appropriate balance with important human rights, such as access to information and freedom of expression. Article 6 of the Act delineates the scope of acts not considered data collection or data processing per se:

> <u>*Art. 6*</u>*:* are exempted from the formalities statement*:*
>
> - *The data processing used by an individual in the exclusive context of his personal, domestic, or family activities;*
> - *The processing of data relating to an individual which publication is prescribed by law or regulation;*
> - *Data processing whose sole purpose is the keeping of a register which is intended for private use only;*
> - *The processing of data for which the responsible person designated a correspondent for the protection of personal data in charge of ensuring in an independent manner, the compliance with the obligations provided for in this Law except where a transfer of personal data to a third country is considered.*

[260] Joao, T. Privacy / Data protection Law: How much disclosure does growth need? (Supra note 258) P.156.

Cote d'Ivoire is one of fourteen African members of the international organization called "Open Government Partnership" or OGP[261]. Of those 14 members, only 8 including Cote d'Ivoire have enacted data protection law.

The Open Government Partnership has analysed 4 focus areas regarding the transparency of the process of protecting data and has made recommendations for the member-states. The 4 focus areas are as follow:

The Right to Notification: Twelve African countries within the OGP provide data subjects with the right to be notified that their personal data is being processed. The transparency of the collection and processing of data in Cote d'Ivoire is taken care of at articles 18 and 28 of the Personal Data Protection Act:

> *Article 18: The principle of transparency requires a mandatory and clear information from the responsible person on the processing of the personal data*[262].
>
> *Article 28:* The person responsible for the processing shall provide the person whose data are being processed, at the latest, during the collection and whatever the means and media used, with the following information:
>
> - *His/her identity and, if applicable, his/her authorized representative;*
> - *The purpose (s) set for which the data are intended;*
> - *The categories of data concerned;*
> - *The recipient (s) to whom the data might be disclosed;*
> - *The possibility of refusing to appear on the file in question;*
> - *The existence of a right of access to data concerning the person and the right to rectify any such data;*
> - *The shelf life of the data;*

[261] *Data Protection in Africa: A Look at OGP Member Progress*. (2021, August 11). Open Government Partnership. Retrieved 2021, from https://www.opengovpartnership.org/documents/data-protection-in-africa-a-look-at-ogp-member-progress/

[262] See Art. 18 of Law. No. 450. 19 June 2013.

- The possibility to transfer the data to third countries[263].

Breach Notification: The notification of a breach of personal data by the person responsible for the collection and or processing of the data is not included in most Personal Data Protection Laws in Africa including Cote d'Ivoire.

As the Open Government Partnership[264] pointed out, the obligation to notify a data subject in the event of a data breach contributes to increased transparency and enables a data subject to control their personal data. The OGP organization noted a number of legal ways that might prevent the non-reporting:

> *(1) through the absence of a prescribed timeframe for notification;*
> *(2) through the use of vague terms for the notification period; and*
> *(3) through the inclusion of exceptions which allow for non-reporting.*

The Personal Data Protection Act of Cote d'Ivoire does not mandate the notification of a breach of personal data by the person responsible for the collection and or processing to the victim of the breach.

The law does not even hint at the possibility that the personal data of Ivorian citizens collected and/or processed can be breached by cybercriminals operating from anywhere in the world.

We think that as the OGP put it, the notification of any breach to personal data to the victim should occur not only to show transparency of the process but also to avoid security risks to the potential victim of a data breach.

A victim of data breach who is unaware of the breach, may be ensnared in a situation where her knowledge of the illegal use of her is presumed.

[263] See Art. 28 of Law. No. 450. 19 June 2013.
[264] *Data Protection in Africa: A Look at OGP Member Progress*.(Supra note 261) P.159.

The other two areas analysed are the creation of *Data Processing Registers*[265] and the use of *Terms of Service Icons* which does not exist in any of the Data Protection Laws enacted on the African continent.

On the other hand, the creation of Data Processing Registers exists in a dozen legislations continent-wide, including in Cote d'Ivoire. To be effective, and to contribute to transparency and enable the exercise of data subject rights, the register must be accessible which requires digital access.

In the specific case of the Ivorian legislation, a number of formalities must occur before personal data is allowed to be processed. The treatment of personal data is subject to prior notification to the personal data protection body(art.5).

Article 5 went on to state that *"The statement includes a commitment that the processing meets the requirements of the law".* If article 6 enumerates the kind of data processing exempted from prior notification (see Art.6, p141), article 7 describes those types of data processing and / or collection which require prior authorization from the Protection Authority:

> *Art.7:* are subject to prior authorization by the data protection body before implementation:
>
> - *The processing of personal data relating to genetic, medical data and scientific research in these areas;*
> - *The processing of personal data on data relating to offenses, convictions or security measures imposed by the courts;*
> - *Processing on a national identification number of the same nature, such as telephone numbers;*
> - *The processing of personal data with biometric data;*

[265] *Data Protection in Africa: A Look at OGP Member Progress*. (Supra note 261) P.159.

- *The processing of personal data having a pattern of public interest, particularly for historical, statistical, or scientific purposes;*
- *The transfer of personal data considered to a third country.*
-

The last part of article 7, which is related to the transfer of personal data to a third country, was put to test in a decision[266] (No.2016-0215) by the Protection Authority, dating November 22, 2016, on the authorization of data processing by Citibank Cote d'Ivoire (Mobile Pass). In its decision (art.4), the Protection Authority said:

> *Citibank Cote d'Ivoire is authorized to communicate the processed data to its authorized agents and to those of the public authorities of the Republic of Côte d'Ivoire, acting within the framework of their missions.*
> *It is prohibited for Citibank Cote d'Ivoire to transfer data processed to third countries without prior authorization from the Protection Authority.*

In other words, Citibank Cote d'Ivoire needed to submit a separate application for the transfer of personal data to its sister company, Citibank London, UK, a third country and obtain the said authorization to do so.

The Protection Authority in that decision, recognizes the right of Citibank Cote d'Ivoire to process the personal data of its customers using its product, the Mobile Pass, to communicate the processed data to its agents in Cote d'Ivoire but not to its sister company Citibank London without a specific application solely aimed at transferring the processed data to a third country that satisfy the requirements of the Ivorian law regarding data processing.

The request for data processing authorization can be made to the Protection Authority by email (art.10). The Protection Authority has one month to make its decision known to the applicant, but

[266] Protection Authority. (2016). Decision- No.2016-0215- on Authorization of Data Processing by the Company Citibank Cote d'Ivoire P.L.C. Retrieved December 25, 2021, from https://www.artci.ci/images/stories/pdfenglish/decisions_conseil_reg_english/decision_2016_0216_english.pdf

that timeline can be extended for another month (art.11) with a motivated reason by the Protection body.

The same (art.11) says that the lack of response of the data protection body within the time limit is equivalent to a rejection of the statement or request for authorization. Like in other legislations worldwide, mandating the express consent of the data subject before any data processing, article 14 of the Ivorian law recognizes this right of the data subject to give an informed consent to the collection and processing of his personal data with some notable exceptions:

> *Art.14*: *The processing of personal data is considered legitimate if the person concerned gives his express consent.*
> *However, there may be exceptions to this requirement of consent when the responsible person of the processing is duly authorized, and the processing is necessary;*
> *- Either for the compliance with a legal obligation to which the responsible person of the processing is subject;*
>
> *- or for the execution of a task in the public interest or in the exercise of official authority vested in the responsible person of the processing or the third party to whom the data are disclosed;*
>
> *- or for the execution of a contract to which the concerned person is a party or the execution of pre-contractual measures taken in the application;*
>
> *- or for safeguarding the interests or fundamental rights and freedoms of the concerned person.*

The law obliges the person responsible for the processing to choose a subcontractor to do the processing and both the person responsible for the processing and the subcontractor are obligated to make sure the processing follows the law (art.20)[267]. Here, the Ivorian Lawmaker puts the onus on both the person seeking the processing of data and the third-party executing the tasks of collecting and processing the data. It means that third parties doing the work of collecting and processing personal data on behalf of the person seeking the processing can be held liable for the violation of the law with regard to personal data processing in Cote d'Ivoire. Direct marketing using the personal data of a nonconsenting individual is punished by the law (art.22).

[267] See Art.20 of Law. No. 450. 19 June 2013.

With respect to the transfer of personal data to third countries, the law imposes some conditions: Art.26: *The person responsible for the processing can be allowed to transfer personal data to a third country only if the state provides a higher level of protection or equivalent privacy, freedoms, and fundamental rights of individuals with regard to the processing which the data are or may be subjected. Before any actual transfer of personal data to that third country, the person responsible for the processing must first obtain the permission of the Protection Body.*
The transfer of personal data to third countries is subject to regular monitoring of the data protection body in light of their purpose.

Thus, the decision by the Protection Body (No.2016-0215) to deny the company Citibank Cote d'Ivoire, the right to transfer personal data to its sister company Citibank London without a proper request. It means that, Citibank Cote d'Ivoire had to show that the third country, here, the UK satisfied all the requirements of article 26, among others, a higher level of protection or equivalent privacy, freedoms, and fundamental rights of individuals with regard to the processing which the data may be subjected to.

In practice, Citibank needed to submit a specific application regarding personal data transfer to Citibank London instead of just mentioning it in its application for the processing of the personal data of its customers using its product, the Mobile Pass.

Whoever obstructs the Protection Body in any way can held liable for the obstruction (art.45). In a node to civil rights advocates in Cote d'lvoire, the law in its article 47 says:

The data Protection Body ensures that the use of Information and Communication Technologies shall not affect or does not include a threat to freedom and privacy for users located throughout the national territory[268].

[268] See Art.47 of Law. No. 450. 19 June 2013.

In line with its regional obligations, Cote d'Ivoire has implemented a personal data protection law in line with the ECOWAS Supplementary Act A/SA.1/01/10 as the Oxford Business Group[269] pointed out in its 2019 report about Cote d'Ivoire.

In their report, the Oxford Business Group identified four (4) principles governing personal data processing through Law No. 450. 19 June 2013 which are:

- ✓ The legality principle relating to Article 15 of the law, according to which processing must follow licit and loyal principles;
- ✓ The finality principle, related to the responsible collection of data to be processed for a pre-determined, explicit, and legitimate purpose. The data collection must not be treated at a later date in a manner that is incompatible with the initial agreement.
- ✓ The proportionality principal results from Article 16 and 27 of the law: data must be adequate, relevant, and non-excessive with regard to the finality for which they are collected and processed at a later date. Furthermore, file interconnection is unauthorized unless it presents a "legitimate interest," under the condition of the "relevant principle" of data sets subject to interconnection; and
- ✓ The legitimacy principle, mentioned in Article 14 and according to which the person in question must have expressed their consent prior to data processing.

To sum up, the Personal Data Protection Act of Cote d'Ivoire, is similar to other African nations. The universality of the public's right to privacy in every nation makes it fairly reasonable to find the same types of legislations dealing with privacy.

As always, the most important issue is not the taking of the law, rather its enforcement by the justice system which in the case of Cote d'Ivoire, is flawed in every metrics.

Besides, the Personal Data Protections Act, the Ivorian parliament adopted on the same day, the Electronic Transactions Act which we are going to analyze in the next section.

[269] *The legal framework principles guiding the handling of personal data in Côte d'Ivoire*. (2019). Oxford Business Group. https://oxfordbusinessgroup.com/analysis/authorised-use-four-principles-guiding-handling-personal-data

3-5: The Electronic Transactions Act

In accordance with the Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS, Cote d'Ivoire through its parliament enacted the Electronic Transactions Act also known as Law No. 2013-546 on July 30th, 2013.

The ECOWAS Supplementary Act on electronic transactions was in part based on the Supplementary Act A/SA/01/07 of 19 January 2007, which prescribed the harmonization of the policies and regulatory framework of the Information and Communication Technologies sector.

The aim pursed by ECOWAS has always been about judicial cooperation and legislations harmonization within the regional organization. The Electronic Transactions Act or Law No. 2013-456 reprises word for word, the Supplementary Act on Electronic Transactions within ECOWAS.

The same is also true as we previously saw for the *Personal Data Protection Act* and the *Fight Against Cybercrimes Act*. The Electronic Transactions Act of Cote d'Ivoire in its first chapter, defines Electronic Commerce[270] as any economic activity by which a person offers or ensures, at a distance and by electronic means, the supply of goods and the provision of services.

Also included in the field of electronic commerce are service provision activities such as those consisting in providing online information, commercial communications, search tools, data access and retrieval, access to a data network, communication, or hosting of information, even if they are not remunerated by the beneficiaries.

The definition of electronic commerce by the Ivorian legislator is quite broad and somehow confusing toward the end of the definition. The first part of the definition - any economic activity

[270] See Law No. 2013-456, 30 July 2013 a.k.a Electronic Transactions Act. First chapter, Definitions.

by which a person offers or ensures, at a distance and by electronic means, the supply of goods and the provision of services- is clear and simply means traditional economic activity done using the Information and Communication Technologies of today.

The second portion of the definition is about activities specific to the Internet that have a monetary value which is quite realistic in today's world. For example, paying money to get your website hosted on a third-party server.

The end of the definition talks about communication, hosting of information even if they are not renumerated (paid for) by the users. Can we talk of e-commerce when Yahoo allows me to have a free email address where my messages sent or received are kept on Yahoo's servers for free?

The answer is obviously no, since there is no bargain-for-exchange, something that causes a legal detriment to the beneficiary of such service. Certainly, a clarification is needed from the legislator with regard to this point.

The chapter 3 in its article[271] 5 requires the offeror of electronic business to let the offeree have an easy, permanent access to his information through certain means enumerated therein.

The law also through article 6 requires the pricing of goods or services offered by electronic means, to be in a clear and unambiguous manner, namely where taxes and cost of delivery are included.

This article reprises Article 5 of the Supplementary Act[272] on Electronic Transactions within ECOWAS regarding the price when the seller mentions it. For the applicability of the law in case of a dispute, article 6 of the law states that Ivorian jurisdictions are competent to resolve any legal

[271] See Article 5, Law No. 2013-456, 30 July 2013
[272] See Economic Organization of West-African States. (2010). *Supplementary Act on Electronic Transactions within ECOWAS*. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

matter having to do with electronic commerce if one party to the contract is located / has residency in Cote d'Ivoire or is an Ivorian national.

There is an exception in that the parties can freely choose the authority competent to resolve their eventual disputes. This rule is quite universal and is accepted by most countries when it comes to traditional commerce.

To apply it to electronic commerce can be challenging at times due to the ubiquity of the Internet which is everywhere and nowhere at the same time but the principle of the authority of the place where part or all of the facts took place being legally competent is accepted by most jurisdictions.

Article[273] 9 went further by stating that in the case, where the parties have not decided on the competent jurisdiction, the Ivorian laws apply if the activities of one of the parties occurred on Ivorian soil or are accessible to users in Cote d'Ivoire and there is a significant nexus between the provision of services and the users of internet services in Cote d'Ivoire, namely through the language used, the currency employed, the products offered and the domain name used by the website offering its services.

This is true for technology giants like Facebook, Google, Amazon who tend to localize their services in the respective countries where they are operating from.

For example, the domain name www.google.ci refers to Google in Cote d'Ivoire. The downside of Article 9 is that small and medium size companies offering their services worldwide do not always localize their services due to the cost involved.

[273]See Article 9, Law No. 2013-456, 30 July 2013.

These websites can be only in English, with the Dollar as the currency and the domain name by excellence being the .com. In these cases, there is not a sufficient nexus between the business offering its services and products and the Ivorian users of such services.

We think that the Article 9 should encompass all online services/products accessible to Ivorian users in Cote d'Ivoire at the time of an online transaction involving them and an outside business (foreign).

The chapter 4 of Law No. 2013-456, 30 July 2013, is dedicated to electronic advertising which corresponds to chapter 3 of the Supplementary Act on electronic transactions within ECOWAS. Article 10 of the chapter 4 mandates that any online advertisement shall be clearly identifiable as such. Such identification must include the identity of the individual or legal entity on whose behalf the advertisement is done.

Direct prospecting[274] (Article 14) through electronic means is forbidden when using the contact information of someone who has not given his or her consent. Some exceptions do exist within Article 14 where direct prospecting through electronic mail is acceptable:

- The recipient's contact details have been collected with full knowledge of the facts, directly from himself.
- Direct prospecting is addressed to the subscribers or customers of a business.

Article[275] 15 opens the possibility of recipients of advertising e-mail to opt-out from future e-mails without incurring any cost to them. The chapter 5 of the Act is dedicated to the conclusion of a contract by electronic means.

[274] See Article 14, Law No. 2013-456, 30 July 2013.
[275] See Article 15, Law No. 2013-456, 30 July 2013.

Regarding the freedom of choice of electronic means, Article[276] 17 says that no individual shall be compelled to commit himself legally through electronic means. This freedom of choice of electronic means echoes Article 22 of the Supplementary Act[277] on electronic transactions within ECOWAS. As Thomas Smedinghoff[278] pointed out, all transactions must comply with the substantive legal requirements applicable to the specific form of transaction.

Contracts involving the sale of goods, for example, must comply with substantive rules that require offer, acceptance, signature, consideration, and so forth. They are also governed by substantive rules addressing issues such as warranties, mistake, risk of loss, breach, liability, and termination.

Here, the Electronic Transactions Act like the Supplementary Act on Electronic Transactions within ECOWAS does not address the substantive rules such as offer, acceptance, consideration etc. because the aim of the Supplementary Act was to address a series of electronic-specific legal requirements that focus on how to do the transaction in electronic form.

In order to transact electronically securely and efficiently, Smedinghoff[279] asks three (3) fundamental questions related to the authorization, the electronic requirements, and the security of those transactions. Does the Supplementary Act and the Electronic Transactions Act of Cote d'Ivoire for that matter, answer the 3 questions posed by Smedinghoff?

[276] See Article 17, Law No. 2013-456, 30 July 2013
[277] See Economic Organization of West-African States. (2010). *Supplementary Act on Electronic Transactions within ECOWAS*. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf
[278] Smedinghoff, Thomas J., The Legal Challenges of Implementing Electronic Transactions (September 28, 2008). Uniform Commercial Code Law Journal, Vol. 41, No. 3, 2008. *"The electronic-specific legal requirements are often set forth in general purpose e-transaction laws and address issues such as how to electronically satisfy paper-based requirements for a signature or an original and how to properly protect the interests of the various parties to the transaction."*
[279] Ibid.

With regard to the *Authorization*, he asks:

> *Can this transaction be done in electronic form?*
>
> *Does existing law in the relevant jurisdictions allow the parties to conduct the proposed transaction in electronic form, or does existing law either prohibit doing the transaction electronically or present legal barriers that make its enforceability uncertain[280]?*

The question of the legality of electronic transactions in Cote d'Ivoire is clearly answered by the Electronic Transactions Act a.k.a Law No. 2013-456, in that it officially recognized and set the rules of electronic commerce in the land.

The second question posed by Smedinghoff is as follows:

> *What are the electronic-specific rules?*
>
> *What electronic-specific rules apply, and what requirements must be satisfied to ensure that the transaction is legally valid and enforceable? The focus here is on electronic procedural requirements applicable to all transactions, not on the substantive legal requirements for this particular transaction[281].*

The second question is easily answered by the Supplementary Act on Electronic Transactions within ECOWAS from which derived Law No. 2013-456 or Electronic Transactions Act. Indeed, both Acts define the general requirements for all electronic transactions occurring within ECOWAS and in Cote d'Ivoire.

Does an electronic signature is equivalent to a written signature? Can a business transaction take place online at least, legally?

All these questions have their tentative answers in both the Supplementary Act of ECOWAS and the Electronic Transactions Act of Cote d'Ivoire.

[280] Smedinghoff, Thomas J., The Legal Challenges of Implementing Electronic Transactions. (Supra note 278) P.171.
[281] Ibid.

The third and most consequential question Smedinghoff asks is this:

> *Is the transaction trustworthy?*
>
> *What is required before the parties will be comfortable relying on the transaction? How can the parties be sure who sent an electronic message or who signed an electronic record? How can the parties be sure that the record has not been altered since it was created? Are the electronic records sufficiently trustworthy such that it will be enforced by a court[282]?*

The question of the security of e-transactions between businesses and consumers and even among businesses is at the heart of the whole issue of cybersecurity around the world.

The trustworthiness of online interactions not just for business purposes but also for any other form of online communication is dependent on a number of factors, among them, the regularity of transactions between the parties, how well they know each other, the use of offline means to verify when in doubt, having a reliable and secure information system and many more actions to safeguard one's online presence.

Even taking the maximum precautions by following industry standards plus other measures, the security of online transactions is never guarantee 100%.

The same is also true in the material world. An article[283] on the security of e-commerce revealed that online businesses experienced 32.4% of all successful cyber-attacks in 2018. Therefore, a

[282] Smedinghoff, Thomas J., The Legal Challenges of Implementing Electronic Transactions. (Supra note 278) P.171.

[283] Varghese, J. (2021). *Ecommerce Security: Importance, Issues & Protection Measures*. https://www.getastra.com/blog/knowledge-base/ecommerce-security/ *"Online buyers face uncertainty and complexity during critical transaction activities. Such activities include payment, dispute resolution, and delivery. During those points, they are likely to fall into the hands of fraudsters. Businesses have improved their transparency levels, such as clearly stating the point of contact when a problem occurs. However, such measures often fail to disclose fully the collection and usage of personal data."*

serious business should, employ rock-solid eCommerce security protocols and measures. It will keep the business and customers free from attacks.

One must say that the author is quite optimistic about businesses and customers being free from cybercriminals just by applying "rock-solid" eCommerce security protocols.

First of all, being 100% secure online is an illusion as we previously said.

Secondly, those security protocols cost too much money, small businesses do not usually have. In the end, the security aspect of e-commerce is as complete as the security of physical businesses, meaning the best tools are employed to guarantee a maximum security but users and businesses ought to know that it is not 100% guaranteed.

The Electronic Transactions Act allows the parties to a contract to exchange all documents by electronic means (Article 18 al).

In other words, a contract entered into online by two or more people and or entities is legally enforceable in Cote d'Ivoire.

The chapter 6 of the Act is about the legality of the electronic written form. The Article 23 of the Act states that:

> *Writing in electronic form is accepted as a mode of proof in the same way as writing on paper ....*

Therefore, Ivorian businesses and consumers should be confident to enter into contractual obligations online without fearing the illegality of those online transactions. Article 25 reinforces article 23 by stating that:

> *The copy or reproduction of an act passed electronically on paper has the same probative value as this act….*

The Electronic Transactions Act of Cote d'Ivoire naturally talks of the security of electronic transactions in the country. An entire chapter (7) is dedicated to that effect. Article 36, al. 2 states:

> *When the signature is electronic, it consists of the reliable use of an identification process guaranteeing its link with the act to which it is attached*[284].

Here, the Ivorian legislator wants to reassure online businesses and customers of the legality of the electronic signature as long as it identifies the authors of the act to which it is attached. The viability of the electronic signature cannot be opposed on the sole account that it is electronic and not a physical writing (Article 37).

An electronic certificate delivered by a provider outside of Cote d'Ivoire is as legal as the one delivered by a company operating in Cote d'Ivoire (Article 38).

In sum, Law No. 2013-456 on electronic transactions in Cote d'Ivoire is wholly or partly based on the recommendations of the ECOWAS Supplementary Act on electronic transactions within the regional bloc, which in fact relied heavily on European legal instruments like the European Union Data Protection Directive (95/46/EC). Therefore, it is natural for us to measure the impact of international treaties on the legal apparatus set in motion in West-African countries like Cote d'Ivoire.

As the saying goes, there is no need to waste a lot of time for no reason. That being said, the African cultural, political, and economic realities require some degree of caution when copying European legal instruments due to the differential in terms of development and individual freedoms.

[284] See Article 36, Law No. 2013-456, 30 July 2013.

3-6: The Influence of International Treaties

When the legal aspects of the internet arose in the 90s, the Council of Europe[285] was the first international organization to tackle those issues. The Council of Europe was born in 1949 to unify the European continent after the second world war.

[285] Council of Europe. (2000). *Who we are*? The Council of Europe in Brief. https://www.coe.int/en/web/about-us/who-we-are?l=sq

Wim de Leeuw[286] explains here what the Council of Europe was all about:

> *Shortly after the end of World War II, several movements and activities were born that were dedicated to European unification. As an overall result, the Council of Europe was founded as an international political institution in 1949. It is designed only with international cooperation in mind. The general aims of the Council of Europe are to:*
>
> - *Protect human rights, democracy, and the rule of law in all member states;*
> - *Promote awareness and encourage Europe's cultural identity and diversity;*
> - *Seek solutions to (social) problems facing European society;*
> - *Consolidate democratic stability in Europe;*
> - *Promote social cohesion and social rights; and*
> - *Promote and develop a European cultural identity with emphasis on education.*

[286] National Research Council (US) Institute for Laboratory Animal Research. The Development of Science-based Guidelines for Laboratory Animal Care: Proceedings of the November 2003 International Workshop. Washington (DC): National Academies Press (US); 2004. The Council of Europe: What Is It? Available from: https://www.ncbi.nlm.nih.gov/books/NBK25399/ Council of Europe: How does it work:" The headquarters of the Council of Europe, Le Palais de l'Europe, is situated in Strasbourg, France. The Committee of Ministers is the decision-making body of the Council of Europe. It is composed of the Ministers of Foreign Affairs of the member states. This body officially adopts Conventions, Resolutions, Agreements, and Recommendations. The Committee of Ministers also ensures that the conventions and agreements are implemented. In addition, there are two other institutions: (1) The Parliamentary Assembly is the organization's deliberative body, the members of which are appointed by national parliaments. (2) The Congress of Local and Regional Authorities of Europe is a consultative body that represents local and regional authorities. Governments, national parliaments, and local and regional authorities are thus represented separately at the Council of Europe level. The main tools of the Council of Europe to achieve its objectives are the following legal instruments: Recommendations—often referred to as "soft law." There is no legal obligation to follow or implement these recommendations; and
Conventions or treaties concluded between states. The member states are not legally obliged to sign a Convention, although they may be expected to do so since under the Council of Europe's Statute, they have undertaken to "collaborate sincerely and effectively in the realization of the aim of the Council." Nonetheless, there are diverse ways a member can deal with a Convention. It may choose to ignore the Convention as being not relevant or not applicable to the national situation. By taking that position, a member is not obliged to comply with its provisions. A member can sign the Convention, thus recognizing the value and existence of the Convention. After having signed a Convention, a member is still not obliged to comply with the provisions of the Convention. However, once a state has signed and ratified (i.e., its Parliament has approved the instrument) and the Convention has become effective, the state will be morally and legally bound under international law to implement the Convention. Thus, the state has become a Party to that Convention and must ensure that the provisions will be respected on its territory. Most Council of Europe Conventions are not directly applicable within a member state; they are not "self-executing." The most common way for a state to implement them is to enact appropriate national legislation or to adapt its existing domestic law to make it correspond to the rules in the Convention."

The Council of Europe has been continually active when it comes to data protection within the confines of the European Union by adopting the EU Data Protection Directive (95/46/EC)[287] which is the ancestor of the General Data Protection Regulation or G.D.P.R.

In 2001, the Council of Europe adopted the Budapest Convention[288]on cybercrime. These initiatives of the Council of Europe have had and continue to have an impact on regional initiatives to combat data breach and theft and cybercrimes.

The Economic Community of West-African States (ECOWAS) has done just that by adopting in 2010, a legally binding act, the Supplementary Act on Personal Data Protection within ECOWAS that was strongly influenced[289] by the EU Data Protection Directive (95/46/EC). Let us analyse the Budapest Convention followed by the General Data Protection Regulation or G.D.P.R.

3-6-1: The Budapest Convention

The convention on cybercrime by the Council of Europe was launched in November 2001. The convention is the first international treaty[290] on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

---

[287] EU. (2003). *EUR-Lex - 31995L0046 - EN - EUR-Lex*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1995/46/oj

[288] Council of Europe. (n.d.). *What are the benefits and impact of the Convention on Cybercrime?* Cybercrime. https://www.coe.int/en/web/cybercrime/home

[289] Greenleaf, Graham, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108 (October 19, 2011). International Data Privacy Law, Vol. 2, Issue 2, 2012, UNSW Law Research Paper No. 2011-39, Edinburgh School of Law Research Paper No. 2012/12, Available at SSRN: https://ssrn.com/abstract=1960299

[290] *The Budapest Convention on Cybercrime: a framework for capacity building – Global Forum on Cyber Expertise*. (n.d.). Thegfce.Org. Retrieved January 12, 2022, from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/

For the countries who helped open the Budapest Convention for signature, it reconciles the vision of a free Internet, where information can freely flow and be accessed and shared, with the need for an effective criminal justice response[291] in cases of criminal misuse.

Restrictions are narrowly defined; only specific criminal offences are investigated and prosecuted and specified data that is needed as evidence in specific criminal proceedings is secured, subject to human rights and rule of law safeguards.

Among the benefits touted by the signatories is that the Budapest Convention requires States to ensure that the offences against and by means of computers of Articles 2 to 12 are criminalised in their domestic law[292], and that their criminal justice authorities have the powers prescribed in their procedural law not only to investigate cybercrime, but any offence where evidence is in electronic form.

Also touted as a benefit is the fact that, domestic legislation consistent with the Budapest Convention further facilitates international cooperation in that it helps meet the dual criminality requirement. As of May 2020, 76 nations were either parties to the convention on cybercrime (65) or are signatories (3) or had been invited to accede (8). A recent survey[293] has shown that in fact 92 % of nations worldwide have used or are using the Budapest Convention as a guideline or as a source for reforming their domestic legislation.

The Budapest Convention have inspired member States of the Economic Organization of West-African States when drafting the supplementary Acts on personal data protection and on electronic

[291] Council of Europe. (2020). *The Budapest Convention on Cybercrime: benefits and impact in practice*. coe.int. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac
[292] Ibid.
[293] Ibid.

transactions within ECOWAS. The same can be said of the Directive on fighting cybercrimes of 2011 by ECOWAS.

Graham Greenleaf[294] pointed out the fact that examination of the current 29 national data privacy laws outside Europe shows that the 'European standards' have had by far the greater influence outside Europe, and this is increasing.

In the real world, cooperation between West-African nations and the European Union, the Council of Europe and the African Union Commission is so advanced that those institutions have organized the second African Forum on cybercrime in June 2021. The organizers noted that the heterogeneous legal frameworks[295], lack of national strategies, and information infrastructures that are still scarcely secured in a number of countries, has made the African region a vulnerable target for cyber-criminal activities.

A direct impact is evidenced not only on citizens, but also – and most worryingly – on the social stability of the States. Cote d'Ivoire, through bilateral or multilateral mechanisms, receives help not only from the European Union, but also from France and the United States in the field of cyber awareness.

Most of the Ivorian cyber laws (Fight Against Cybercrimes Act, Personal Data Protection Act, and the Electronic Transactions Act) have been more or less influenced by international treaties like the Budapest Convention. In fact, Cote d'Ivoire has ratified the Budapest Convention[296] in 2019.

---

[294] Greenleaf, Graham, The Influence of European Data Privacy Standards Outside Europe. (Supra note 289) P.178.
[295] EU, CE, AU Commission. (2021). *Second African Forum on cybercrime to take place on 28 and 29 June online*. https://www.coe.int/en/web/human-rights-rule-of-law/-/second-african-forum-on-cybercrime-to-take-place-on-28-and-29-june-online
[296] Deutsche Welle. *Abidjan strengthens its system against cybercrime*. (2019). https://www.dw.com/fr/la-c%C3%B4te-divoire-renforce-son-dispositif-contre-la-cybercriminalit%C3%A9/a-50706017 "In order to strengthen

This ratification now allows Côte d'Ivoire to benefit from international collaboration in its fight, explains a police officer who requested anonymity.

International cooperation is paramount in the fight against cybercriminality as one Ivorian cybercrime expert, Aristide Ouattara[297] pointed out:

> *International collaboration is especially important. Because you can be attacked in Côte d'Ivoire by a hacker based in North Korea. So, we have to set up international surveillance systems.*

The cooperation between Cote d'Ivoire and its international partners extend to organizations such as Europol and or Interpol which respectively translate into European Police (Europol) and the International Police (Interpol).

The country also benefits from the aid offered by the United States Justice Department and its agencies like the Federal Bureau of Investigations (FBI) through information-sharing, training for Ivorian stakeholders at all levels.

In the absence of a United Nations treaty agreed upon by all nations, the Budapest Convention is a viable alternative for developing countries dealing with the scourge of cybercrimes like Cote d'Ivoire.

Though the ratification of the Budapest Convention by African nations is more than helpful in the near – term, one must acknowledge that this convention is the product of the Council of Europe, thus largely based on the European social, legal, economic, and political environments. Therefore,

---

its fight system, Côte d'Ivoire ratified, in March 2019, the Budapest Convention on Cybercrime of the Council of Europe. This ratification now allows Côte d'Ivoire to benefit from international collaboration in its fight, explains a police officer who requested anonymity.
"We will rather intervene, for example, in investigations at the level of State attacks. Because there are many cybercriminal groups which try to infiltrate an organization for political or electoral reasons. So, we sometimes collaborate with organizations such as Europol or Interpol. But also, with France in any case, with the State organization for the prevention and detection of cyber-risks."

[297] Deutsche Welle. *Abidjan strengthens its system against cybercrime*.(Supra note 296) P.180.

it is paramount for African countries ratifying the Budapest Convention to strive in the long term through the African Union, to ponder a convention that takes the African environment into account.

It has been done in 2014 for the Personal Data Protection by the African Union Commission. In the meantime, taking advantage of the Budapest Convention, but also of the General Data Protection Regulation (GDPR) is the wise path to follow./.

3-6-2: The General Data Protection Regulation

The General Data Protection Regulation or GDPR is a European Union regulation on privacy and personal data protection, which was first published on April 27th, 2016, and went into effect on May 25th, 2018.

The GDPR is certainly the toughest privacy and security law in the world. The right to privacy was part of the European Convention on Human Rights of 1950, which states: "Everyone has the right to respect for his private and family life, his home, and his correspondence[298]."

Before the advent of the GDPR, the Council of Europe in 1995, considering the fact that the added information and communication technologies were posing new risks for personal privacy, adopted the European Data Protection Directive (95/46/EC), establishing minimum data privacy and security standards, upon which each member state based its own implementing law.

That directive was the one upon which the Economic Organization of West-African States or ECOWAS based its Supplementary Act on Personal Data Protection within ECOWAS. Most if not all of the regulations adopted around the world, including within ECOWAS are based on the principles outlined by the GDPR.

For the protection of personal data, here are some definitions found in the GDPR that are also found in the Supplementary Act on personal data protection within ECOWAS and in Cote d'Ivoire for that matter.

The definitions are taken from a website dedicated solely to the GDPR:

[298] Wolford, B. (2019, February 13). *What is GDPR, the EU's new data protection law?* https://gdpr.eu/what-is-gdpr/

Personal data *— Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.*

Data processing *— Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.*

Data subject *— The person whose data is processed. These are your customers or site visitors.*

Data controller *— The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.*

Data processor *— A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers like Tresorit or email service providers like ProtonMail*[299].

All these definitions regarding data processing are the same found in the Ivorian law related to the protection of personal data.

The GDPR defines seven (7) protection and accountability principles that are also present both in Supplementary Act of ECOWAS and the Ivorian law on personal data protection.

Here are the seven principles[300] of the GDPR when it comes to data processing and or collection:

1. ***Lawfulness, fairness, and transparency*** *— Processing must be lawful, fair, and transparent to the data subject.*
2. ***Purpose limitation*** *— You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.*
3. ***Data minimization*** *— You should collect and process only as much data as absolutely necessary for the purposes specified.*
4. ***Accuracy*** *— You must keep personal data accurate and up to date.*
5. ***Storage limitation*** *— You may only store personally identifying data for as long as necessary for the specified purpose.*

[299] Wolford, B. (2019, February 13). *What is GDPR, the EU's new data protection law?* (Supra note 298) P.183.
[300] Ibid.

6. ***Integrity and confidentiality*** *— Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption).*
7. ***Accountability*** *— The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.*

The influence of international treaties like the Budapest Convention and the General Data Protection Regulation (GDPR) on legislations adopted in developing countries like Cote d'Ivoire is undeniable as one can see here with these GDPR principles also present in the Ivorian law (See Law No. 450 19 June 2013 on Personal Data Protection).

Technology is moving too fast for the law to always catch up with it in a timely manner. To avoid unnecessary waste of time, many countries including African ones, are working with the most advanced economies mostly in the European Union and North America to be up to date of technology changes and their implications from a legal standpoint.

These collaborations are extremely important if we are to harmonize legislations worldwide to fight and win against cybercriminality, in the absence of a United Nations treaty on cybercrime. In that respect, the Budapest Convention and the General Data Protection Regulation of the Council of Europe are the prime examples nations like Cote d'Ivoire must follow while at the same time adapting these laws to the local environment.

It is fundamental, however, to enforce cybercrime laws to the fullest extent of those laws from the investigations of cybercrimes to the sentencing of cybercriminals after their prosecution.

CHAPTER 4: Enforcement of Cybercrimes Laws in Cote d'Ivoire

The enforcement of cybercrime laws in Cote d'Ivoire is no different than the enforcement of laws in general. The justice system in Cote d'Ivoire like in most West-African countries suffers from many ills among them, the lack of a qualified and skilled personnel at all levels of the judiciary, the corruption within law enforcement agencies (Police, Judiciary Police (Investigative unit), Economic Police, etc.) but also within the judiciary itself (Judges, Lawyers, and other personnel).

As the saying goes in Cote d'Ivoire, if you are poor, you will lose any lawsuit against the rich and well-connected. An international study[301]co-led by UCLA political scientist Graeme Blair and related to community policing efforts in six developing countries, shows that they were ineffective in reducing crime or restoring civilians' trust in law enforcement.

According to the article[302], the practice of community policing was developed in the U.S. in the early 1990s and has since gained popularity across the world. It typically involves collaboration between police and neighborhood watch groups and introduces new mechanisms for citizens to report crimes as well as abuses of power by police.

In Cote d'Ivoire, where community policing is inexistent, the police have a free reign when it comes to policing anything. Therefore, it is not surprising to find out that the enforcement of cybercrime laws in the country, suffers the same ills as in other areas of law enforcement. Most law enforcement officers are ill-paid, and so extortion through threat of jail time is routine among them. Even Judges, magistrates and other personnel are also ill-paid, making corruption in their

[301] UCLA. (2021). *In developing countries, no quick fix for strengthening police–civilian relations*. Newsroom.ucla.edu. https://newsroom.ucla.edu/releases/community-policing-developing-nations "The data showed no improvements in terms of trust in law enforcement, crime reduction or cooperation between civilians and police — the three primary benefits touted by advocates of community policing."
[302] Ibid.

ranks inevitable. We will analyse the specific investigations of cybercrimes in Cote d'Ivoire through the lens of the Platform Against Cybercrime (PLCC).

4-1: The Investigation of Cybercrimes

A cybercrime investigation[303] is the process of investigating, analysing, and recovering forensic data for digital evidence of a crime. Examples of evidence in a cybercrime investigation include a computer, cellphone, automobile navigation system, video game console, or other networked device found at the scene of a crime.

This evidence helps cybercrime investigators determine the perpetrators of a cybercrime and their intent. In order to successfully dismantle cybercrime networks, a number of investigation techniques are used by cybercrime investigators. Among those techniques are:

> ***Performing background checks****: At this level of the investigation, one must determine the when, where, and who might be involved in the crime, object of the investigation.*
>
> ***Information gathering****: This technique is one of the most critical in cybercrime investigations. Here, investigators ask questions such as: What evidence can be found? What level of access to sources do we have to gather the evidence? The answers to these and other questions provide the foundation for a successful investigation.*
>
> ***Running digital forensics****: Cybercrime investigators use their digital and technology skills to conduct forensics, which involves the use of technology and scientific methods to collect, preserve, and analyse evidence throughout an investigation. Forensic data can be used to support evidence or confirm a suspect's involvement in a crime.*
>
> ***Tracking the authors of a cybercrime****: with information about a crime in hand, cybercrime investigators work with internet service providers and telecommunications and network companies to see which websites and protocols were used in the crime. This technique is also useful for monitoring future activities through digital surveillance. Investigators must seek permission to conduct these types of activities through court orders.*

[303] *Cyber Crime Investigation: Making a Safer Internet Space*. (2021, September 8). Maryville Online. Retrieved January 19, 2022, from https://online.maryville.edu/blog/cyber-crime-investigation/

Cybercrime may come to the attention of Law enforcement either after the fact or while in progress which is extremely rare. As Professor Grabosky[304] pointed out, the initial indication of cybercrime is an attempt at unauthorized access.

When the unauthorized access is detected, he posits, it may not be apparent if the intruder is a teenage adventurer, a technician working for an organized criminal group, or the intelligence service of a foreign state.

If in most cases, the unauthorized access can be traced to an IP address, when the perpetrator is either new or lack experience in hacking, the situation is different when the perpetrator is a veteran of cybercrimes and usually covers his or her tracks by encrypting her presence.

In the latter case, law enforcement encounters some difficulty to pinpoint the origin of the attack.

Professor Grabosky[305] also notes the variety of cybercrimes scenes going from a workstation within a big organization to the comfort of one's living room.

In Africa, in general, cybercriminals operate from cybercafes and as they become increasingly financially powerful, from private residences in unsuspecting areas of big cities like Lagos or Abidjan in Cote d'Ivoire, where the Ivorian government has created an agency tasked with investigating cybercrimes in the country.

This agency is called Platform Against Cybercrime or by its acronym PLCC. We will analyse the role played by this agency in the investigations of cybercrimes in Cote d'Ivoire.

[304] Grabosky, P. (2015). *Cybercrime. (Supra note 155)P.103.*
[305] Ibid.

4-1-1: The role of the Platform Against Cybercrime (PLCC)

Cote d'Ivoire is one of the three (3) countries in West-Africa, hardest hit by cybercrimes due to its position as a regional driver of immigration. The other two (2) being Nigeria and Ghana.

Since the early 2000s, cybercrime has grown in Côte d'Ivoire to the point that this phenomenon has a strong impact on everyone's daily life as a report of the United Nations Office on Drugs and Crimes (UNODC)[306] posited.

The report cited the negative impacts of this phenomenon on the reputation of Cote d'Ivoire around the world. Here are some of the effects of cybercrime on the country:

- Brake on the development of the digital economy: discrediting of electronic systems: blocked IP addresses and credit cards.
- Bad reputation of the country: bad reputation of the institutions of the countries of origin of the offenses in the face of the great distress of the victims and the feeling of powerlessness of the police of the countries of origin of the victims.
- Moral bankruptcy of youth (mortgaged future): the lure of easy gain by increasingly young delinquents who drop out of school, in a country like Côte d'Ivoire where 4/5 of the population is under 35 years old. (Ritual crimes, sex, drugs, etc.)
- Obvious issue of safety of people and their property in virtual space: like the physical environment, public and private virtual spaces (people and companies) must benefit from a level of security guaranteeing trust and social peace.
- Fight against terrorism: the following aspects are each a challenge: (1) virtual space as a target, (2) planning and coordination environment, (3) communication and propaganda environment.

Conscious of the dangers posed by cybercriminality on the reputation of the country, Côte d'Ivoire has developed institutional and legislative countermeasures, some of which we have already dissected in this document.

[306] United Nations Office of Drugs and Crimes-UNODC-. (2014). *About the PLCC-Platform Against Cyber Crimes*. unodc.org. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Cote_DIvoire.pdf

Thus, Cote d'Ivoire took part in the adoption of the Directive C/DIR/1/08/11 on the fight against cybercrime within ECOWAS, the Supplementary Act A/SA.1/01/10 on the Protection of Personal Data and Privacy within ECOWAS and last but not least, the Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS.

At the National level, there have been a number of legislations to tackle cybercrimes, like the law on the Protection of personal Data (Law No. 2013-450), the law on the Fight Against Cybercrimes (Law No. 2013-451) and the law relating to the Protection of Electronic Transactions (Law No. 2013-546).

These laws have been supplemented by ordinances and decrees in their practical enforcement. A number of agencies were put in place to deal with the day-to-day operations related to the enforcement of the different cyber laws adopted by the Ivorian Parliament. Among them, are the creation of the Directorate of Computing and Technological Traces or DITT, its French acronym, by the national police, the creation of CI-CERT meaning Cote d'Ivoire Computer Emergency Response Team by the Authority for the regulation of Telecommunication of Cote d'Ivoire or ARTCI, its French acronym.

On September 2, 2011, through an agreement between the DITT and the ARTCI, was founded the Platform for the Fight Against Cybercrime or PLCC, its French acronym.

According to the report[307], the Ministry of the Interior and Security has restructured the National Police by creating the Department of Computing and Technological Traces (DITT) to respond more effectively to this security issue.

[307] United Nations Office of Drugs and Crimes-UNODC-. (2014). *About the PLCC-Platform Against Cyber Crimes*.(Supra note 306) P.189.

This reaction is all the more important since, in addition to attacks against computer systems and networks (computing and telecommunications), the use of technology in the commission of classic offenses has the effect of making them more complex and multiplying them.

The DITT thus defines two axes in the fight against cybercriminality according to the report:

- *Cybercrime investigation, where technologies and networks play a decisive role in the commission of the offence, in particular cases of pure cybercrime or use of complex technologies by offenders. This is the area of competence of the Platform for the Fight Against Cybercrime - PLCC.*
- *Technical support for the services in charge of classic criminal code offences, where investigators need expertise to collect and make technological traces intelligible. This support is provided by the Digital Forensics Laboratory - LCN.*

The operational and technical skills of the PLCC in the field of cybercrimes cover specific offenses linked to modern technologies and those whose commission is facilitated by the use of these same technologies. Here are some of the missions of the PLCC, the list being not exhaustive:

The mission of the PLCC is to:

1. *Conduct judicial investigations relating to offenses aimed at or using computer systems, provide technical assistance to the police services and related services responsible for applying the law during judicial investigations.*
2. *Contribute to the establishment of technical means and the development of expertise for the examination and tracing of information systems.*
3. *Conduct awareness-raising and information campaigns on cybercrime among the population and other public administration services and the private sector.*
4. *Participate in the definition and implementation of technical measures, organizational and regulatory measures in the fight against cybercrime.*
5. *Contribute to the technical training of staff to build capacity in the fight against cybercrime.*

The Platform for the Fight Against Cybercrimes comprises three (3) sections, namely the Investigation Department, and the Communication and Statistics Department.

The Investigation Department is responsible to investigate cybercrimes; it is led by the Judicial Police Officers (OPJ) whose role consists of the observation of offenses, the gathering of digital evidence and the search for the perpetrators of those offenses.

The Investigation Department has a Police Cooperation Service, which as its names indicates, is in charge of the cooperation between the PLCC and the Police forces of different countries in the context of investigations related to cybercrimes beyond state borders.

The Communication and Statistics Department is responsible for producing communication media, designing, and organizing events. The Department participates in meetings organized within the Department, in order to always have an up-to-date information and to distribute it. It is also responsible for the maintenance and development of information networks and correspondents inside and outside the Platform. Finally, it takes part in awareness-raising activities on cybercrime with target audiences. Practically, the communication and statistics service are split into two departments:

The communication department which is responsible for designing and coordinating all communication actions towards the public and the media. Its purpose is to make public and explain the action of the PLCC, to make it known and to disseminate its activities. This department consists of three (3) cells:

1. "Press communication" in charge of all relations with the media,
2. "Institutional communication" ensuring the creation and management of internal and external communication tools.
3. "Internet and Multimedia", responsible for updating the website or managing the PLCC's image (its e-reputation), through social networks. As of this writing, the website is nowhere to be seen, though they have a strong Facebook presence.

The statistics department's main activity is the production and dissemination of statistics on cybercrime. Its main mission is to collect data relating to judicial investigations into cybercrime offenses. As such, it collects and analyses data, is responsible for the production and distribution of activity reports through regular publications.

After dissecting the Agency responsible for the investigation of cybercrimes in Cote d'Ivoire, it is important to analyse how cybercriminals are prosecuted in Cote d'Ivoire. Are there differences in treatment of cybercriminals compared to ordinary criminals? We will also dissect the sentencing of cybercriminals, and later enumerate a number of obstacles when it comes to enforcing laws against cybercriminals./.

4-2: The Prosecution of Cybercriminals

Investigating and prosecuting cybercrimes is an arduous task for many reasons, among them, the transnational nature of the Internet, traceability issues, the technical know-how of Law enforcement etc.

In practical terms, there are many challenges in taking a cybercrime to trial as Self B.[308] rightly pointed out in her blog. She cited the fact that cyber criminals usually disguise their originating location by using various tools and methods of concealment, such as the use of virtual private networks, anonymizing network Tor, or other types of proxy servers.

Second, because crimes are digital, they span country borders and a large majority of hackers operate internationally, which prevents law enforcement officers from prosecuting these individuals without extradition.

Some clever cybercriminals use "handles" or pseudonyms and prefer the dark web as their "headquarters" from which they operate virtually "unknown." Others use VPNs and proxies to hide their true IP address which makes it extremely difficult to locate them.

That being said, the company that provides the proxy or VPN will usually have the real IP address in their records, but if it is not willing to voluntarily share this information, investigators would be powerless to compel it to do so, unless they secure a warrant.

[308] Self, B. (2016, March 30). *The Difficulties of Litigating Cyber Crime*. Law Enforcement Cyber Center. Retrieved February 22, 2022, from https://www.iacpcybercenter.org/the-difficulties-of-litigating-cyber-crime/ "In 2013, approximately 18 percent of cyber-attacks originated in the United States, with 30 and 28 percent of attacks originating in China and Romania respectively. Of the total, 25 percent of the attacks were not attributable to any specific country of origin. The international nature of cyber-attacks continues to present a significant challenge to law enforcement officers."

In the case of Cote d'Ivoire, a substantial number of cybercriminals are high school or college students who are not always as skilled as hackers in Eastern Europe. The issue most talked about in the earlier years of cybercrimes spreading in West-Africa, was the reluctance of victims of scams to report them to the authorities.

The fear of being stigmatized, shamed in the community was a powerful inhibitor to reporting cybercrimes. This situation reduces drastically the number of cybercrimes cases to be investigated and if needed, prosecuted in court. The fact that most cybercrimes cases in Cote d'Ivoire are committed by young Ivorian nationals does not make it easier for the Ivorian authorities to prosecute those responsible for these crimes for many reasons, among them the cultural, economic, and social inhibitors that we talked about in the beginning of this paper.

Now, what about a foreign authority wanting to prosecute a cybercriminal located in Cote d'Ivoire?

As Roger Grimes[309] put it, it is hard enough to successfully prosecute a cybercriminal if they originate in the same authority as the victim, but close to impossible when both reside in

[309] Grimes, R. A. (2016, December 6). *Why it is so hard to prosecute cyber criminals*. CSO Online. Retrieved March 1, 2022, from https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html "This is the No. 1 barrier to prosecuting cybercrime. Most of the time, the person committing the crime is located outside of the country (or at least outside the legal authority of the court and prosecutors seeking the conviction). It is hard enough to successfully prosecute a cybercriminal if they originate in the same authority as the victim, but close to impossible when both reside in different locations. Many times, we successfully collect good legal evidence and even verify the identity and location of the cybercriminal, but we have no legal ability to arrest the person. We have established cross-boundary, reciprocal legal rules with many cyber allies, but many more countries do not and will not participate. China and Russia will never honor our warrants of arrest any more than we would honor theirs. Our legal system, refined over centuries, was forged in the physical world for physical crimes. Internet crime is not even three decades old. Localities, cities, and states have had a hard time figuring out what is or isn't illegal in the computer world for a particular location, especially if that crime involves computers or people outside of their jurisdiction. For example, if porn is illegal in a particular locality but is accessed on a computer that is located outside that locality, is it illegal? Is it prosecutable? Some local court systems say yes, but many more say no. For that reason, most smaller entities leave it up to the federal legal system to define and prosecute computer crime. In the United States, most federal crimes are defined in what is known as Title 18. Most Title 18 crimes could be construed to cover their electronic counterparts but do so imperfectly. Congress created a special Title 18 section called 1030 in 1986, which has been updated and

different locations. For a foreign authority to be able to get its first-hand an Ivorian cybercriminal, there has to exist an extradition treaty between the country where the authority sits and the Republic of Cote d'Ivoire.

Even if that is the case, practical reasons may create roadblocks in seizing and extraditing the criminal in question. For example, when the crime has been committed through the use of a cybercafe, it is extremely difficult if not impossible to pinpoint the individual behind the offense.

To remedy this issue, Cote d'Ivoire through its numerous cyber laws, has made mandatory for Internet Service Providers, to identify those using their services; even here the potential for fraud is huge as most young people do not have real addresses where you can find them on any given day.

amended many times since its creation and is known as the Computer Fraud and Abuse Act. It has taken decades for law enforcement agencies, legal systems, and juries to get up to speed on cybercrime. Law enforcement agencies have had to train their officers to recognize the various forms of cybercrime, how to collect and preserve related evidence, and how to hire and train specialized forensic investigators. Prosecutors, judges, and juries have to be educated as well. It is just now, after 20 years of cybercrime, that we are beginning to understand how to successfully prosecute internet-related crime".

The Director of the Directorate (DITT) in charge of the fight against cybercrimes, Colonel Ouattara Moussa, noted that the action of the DITT is undermined by many difficulties:

> *These obstacles to the activity of the Directorate are at the level of international cooperation with regard to the sharing of information and cooperation with private companies, specifically with the large telecommunications groups, which must be reinforced for a better assembly of evidence. The other pocket of resistance is the ability of the DITT to educate the greatest number of people on the fight against cybercrime, he continued*[310].

The good news according to the Director is that the Directorate is now able to resolve at least 50% of all cybercrime's cases reported to the authorities. While these numbers are encouraging, one must not forget the hidden number of cybercrime victims who do not report it to the Police.

[310] Ehouman, A. (2021, December 22). *Côte d'Ivoire records an estimated 50% resolution rate for cybercrime offenses (Ministry)*. Ivorian Press Agency-AIP. Retrieved March 1, 2022, from https://www.aip.ci/aip-la-cote-divoire-enregistre-un-taux-de-resolution-dinfractions-en-lien-avec-la-cybercriminalite-estime-a-50-ministere/ See article: "Abidjan, Dec 22, 2021 (AIP)- The resolution rate for cases of offenses related to cybercrime in Côte d'Ivoire is estimated at 50%, a feat recognized in the sub-region, said the Director of the computer and technological traces (DITT) at the Ministry of the Interior and Security, Colonel Ouattara Guelpetchin Moussa.
Colonel Ouattara responded, Tuesday, December 21, 2021, to the invitation of the weekly press briefing of the Center for Government Information and Communication (CICG) called "All about" and relating today to the fight against cybercrime. The head of the cybercrime platform in Côte d'Ivoire said that the cybercrime environment has improved little bit. "Today, the average rate of financial damage has dropped dramatically. We are currently in a form of explosion of crime which concerns petty crimes. At the end of 2011, the DTT was resolving approximately 150 cases. In 2021, it is at 5,000 resolved cases," he said.
Also, there are five most recurrent offenses in the country. In 2021, the most significant offenses in terms of number were, in order, "attacks on human dignity, then fraud on electronic transactions, followed by fraudulent use of identification elements, then attacks on the image and in the spotlight, and finally the scams that most often concern, online shopping, fake scholarships, employment, buying a house online," listed the expert. However, fraudulent access to information systems is the damage that causes the most damage in terms of loss of money, apart from moral damage. Admittedly, this offense represents 1% of the cases of infringement presented in 2021, but generated two billion CFA francs in damage caused, underlined the director of IT and Technological Traces.
Indicating that efforts are being made to step up the fight against cybercrime in the country, Colonel Ouattara Moussa, noted that the action of the DITT is undermined by many difficulties.
These obstacles to the activity of the Directorate are at the level of international cooperation with regard to the sharing of information and cooperation with private companies, specifically with the large telecommunications groups, which must be reinforced for a better assembly of proofs. The other pocket of resistance is the ability of the DITT to educate the greatest number of people on the fight against cybercrime, he continued. However, the DITT plans, for greater efficiency, to deploy its services within the country, improve the cooperation framework and strengthen qualified human resources. Because, the interpellation, the tracking, the referral to the prosecution cannot be done without the competent human resources.
Cybercrime is all criminal offenses committed through computers or the Internet. The head of the platform for the fight against cybercrime, Colonel Ouattara Moussa urges victims to imperatively file a physical complaint with the police so that any action can be taken by the DITT. He recommends that companies who are victims of abuse report the facts and that the public be more vigilant." (AIP).

To show how monumental the task of investigating and prosecuting cybercriminals in Cote d'Ivoire is, let us take a look at the number of arrests in the year 2018:

> *In 2018, 89 "grazers" (scammers on the internet) were arrested, after 2,860 complaints, of which 73 were brought before the courts for fraud on the net", announced the Telecommunications Regulatory Authority of Côte d' Ivoire (ARTCI), using figures from the National Police's Cybercrime Platform (PLCC). Source: Jeune Afrique*[311].

Of the close to 3000 complaints, only 73 cybercriminals were brought before the courts for prosecution. When you consider the number of hidden victims, it is a clear indication that investigating and prosecuting cybercrimes in Cote d'Ivoire is extremely difficult.

Some of the reasons we analyse elsewhere are the obvious lack of sufficient and skilled human resources at all levels of the justice system in Cote d'Ivoire.

Faced with the bad "e-reputation" of Cote d'Ivoire in the field of cybersecurity, some Ivorian bloggers[312] have decided to "go to war" against cybercriminals by denouncing them whenever

---

[311] Afp, J. A. A. (2019, April 2). *Côte d'Ivoire: nearly 100 cybercriminals were arrested in 2018*. JeuneAfrique.com. Retrieved March 1, 2022, from https://www.jeuneafrique.com/757600/societe/cote-divoire-pres-de-100-cybercriminels-ont-ete-interpelles-en-2018/ "Some 92% of fraudsters are men, aged 24 on average and having experienced difficult schooling or dropped out around the 3rd grade, according to ARTCI. 339 accounts were deleted or recovered in 2018, according to police. The amount of damage linked to this cyberfraud is substantial: it amounts to 5.5 billion CFA francs (about eight million euros), of which 98% of the victims reside in Côte d'Ivoire. In 2013, cyber-fraud cost Côte d'Ivoire 26 billion CFA francs (39.6 million euros), according to the latest official figures".

[312] Kouade, L. (2017, August 4). *Côte d'Ivoire: fight against cybercrime, the participatory role of Internet users*. Ivoire Intellect. Retrieved March 1, 2022, from https://ivoireintellect.mondoblog.org/cote-divoire-lutte-contre-cybercriminalite-role-participatif-internautes/ See article below:

Côte d'Ivoire: fight against cybercrime, the participatory role of Internet users

"Cybercrime, in its infancy, is in no way the product of Ivorian criminal minds. The precursors of these frauds organized via the Internet in Côte d'Ivoire are Nigerian nationals and sometimes Cameroonians (Source: PLCC).

However, young Ivorians commonly known as "grazers", mostly aged between 13 and 30, have appropriated it to an excessive degree, attributing to the capital Abidjan the coat of arms of the African city with the worst "e -reputation" in 2013, stealing the limelight from the Nigerian capital. The techniques to their credit are increasingly sophisticated. Phishing, inheritance frauds, sentiment scams, lottery scams, equipment ordering and promise of payment by credit card or bank transfer, misappropriation of mail intended for banks, used car scams, etc. The list of these Cyber-delinquents is exhaustive. In 2012, the damage of their actions amounted to forty million dollars. In 2013, Côte d'Ivoire was relegated to the rank of the countries most at risk in terms of e-commerce. It is therefore the entire Ivorian digital economy that is accused of discrediting frauds, insecurity, and fraud.

The Government Response to Cybercrimes

Faced with the resurgence of Cyber-crimes and the damage caused by them, the governing authorities have taken drastic measures. To this end, a platform – Platform for the Fight Against Cybercrime (PLCC) – was set up in 2012

possible to the authorities. Though this private initiative is to be encouraged, it can nevertheless be problematic in bringing about false denunciations for other reasons not related to cybercrime activity.

The primary responsible tasked with investigating and prosecuting cybercriminals is the Ivorian justice system, notwithstanding its lack of human and financial resources.

---

with an “anti-grazing” brigade. Its mission is to intercept suspicious activities on the Internet and to transmit data to the scientific police in order to track down and arrest cybercriminals. In 2015, the number of cyber-delinquents arrested rose to 205, including 189 men (92%) and eight young girls (8%). In addition to the previous measures, an operation to identify mobile phone subscribers has identified more than two (02) million subscribers. Alongside this, the census of Cyber-cafés throughout the territory and the adoption of a bill relating to the fight against cybercrime and data protection have been part of the Cyber defense system. Ivorian. In view of the measures taken and the climate unfavourable to cybercrime, cybercriminals or "grazers" will initially opt for refuge in inland towns where the control of the forensic services is almost non-existent, and then exile in Morocco - for some - when the tranquillity in the said localities proved to be uncertain.

The participatory role of Internet users in the fight to eradicate the phenomenon

To believe the effectiveness in the application of the public measures mentioned above, the police services and the Ivorian justice are hard at work to limit as much as possible the acts of vandalism perpetrated in cyberspace, in particular against foreign targets. But Ivorian cyber-delinquents, like e-employment workers, remain continually active internet users on the web, who over time have acquired a good command of the use of virtual technologies. Thus, the participatory fight of the population of Internet users in Côte d'Ivoire would be summed up overall in a prevention strategy favouring on the one hand information relating to the techniques of cybercriminal approaches and then to an active denunciation of acts of depredation on the internet.

In practice, it will be a question

For the informational component to reveal new cybercriminal strategies other periodically and actively than those already known. As a result, more than one population of Internet users will be notified of the next manoeuvres of our Cyber-crooks and as many wallets and goods will be sheltered and secured. With regard to whistleblowing, it should be noted as a prelude that the proximity of Internet users to criminals is a major asset, all the more so as we recommend, as part of this participatory struggle, the involvement of these populations who are intended to hold recurring the candle to Cyber-delinquents. Concretely, to denounce acts of crime orchestrated on the Internet, it will be necessary for people tagged with good citizenship to proceed as soon as they identify cybercriminal content (inheritance scams, love scams, lottery scams, promise of payment by credit card or bank transfer, and that: Alert the competent authorities of the offense in progress and transmit, if possible, the identity of the presumed criminals in order to facilitate possible arrests

Report messages and publications from suspicious sources online to its network on social networks and to its contacts by e-mail and telephone messages in order to inform as many people as possible of the current threat

Block the continual receipt of unwanted e-mails (spam) in e-mail boxes and in certain circumstances report them

As far as possible, make your network, contacts, and entourage aware of the cybercriminal risks of which we are aware. Whatever happens, let us remain active in the fight and contribute as best we can to cleaning up cyberspace and the Ivorian economic climate.

The league of Ivorian bloggers has already sounded the start of the fight between bloggers and "grazers" in Côte d'Ivoire. We say in turn that for a risk-free cyberspace, an effective digital revolution and an almost zero cybercriminal risk rate, the war has only just begun.”

To resolve with a high degree of success the issue of skilled human resources and financing, the state of Cote d'Ivoire must prioritize the training of qualified personnel and devote any financial means necessary to the fight against cybercrimes.

One avenue to resolve the lack of skilled personnel would be for the Ivorian government to entice any skilled Ivorians living abroad to return and help in the fight against the scourge of cybercriminality through financial incentives.

The Ivorian government could sign a contract with skilled Ivorians from the diaspora to pay them the same or bigger wages they make in the West. For the issue of financing, the real problem is a will of the Ivorian government, rather than a lack of financing.

This is a country that like to brag about its status as the number one cocoa producer in the world. Cote d'Ivoire can also explore international financing from both the United Nations agencies and rich countries that are at the receiving end of the actions of African cybercriminals.

Investigating and prosecuting cybercriminals is incomplete if the sentencing of those criminals is botched through some form of corruption within the justice system. Unfortunately, there have been some cases in which the sentencing was not serious enough to deter future cybercriminals, quite the opposite effect.

The famous case in Cote d'Ivoire has been the arrest, prosecution and sentencing of the infamous "Commissaire 5500". We will analyse it in detail in the sentencing of cybercriminals in Cote d'Ivoire.

4-3: The sentencing of cybercriminals

The sentencing of authors of cybercrimes in Africa in general and in Cote d'Ivoire in particular is fraught with many issues, not least, the fact that very few victims of cybercrimes report them to the authorities for investigations. Cybercriminals operating from Cote d'Ivoire have their own networks inside the justice system starting with law enforcement to Attorneys and Judges and everyone in between.

The complexity of cybercrimes investigations adds another layer of weakness to the whole judicial sentencing process. Thanks to both the anonymity and the transnational nature of the internet which can take a substantial amount of time to clear, thus preventing the successful prosecution of all involved in the crime, many cybercriminals get away from prosecution let alone being sentenced to jail time.

With regard to the sentencing process in Cote d'Ivoire, one must note that most sentences handed to cybercriminals are exceptionally light. The infamous "Commissaire 5500" after being arrested in 2016, was sentenced to just two years in prison where he became a soccer player whose exploits were talked about in news articles in Cote d'Ivoire.

Nevertheless, things have been improving in recent years and the Ivorian government has even decided to double the sentence for certain cyber offenses from the 2013 Law against cybercrimes.

In July of 2021, a cyber-activist was sentenced to six months in prison, including one firm, for insulting the former Ivorian first lady, Simone Gbagbo[313]. Last May, another cyber-activist was

[313] Pinto, P. (2021, September 8). *The Ivorian government toughens penalties for cybercrime*. RFI. Retrieved March 20, 2022, from https://www.rfi.fr/fr/afrique/20210908-le-gouvernement-ivoirien-durcit-les-peines-en-mati%C3%A8re-de-cybercriminalit%C3%A9 The article: "This type of case is more and more frequent in the Abidjan court, and the sentences should become even heavier from now on. The maximum penalties in some cases will be doubled compared to those provided for in the 2013 cybercrime law, government spokesperson Amadou

sentenced for having launched an appeal on social networks to attack Nigerien nationals living in Côte d'Ivoire. Sentence pronounced: five years in prison!

This is a recognition of the fact that the sentences contained in the different cyber laws are not dissuasive enough to stop cybercrimes in the country. The sentencing issue is compounded by the pervasive corruption that permeates the judiciary.

Here in the United States, federal sentencing guidelines[314] recommend a prison sentence of up to 20 years for those convicted of cybercrime offenses. If the offense results in the death of another person, then a defendant convicted of the crime could be sentenced to life in prison. This is irrespective of the type of cybercrime.

The penalties for a cybercrime conviction are not as harsh for a first-time offender or someone who has never been convicted of a crime involving computers. Federal sentencing guidelines recommend a prison sentence of up to 10 years for those first-time offenders.

We think the Ivorian authorities should explore the revision of the sentencing guidelines contained in the different cyber laws adopted at the beginning of the previous decade./.

Coulibaly explained on Wednesday. Behavior on social networks is particularly targeted, such as contempt and invective punished until then by five years in prison, as well as publications likely to disturb public order. The penalty should therefore also be doubled for threats of harm to persons or destruction of property, now punishable by a maximum of ten years. Comments of a xenophobic and racist nature are also targeted."

[314] Sample, B. (2020, June 5). *Federal Cyber Crime.* Brandon Sample Attorney. Retrieved March 21, 2022, from https://brandonsample.com/federal-cyber-crimes/

4-4: Obstacles to enforcing laws against cybercriminals

Although law enforcement across the world have had decades of experience enforcing the laws on the books against all kinds of criminals, the fact of the matter remains that, it is extremely difficult to enforce laws against cybercriminals for a variety of reasons.

The transnational nature of cyberspace and specifically the internet, the inadequate readiness of law enforcement in poor countries like Cote d'Ivoire and of course, the old social, political, cultural, and economic determinants playing an outsize role in mostly African countries.

In developed countries like the United States, the main obstacle to enforcing efficiently cyber laws, remains the transnational nature of the internet compounded by the lack of cooperation of some countries when it comes to extraditing their nationals to countries like the United States for prosecution.

This situation has led the FBI to be creative in order to catch cybercriminals from uncooperative nations like Russia and China. The most famous case remains the "Invita"[315] case.

In other cases, international cooperation has worked very well like the "Rome Labs"[316] case in which the FBI and Scotland Yard (UK) cooperated to bring down a cybercriminal living in England while hacking the Rome Air Development Center ("Rome Labs") at Griffiss Air Force Base in New York.

[315] Susan W. Brenner & Joseph J. Schwerha IV, Transnational Evidence Gathering and Local Prosecution of International Cybercrime, 20 J. Marshall J. Computer & Info. L. 347 (2002)
[316] Ibid.

In the specific case of Cote d'Ivoire, the main obstacles while including the transnational nature of the internet, remain primarily, the lack of skilled personnel at every level of the justice system, compounded by the generalised corruption in the country. The causes remain the cultural, social, economic, and political aspects of Ivorian society which can easily be found in most African countries and lead to a ferocious corruption system "allergic" to the rules of law inscribed in the national constitution.

4-4-1: The transnational nature of the internet

The Internet and other aspects of the information infrastructure are inherently transnational[317]. This transnational nature of the information infrastructure is in a way the under-belly of cyberspace.

As Sofaer and Goodman[318] pointed out, the information infrastructure is increasingly under attack by cyber criminals. The number, cost, and sophistication of attacks are increasing at alarming rates. They threaten the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information.

To grasp the magnitude and complexity of the global information society, some experts look up to the way international trade was regulated during the Middle Ages (Lex Mercatoria) and some like Joel Reidenburg[319] have coined the term "Lex Informatica." Reidenburg[320] argued that during the

[317] Granville, J. (2003). The Transnational Dimension of Cyber Crime and Terrorism. By Abraham D. Sofaer and Seymour E. Goodman (Stanford, CA: Hoover Institution Press, 2001, 292 pp. $24.95 pb). *British Journal of Criminology*, *43*(2), 452–453. https://doi.org/10.1093/bjc/43.2.452.
[318] Ibid.
[319] Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Tex. L. Rev. 553 (1997-1998) Available at: http://ir.lawnet.fordham.edu/faculty_scholarship/42
[320] Ibid.

Middle Ages, itinerant merchants traveling across Europe to trade at fairs, markets, and seaports needed common ground rules to create trust and confidence for robust international trade.

The need, he posited, stemmed from the differences among local, feudal, royal, and ecclesiastical law which provided a significant degree of uncertainty and difficulty for merchants. Thus, custom and practices evolved into a distinct body of law known as the "Lex Mercatoria,"[321] which was independent of local sovereign rules and assured commercial participants of basic fairness in their relationships.

The good news is that over the last two decades, governments and regional organizations have stepped up to the plate to produce some form of Lex Informatica, otherwise rules governing the flow of information on a worldwide scale.

The most promising case is the Budapest Convention adopted in 2001 by member states of the Council of Europe. The sad news is, a great disparity[322] exists, in the legal and technological capacity of states to meet the challenges of preventing, investigating, and prosecuting cybercrime.

---

[321]Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology. (Supra note 319) P.204.
. "In the era of network and communications technologies, participants traveling on information infrastructures confront an unstable and uncertain environment of multiple governing laws, changing national rules, and conflicting regulations. For the information infrastructure, default ground rules are just as essential for participants in the Information Society as Lex Mercatoria was to merchants hundreds of years ago. Confusion and conflict over the rules for information flows run counter to an open, robust Information Society. Principles governing the treatment of digital information must offer stability and predictability so that participants have enough confidence for their communities to thrive, just as settled trading rules gave confidence and vitality to merchant communities."

[322] Granville, J. (2003). The Transnational Dimension of Cyber Crime and Terrorism. (Supra note 317) P.204. "An effective program against transnational cybercrime will require legal cooperation among states that involves the enforcement of agreed standards of conduct. A broad consensus exists among states concerning many forms of conduct that should be treated as cybercrime within national borders. This consensus must be translated into a legal regime in which all states that are connected to the Internet prohibit forms of conduct widely regarded as destructive or improper. In addition, much remains to be done to encourage and, as soon as practicable, to require states to adopt common positions to facilitate cooperation in investigation, the preservation of evidence and extradition. States must establish and designate cross-patent agencies to deal with transnational issues, and to cooperate with counterparts throughout the world. To develop and secure the universal adoption of technological and policy standards to defend against, prosecute, and deter cybercrime and terrorism, states should create an international agency, like the International Civil Aviation Organization (ICAO) but designed to reflect the particular needs and nature of the cyber world. International cooperation must include an effective program to upgrade the capacities of states that lack the technological resources

Most African countries lack the technological capacity to heed the challenges of cybercrimes. It is true that most poor nations have to find ways and means to satisfy the basic needs of their people like, food, healthcare, drinking water and other necessities.

Most people in developing countries, do not use the internet for all their transactions as we see in the West. So, they expect their government to create the conditions to have healthcare, food, and good roads to move goods around. The internet is not a priority for most people. That being said, recent data of cybercrime activities in Cote d'Ivoire show that 98% of cybercrime victims are in Cote d'Ivoire and just 2% of victims are outside the borders of the country.

The real issue is when an Ivorian national based in Cote d'Ivoire commits acts of cybercrime against someone abroad. As we have seen throughout this research, many of the victims of Ivorian cybercriminals reside outside of Cote d'Ivoire. This is the case for countries like France, Switzerland, Belgium, and part of Canada (Quebec) which are all French-speaking nations. Some victims were residents of the United States and Great Britain.

In those cases, the transnational nature of the medium of contact (Internet) and the lack of extradition treaties may have hampered the investigations of some of these crimes. As Sofaer and Goodman[323] remind us, all messages on the Internet are broken down into "packets" that separate and travel through available routers and servers located throughout the world.

to cooperate in a comprehensive international regime. These measures, though far-reaching by comparison with current policies, can be fashioned to maximize private-sector participation and control, to ensure that privacy and other human rights are not adversely affected and so as not to impinge on the national security activities and interests of States Parties."

[323] Granville, J. (2003). The Transnational Dimension of Cyber Crime and Terrorism.(Supra note 317) P.204.

Thus, they argued, cybercrime goes beyond this technical, transnational dimension and involves senders who deliberately fashion their attacks and other crimes to exploit the potential weaknesses present in the infrastructure's transnational nature:

> *These weaknesses include: (1) a worldwide target pool of computers and users to victimize, or to exploit in denial-of-service or other attacks, which enables attackers to do more damage with no more effort than would be necessary in attacking computers or users in a single state; and (2) the widespread disparities among states, in the legal, regulatory, or policy environment concerning cybercrime, and the lack of a sufficiently high degree of international cooperation in prosecuting and deterring such crime. The most damaging cyber-attacks thus far experienced have been transnational, originating in many different countries and aimed at computers everywhere*[324].

Now it is important to note that these cases happened at the beginning of the 21st century and since then many more high-profile cases like the "Target" case (2013) or the "Sony" case (2014) involving hackers from North Korea have been more widely publicized. Nevertheless, this is a good reminder that the transnational nature of the internet has been a major issue from the get-go (since the 90s).

[324] Granville, J. (2003). The Transnational Dimension of Cyber Crime and Terrorism.(Supra note 317) P.204.
Here are some prominent examples: The so-called "Phonemasters," a "loosely-knit," "12-member" international "hacking ring" headed by Jonathan Bosanac of Rancho Santa Fe, California (near San Diego), who, using the on-line name "The Gatsby," developed a method for gaining access to telephone networks (such as MCI, WorldCom, Sprint, and AT&T), credit-reporting databases (such as Equifax), and even the FBI's own National Crime Information Center, which they utilized in a number of countries. "The breadth of their monkeywrenching was staggering; at various times they could eavesdrop on phone calls, compromise secure databases, and redirect communications at will. They had access to portions of the national power grid, air-traffic–control systems and had hacked their way into a digital cache of unpublished telephone numbers at the White House. . .. [T]hey often worked in stealth and avoided bragging about their exploits. . .. Their customers included . . . the Sicilian Mafia. According to FBI estimates, the gang accounted for about $1.85 million in business losses." David L. Smith, a New Jersey programmer, pleaded guilty in December 1999 of creating the "Melissa" computer virus and using an X-rated website to spread it through cyber space via e-mail in March 1999, where it "rampaged personal, government, and corporate computers around the world," "caused worldwide devastation," and was estimated to have done $80 million (or more) in damages. From December 1999 through April 2000, five hackers in Moscow stole more than 5,400 credit card numbers belonging to Russians and foreigners from Internet retailers, pocketing more than $630,000 until arrested. The incident pointed up the threat that "Eastern European fraudsters continue to pose . . . for all card issuers, even those with no direct business in the region.

There is not an extradition convention between Cote d'Ivoire and the United States which means that if cybercriminals operating from Cote d'Ivoire are sought by the United States to be prosecuted in an American authority, Cote d'Ivoire is legally not bound to hand its citizens over to the FBI.

That being said, the FBI has other ways to get their first-hand the criminals sought. The most famous case at the beginning of the 21st century was the "Invita"[325] case in which, the FBI was called in to investigate a series of intrusions "into the computer systems of businesses in the United States" that emanated from Russia. The Justice Department described the attacks as follow:

> *The attacks targeted: Internet Service Providers, e-commerce sites, and online banks in the United States. The hackers used their unauthorized access to the victims' computers to steal credit card ... and other..., financial information, and . . . tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims' computers. The hackers also defrauded PayPal through a scheme in which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States*[326].

The FBI identified the Russians[327]-Vasiliy Gorshkov and Alexey Ivanov- responsible for the attacks and used a ruse to entice them to the United States (See description below). One can assume

[325] Susan W. Brenner & Joseph J. Schwerha IV, Transnational Evidence Gathering and Local Prosecution of International Cybercrime. (Supra note 315) P.203.
[326] Ibid.
[327] Ibid. The FBI created a bogus computer security company called "Invita" located in Seattle, Washington, and brought the hackers to Seattle to "interview" with the company. As part of the "interview," the Russians were asked to hack into a network set up by the FBI, the purpose being to demonstrate their computer skills. Using laptops provided by the FBI, they successfully broke into the network and, in so doing, accessed their computer system- "tech.net.ru"-in Russia. The FBI had previously installed a keystroke logger program on the each of the laptops and the program recorded the usernames and passwords Gorshkov and Ivanov used to access their Russian computers. As soon as the "interview" was over, agents arrested Gorshkov and Ivanov; they then used the information retrieved by the keystroke logger to access the Russian computers and download files they contained. They did all this without obtaining a warrant. After being indicted for conspiracy, computer crime and fraud, Gorshkov moved to suppress the evidence obtained from the Russian computers, arguing that it was the product of a search and seizure that (a) violated the Fourth Amendment and/or (b) violated Russian law." The district court denied the motion. As to the FBI's using the keystroke logger program to obtain Gorshkov's password, the court found that Gorshkov did not have a cognizable Fourth Amendment expectation of privacy when he used a "foreign" computer to access his files in Russia. As to the FBI's downloading files from the Russian computer without a warrant, the court held: (a) that the Fourth Amendment did not apply because the computer was in Russia and the Fourth Amendment does not apply to searches and seizures conducted outside the territorial boundaries of the United States; and (b) that if the Fourth Amendment did apply, the agents' actions were "reasonable" because they were justified by the exigent circumstances exception to the warrant requirement. Finally, the court held that Russian search and seizure law did not apply to the agents' conduct.

that the same method or other similar methods can be used by the FBI with respect to countries that do not have an extradition convention with the United States. In 2013, a case of cooperation between the FBI and the Platform for the Fight Against Cybercrimes or PLCC led to the arrest of two Ivorian cybercriminals in Cote d'Ivoire.

In this case[328], the FBI alerted the PLCC regarding cybercriminals from Cote d'Ivoire who had scammed victims around the world in the amount of $2 million dollars. To congratulate the PLCC for a job well done, the FBI sent two (2) of its agents to Abidjan to thank their Ivorian counterparts.

This is an example of informal cooperation between the PLCC and the FBI that is certainly replicated elsewhere in Africa by the FBI. On the other hand, such cooperation between West-African law enforcement with regard to cybercrimes is at best "nascent" and need to be reinforced by the different stakeholders in the West-African region, true hub of cybercrime activities around the world.

One of the Achilles heels in the global fight against cybercrime, especially in poor countries in Africa, is the inadequation between the urgent need to enforce cybercrime laws and the lack of readiness of most African law enforcement agencies, including in Cote d'Ivoire where the necessary agencies to fight cybercrime have been put in place a decade ago.

Creating an agency to fight a scourge like cybercrime and dotting that agency with the right tools to do the work are unfortunately two different things in the African context.

[328] The FBI in Abidjan to note the arrest of the gang of cyber crooks who have committed frauds of 900 million FCFA. (2013, June 25). Edith Brou Island. Retrieved March 10, 2022, from https://lactuwebdedith.wordpress.com/2013/06/25/le-fbi-a-abidjan-pour-constater-larrestation-du-gang-de-cyberescrocs-auteur-descroqueries-de-pres-de-900-millions-de-fcfa/

It is also practical and fundamental to go beyond the usual lack of funds to dissect the different determinants that have always prevented the rendering of justice in poor countries like Cote d'Ivoire. Those determinants are social, cultural, economic, and also political./.

4-4-2: Inadequation between Cybercrimes Enforcement and Readiness

> *There is a rise in the frequency and sophistication and the reason for that development, is attributable to the fact that, as efforts are being made to stem the tide of cybercrimes, so are cybercriminals devising methods and means of thwarting global measures targeted at addressing the problem*[329].

When it comes to enforcing cybercrime laws in most African countries, including in Cote d'Ivoire, two sets of problems related to the readiness of law enforcement appear:

1- The lack of skilled personnel and resources (tools) needed to go after the criminals and,
2- The sophistication of the methods used by cybercriminals who operate in every corner of the world.

In the first case dealing with the lack of skilled workforce to successfully undertake the fight against cybercriminality, this is a poor country issue as most of their skilled nationals are working abroad where they make more money than they could ever dream to earn back home.

In the case of Cote d'Ivoire, as in the case of most African countries for that matter, the lack of skilled personnel is present at every level of the justice system. The country does not train a critical mass of specialists in information systems locally.

Those who are lucky to go abroad to attend a foreign university, in most cases remain there to work after graduation due to the poor prospects waiting for them back home.

[329] Ajayi, E. (2016, July 25). *Challenges to enforcement of cyber-crimes laws and policy*. Journal of Internet and Information Systems. Retrieved March 10, 2022, from https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210

Even those students sent by the government to be trained abroad, in some cases, choose to remain in the country where they graduated for better prospects of wages, freedom and stability. The same issue is also present in about any other field of education.

On the second point regarding the sophistication of the methods used by cybercriminals, one such method or tool is the anonymization of online presence by cyber-crooks looking to deceive their potential victims.

As Marie-Helen Maras pointed out in her book Cybercriminalogy[330], anonymity enables individuals to engage in activities without revealing themselves and/or their actions to others. One such technique is the use of proxy servers.

A proxy server is an intermediary server that is used to connect a client (i.e., a computer) with a server that the client is requesting resources from.

Anonymization techniques[331] are used for legal and illegal reasons. There are legitimate reasons for wanting to remain anonymous online and maintaining the protection of anonymity online. For example, anonymity facilitates the free flow of information and communications without fear of

[330]Maras, M. (2016). *Cybercriminology* (1st ed.). Oxford University Press.

[331] K. (2019, March). *Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations*. UNODC.ORG. Retrieved March 12, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html "

Cybercriminals can also use anonymity networks to encrypt (i.e., block access) traffic and hide Internet Protocol address (or *IP address*), "a unique identifier assigned to a computer [or other Internet-connected digital device] by the Internet service provider when it connects to the Internet" (Maras, 2014, p. 385), in an effort to conceal their Internet activities and locations. Well-known examples of anonymity networks are Tor , Freenet , and the Invisible Internet Project (known as I2P).

The Onion Router (or Tor), which enables anonymous access, communication, and information sharing online, was originally developed by the United States Naval Research Laboratory to protect intelligence (Maras, 2014a; Maras, 2016; Finklea, 2017). Since the release of Tor to the public, individuals have used it to protect themselves against private and government surveillance of their online activities. Nonetheless, Tor and other anonymizing networks have also been utilized by cybercriminals to commit and/or share information and/or tools to commit cyber-dependent and cyber-enabled crimes (Europol, 2018).

These anonymity networks not only "mask users' identities, but also host their websites via…[their] 'hidden services' capabilities, which mean[s] that these sites can only be accessed by people on" these anonymizing networks (Dredge, 2013). These anonymity networks are thus used to access darknet (or Dark Web) sites.

repercussions for expressing undesirable or unpopular thoughts as long as there are no overriding legal reasons to restrict this expression, for legal and legitimate restrictions of the freedom of expression.

Another obstacle is called "attribution" that deals with the ownership of the theft or hacking. The UNODC has a simple explanation on its website that we are reproducing here for education purposes:

> *Attribution is another obstacle encountered during cybercrime investigations. Attribution is the determination of who and/or what is responsible for the cybercrime. This process seeks to attribute the cybercrime to a particular digital device, user of the device, and/or others responsible for the cybercrime (e.g., if the cybercrime is state-sponsored or directed) (Lin, 2016). The use of anonymity-enhancing tools can make the identification of the devices and/or persons responsible for the cybercrime difficult.*
>
> *Attribution is further complicated through the use of malware-infected zombie computers (or botnets; discussed in Cybercrime Module 2 on General Types of Cybercrime) or digital devices controlled by remote access tools (i.e., malware that is used to create a backdoor on an infected device to enable the distributor of the malware to gain access to and control of systems). These devices can be used, unbeknownst to the user whose device is infected, to commit cybercrimes.* Source: unodc.org[332]

[332] K. (2019, March). *Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations*.(Supra note 331) P.211.

"Back-tracing (or *traceback*) is the process of tracing illicit acts back to the source (i.e., perpetrator and/or digital device) of the cybercrime. Traceback occurs after a cybercrime has occurred or when it is detected (Pihelgas, 2013). A preliminary investigation is conducted to reveal information about the cybercrime through an examination of log files (i.e., *event logs*, which are files systems produce of activity), which can reveal information about the cybercrime (i.e., *how* it occurred). For instance, event logs "automatically record… events that occur within a computer to provide an audit trail that can be used to monitor, understand, and diagnose activities and problems within the system" (Maras, 2014, p. 382). Examples of these logs are *application logs*, which record "events that are logged by programs and applications," and *security logs* that "record all login attempts (both valid and invalid) and the creation, opening or deletion of files, programmes or other objects by a computer user" (Maras, 2014, p. 207). These event logs may reveal the IP address used in the cybercrime.

Traceback can be time-consuming. The time it takes to complete this process depends on the knowledge, skills, and abilities of the preparators and the measures they have taken to conceal their identities and activities. Depending on the tactics used by cybercriminals to perpetrate the illicit acts, tracing may not lead to a single identifiable source (Pihelgas, 2013; Lin, 2016). For example, this can be observed in cases where malware-infected zombie computers are utilized to commit cybercrime or when multiple perpetrators simultaneously conduct a distributed denial of service attack (i.e., DDoS attack) against a system or website (for more information about these cybercrimes, see Cybercrime Module 2 on General Types of Cybercrime)".

According to some Ivorian experts in cybersecurity, cybercriminals operating in Cote d'Ivoire are less sophisticated than their counterparts in places like Eastern Europe for example.

This is not always the case as increased cybercrimes originating from West-Africa, including in Cote d'Ivoire use sophisticated methods to lure and steal from unsuspecting internet users.

As Swiatkowska[333] reminds us, countering cybercrime often requires skills and resources that national law enforcement agencies do not have. She went on to argue that the architecture of the internet – in so far as it enables anonymity, and criminals can often operate behind multiple layers of fake identities – promotes clandestine actions, as it complicates even basic actions to identify the offender[334].

She also pointed out in the case of developing countries, the fact that technological innovation[335] offers countless, constantly evolving tools to commit cybercrime and that to keep up with technological changes, law enforcement and the judiciary must constantly perfect their methods and invest in knowledge, equipment, and skills – all of which require the time and resources public bodies often lack – particularly in developing countries.

Another issue when it comes to the readiness of law enforcement to combat more effectively cybercrimes is the reluctance of the private sector to collaborate with law enforcement for multiple

[333] Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.
[334] Ibid.
[335] Ibid. More on the technological constant innovation: "Keeping up with technological advancements causes operational issues and difficulties solving fundamental security problems. Very often the technologies that bring innovation and benefits for society also hamper the efforts of law enforcement agencies. Encryption is a good example – it brings enormous benefits for users, enhancing privacy and confidentiality of data and communication. It serves as an essential element of cybersecurity and a building block for secure solutions that enable the digital economy to thrive (Kelly 2018). At the same time, it creates significant obstacles and challenges for entities responsible for combating cybercrime, as often they are not able to track criminals and have access to important evidence or information. There is currently a vivid global debate on whether or not to introduce 'backdoors' into systems to enable more efficient work of law enforcement agencies. Backdoors are a double-edged sword: while helping police action, they can significantly weaken the security and cause hard-to-predict damages to the security ecosystem.

reasons, among them, the fact that companies want to keep quiet on cases of data breaches for PR purposes. Unfortunately, without the participation of private companies many cases deserving of a thorough investigation cannot be had.

As Swiatkowska[336] rightly pointed out, in the digital realm, private companies predominate: they own and operate infrastructure, provide products and services to end users, and maintain databases. They often have sole access to the potential evidence and information necessary for an investigation.

Recently, the Director of the Directorate for computing and technological traces (DITT), talked about the need of a sound cooperation between the DITT and the private sector in the investigations of cybercrime cases involving the use of the infrastructure of a private company. It is also vital that the state of Cote d'Ivoire invest heavily in the training of skilled personnel both at the law enforcement level and at the judiciary level, to enhance its capabilities to effectively fight and reduce the scourge of cybercrime in the country.

The reputation of Cote d'Ivoire will continue to suffer in the world unless drastic measures are implemented to eradicate cybercrimes. That being said, those measures should encompass the whole justice system as the old determinants that inhibit the rule of law in the nation are still there and more powerful nowadays than during the reign of the father of the nation, Felix H. Boigny.

We will examine the persistence of those old determinants in the fight against cybercrimes in Cote d'Ivoire starting with the social and cultural determinants, followed by the economic determinant and last but not least, the powerful political determinant.

[336] Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. (Supra note 333) P.213.

From there, we will summarize our research and make the necessary recommendations both to the Ivorian authorities and to West-African countries in general./.

4-4-3: Persistence of the Old Determinants in the Fight Against Cybercrimes

4-4-3-1: Social and Cultural Determinants

Society[337] means an interdependent group of people who live together in a particular region and are associated with one another, while culture refers to the set of beliefs, practices, learned behavior and moral values that are passed on, from one generation to another.

The Ivorian society is composed primarily of three big ethnic groups, with the Akan being the dominant group in the southern part of the country, the Mande in the northern part of the country and the Kru in the western portion of the country.

To create a nation out of all these different ethnic groups, the first president of Cote d'Ivoire, Felix H. Boigny encouraged a melting pot which led to people marrying across ethnic lines.

This policy has made Cote d'Ivoire, one of the most diverse societies in West-Africa to this day.

The consequence of this policy is that all the regions of the country ended up sharing the same social and cultural norms overtime.

If most of the social behavior, practices and beliefs are to be commended because they are universally shared, they unfortunately also contain negative aspects that taken together make the rule of law at best, challenging, and at worst, a concept in name only.

If it is commendable to encourage a sense of community between people of diverse backgrounds, one must also recognize that, in many instances, people tend to exploit it for their personal gains.

[337] S, S. (2017, August 12). *Difference Between Culture and Society (with Comparison Chart)*. Key Differences. Retrieved March 14, 2022, from https://keydifferences.com/difference-between-culture-and-society.html

Someone who is in trouble with the law will seek the help of an influent member of the community to avoid taking responsibility for their actions, which undoubtedly lead to a general corruption in the nation.

Unfortunately, every region of Cote d'Ivoire has the same approach to the rule of law in general, meaning that people obey the law when it is convenient, but tend to violate and circumvent it when it is getting in the way of their personal needs and wants.

The bigger issue related to the rule of law in developing countries, including in Cote d'Ivoire, derives from the way society control violence, according to Weingast.[338]

For him, missing from the traditional approaches to the rule of law both in developed countries and developing countries is how societies reduce or control the problem of violence.

For Weingast, the most common social order throughout history, the limited access order or natural state[339], solves the problem of violence through rent-creation, granting powerful individuals and groups valuable rights and privileges so that they have incentives to cooperate rather than to fight.

The resulting rents, limits competition, access to organizations and logically hinder long-term economic development.

[338]Weingast, B. (2009, February). *Why are developing countries so resistant to the rule of law?* cadmus.eui.eu. https://cadmus.eui.eu/bitstream/handle/1814/11173/MWP_LS_2009_02.pdf?sequence=1&isAllowed=y
[339] Ibid.

On the other hand, direct access orders use competition, open access to organizations, and institutions to control violence and are characterized by rent-erosion and long-term economic growth.

In developing countries like Cote d'Ivoire, the system of rent-creation[340]and or the granting of rights and privileges to powerful individuals and groups always lead to the rule of law being violated by these groups or individuals.

The fact of the matter is that the political parties that govern the country, always manage to grant rights and privileges to powerful individuals and groups (ethnic) solidifying the rent-creation system that replaces the notion of rule of law.

This in turn will have the resulting effect of turning laws and regulations into tools of corruption. People do not expect justice, fairness, and their basic rights to be respected in the court of justice. As Leanne McKay[341] posited, when people feel that their rights are being denied with no recourse to remedy, that they have no opportunity to participate in decisions that affect their lives, that their grievances are going unresolved, or that their basic needs are not being fulfilled by the state, then a sense of injustice grows, which in the worst case can manifest itself in violence, which in turn creates greater insecurity and instability within the country. The other way can also have adverse effects. For Leanne McKay[342], tipping the balance too far toward justice, with too little attention given to security needs, can also have negative outcomes. For example, a situation where everybody is demanding their rights and seeking to promote their own interests— whether

[340] Weingast, B. (2009, February). *Why are developing countries so resistant to the rule of law?(Supra note 338) P.217.*
[341] L. McKay. (2015). *Toward A Rule of Law Culture. Exploring Effective Responses to Justice and Security Challenges*. usip.org. https://www.usip.org/sites/default/files/Toward-a-Rule-of-Law-Culture_Practical-Guide_0.pdf
[342] Ibid.

economic, ethnic, or political—without concern for the rights of others, can create chaos, confusion, and instability.

In Cote d'Ivoire, there is a strong culture of seeing everything through the prism of one's ethnic group. It is so that, when the head of state is from one particular region or ethnic group, members of that region or that ethnic clan are de facto privileged over the other ethnic groups or regions. This sense of being from a region or from an ethnic group before being an Ivorian national, despite the powerful policy of an Ivorian "melting pot," is still strong to this day. One aspect of successive administrations in Cote d'Ivoire has been to name more members of the President's ethnic group in government and name members from the remaining ethnic groups but in the single digits so that, technically, the whole country is represented in the government.

This kind of governing the nation has been first initiated by President Houphouet Boigny, the founder of modern Cote d'Ivoire. Nevertheless, President Houphouet was very subtle and diplomat in rent-creation among the different ethnic groups of Cote d'Ivoire, to the point that very few Ivorians ever complained of ethnic preference under his leadership. Unfortunately, one cannot say the same with his successors. A tangible consequence of this rent-creation is that people tend to gravitate around the one government minister who is from their region and obviously ask for all kinds of help including financial and legal help to extricate one 'self from a legal exposure. Thus, most people rely on their leader in government to avoid the consequences of their actions because , those in power always manage to avoid the weight of the justice system, so why not the average person. One type of thinking going around within groups of cybercriminals, is to say that white people have colonized and exploited Africa as a whole, so these online scams are just a payback from the misdeeds of the past. Unfortunately, it is not just cybercriminals who think that way, a huge section of the population including some in law enforcement. In recent years, as

cybercriminals target people in Cote d'Ivoire, the population has turned against them. The culture of self-victimization, coupled with corruption, has made enforcing cyber laws as difficult as other laws and regulations. In that respect, the old social and cultural determinants that have always permeated the social fabric in Cote d'Ivoire prevents a successful fight against cybercrimes in that country and in the rest of West-Africa for that matter. Most African countries and especially West-African countries deal on a daily basis with the same issues related to the system of rent-creation described by Weingast[343]. One other issue in developing countries and in Cote d'Ivoire, in particular, is the absence of a "perpetual state" as interest groups can shorten the life expectancy of the governing party through various non-democratic means like a military coup. When that happens, the new dominant group knowing well how it came to power, meaning they can be ousted as fast as they came, will rush to rent creation, hoping to avoid violence. The same cycle of corruption, injustice repeat, leading to the growth of the culture of substituting corruption to the rule of law. In a sense, the lack of a perpetual state is self-explanatory due to the lack of the rule of law. Regional and or ethnic groups who think that they are marginalized and deprived of a portion of the national pie will try to access power through violent means as has happened in Cote d'Ivoire in recent decades with two civil wars within a decade and numerous coup attempts.

As Weingast[344] reminds us, the system of rent-creation in natural states like Cote d'Ivoire, limits access to organizations, limits competition which in turn hinders the long-term economic growth of the country. The country becomes increasingly poorer, reducing the national pie while inciting different interest groups (ethnic essentially) to wanting the total control over the pie. In such

[343] Weingast, B. (2009, February). *Why are developing countries so resistant to the rule of law?*(Supra note 338) P.217.
[344] Ibid.

atmosphere, there is a calculated and intentional plan by those who hold power at the moment to turn the rule of law into a tool to control the masses.

If you defy the rulers, chances are that you might get entangled in the abyss of the justice system one way or another, whereas by being a pro-government supporter, you might get a slice of the pie depending on your capabilities to bring more of your ilk inside the government tentacles. This state of affairs tends to prioritise the survival of the individual, or the group over the respect and adhesion to the legal and moral norms that govern a civilized society. It is therefore easy to comprehend the flaws of the justice system in most poor countries like African countries.

Very few people in power in Cote d'lvoire as in most African countries really do care about the bad reputation, cybercrimes are inflicting on the country around the world. If by chance, they do care, then the first thing they think about is how they can personally benefit in the name of rebuilding the reputation of the country abroad. In financial terms, that means, the budget dedicated to fighting the scourge of cybercriminality will end up enriching some in government who will offer some lip service. In fact, some people in higher power will even devise plans to get international funds for a so-called fight against cybercrimes or other societal ills just to fill their own pockets.

To be successful in the fight against cybercriminality in West-Africa and especially in Cote d'Ivoire, the authorities must forcefully fight the social and cultural determinants that permeate the social fabric. In order to do that, they must lead by the power of their example which will necessitate the purge of self-serving individuals at all levers of power.

However, we have no illusions that this fight against the culture of general corruption will be easy because money drives everything nowadays. The economic determinant at the heart of all

corruption is extremely powerful in a poor country like Cote d'Ivoire, notwithstanding its number one position as cocoa producer in the world.

Let us analyse the economic determinant to see how it is an obstacle in the fight against cybercriminality before dissecting the political determinant./.

4-4-3-2: Economic Determinant

According to the World Bank[345], prior to the global shock triggered by the pandemic, Côte d'Ivoire had one of the most robust economies in Africa and in the world and had grown at an annual average rate of 8% since 2012. However, as noted by the World Bank, the global health situation adversely affected Ivorian households and businesses and slowed the growth rate to 1.8% in 2020.

Although the World Bank Group (WBG)[346] announced that poverty fell sharply from 46.3% in 2015 to 39.4% in 2020, it also recognized that this decline was confined to urban areas as rural poverty levels rose by 2.4% over the same period.

On the paper, Cote d'Ivoire is the economic hub in Francophone Africa, as the WBG stats show. However, in the real Ivorian world, the economic strength of the nation does not necessarily translate into individual gains for the general population.

[345] *Côte d'Ivoire*. (2021). World Bank. Retrieved March 18, 2022, from https://www.worldbank.org/en/country/cotedivoire

[346] Ibid. "Robust domestic demand and stable exports are expected to drive the country's economic recovery in 2021. While the construction sector and public investments were the main drivers of growth in 2019, the manufacturing sector, services, and exports are expected to support the economic turnaround in 2021.The main challenge remains the implementation of a reform agenda that fosters a sustainable economic recovery and more inclusive growth by promoting the private sector in order to create better jobs, improve the business environment, provide access to financing for SMEs and VSEs, build capacity in the agricultural sector, and develop human capital, among other things".

That is why the WBG said that the country should include its most vulnerable population groups in its economic recovery strategy, further integrate women into the economy, and develop its human capital to better meet the needs of the Labor market.

According to the African Development Bank (ADB)[347], from 2001-2010, six of the world's ten fastest-growing economies were in Sub-Saharan Africa. Africa has weathered the 2008 financial crisis and its economies are recovering, driven by higher commodity prices and export volumes. Yet good economic growth has failed to create enough job opportunities for the young while inequalities in income distribution are a real concern both between and within countries (AEO, 2011).

Although the most unequal countries in the world are located in southern Africa (Botswana, Eswatini, Lesotho, Namibia, South-Africa)[348], one can argue that most African countries including Cote d'Ivoire, are unequal when it comes to wealth redistribution.

[347] African Development Bank. (2011). *Income inequality in Africa*. ADB. https://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Revised-Income%20inequality%20in%20Africa_LTS-rev.pdf

[348] Ibid. "In many countries, notably resource-rich countries, income, and wealth are unequally shared, and stronger average income growth does not necessarily reduce poverty. Africa is the second most inequitable region in the world. In 2010, six out of the ten most unequal countries worldwide were in Sub-Saharan Africa, particularly Southern Africa. The highest rates of poverty can be observed among young women and youth living in rural areas. Young Africans constitute the majority of the poor. On average 72% of the youth population in Africa lives with less than US$2 per day. The incidence of poverty among young people in Nigeria, Ethiopia, Uganda, Zambia, and Burundi is over 80% (ADI 2008/2009, World Bank). Africa accounts for a large share of the world's people living in absolute poverty. More than one billion people in the world live on less than US$ 1 a day and 2.7 billion live on less than US$ 2 per day. Since the late 1980s, the number of people living on less than US$ 1 per day in Sub-Saharan Africa, increased by seventy million to 290 million in 1998, over 46 % of total population and Africa's share of the world's poor rose from just below 20% to close to a quarter (Kayizzi-Mugerwa, 2001). Nowadays, close to 50% of the population in Sub-Saharan Africa lives on less than US$ 1 a day, which constitutes the highest rate of extreme poverty in the world. The number of impoverished people has indeed doubled since 1981. The share of people living on less than US$ 2 a day reaches close to 60% of the population in Liberia and close to 50% in Central African Republic. In North Africa, only 2.2% of the population lives on less than US$ 1 a day, and 23% on less than US$ 2.

In Cote d'Ivoire, more than 70% of the population work in the agricultural sector and these farmers are at the mercy of international commodity market fluctuations like cocoa and coffee. This situation is compounded by the inhumane methods employed by non-scrupulous cocoa and coffee buyers who find ways to buy these products at a loss for farmers. A huge portion of the Ivorian population live on less than $2 a day.

The vast majority of these farmers live in rural areas of the country and do not always benefit from the financial opportunities that people in urban areas (Abidjan, Bouake, San Pedro etc.) enjoy. In other words, the income redistribution in Cote d'Ivoire like in most African countries, is extremely unequal which has a serious impact on the rule of law.

The notions of justice, fairness and moral fibre fly out the window when everyone is seeking the control of the rare resources(financial) of the nation, thus encouraging a general atmosphere of corruption at every level of government and among citizens.

The struggling population has no other ways to survive than to use all means available to do so. Hence, the emergence of economic clans fighting for the control of the national pie, however small it has become.

Today, in Cote d'Ivoire, to get an administrative document be it for personal reasons or business purposes and other, you have to pay someone before seeing your application through.

A few decades ago, people would mostly complain about the corruption of law enforcement, especially those police officers regulating road traffic.

Once they pull you over, chances are you will have to pay them something before being allowed to leave. Since everyone could see these police actions in broad daylight, people tended to see law

enforcement as the only corrupt section of society. Not anymore, as most Ivorians who have dealt with some administrative paperwork can testify of the total corruption everywhere.

In that kind of environment, violating the law and we mean any law or regulation, can be resolved through corruption. You can win a lawsuit even though you are guilty, just by paying money to judges, Attorneys, and everyone in between the judicial ecosystem. Those who are poor and have no connections whatsoever are unfortunately the ones to go to prison when they get caught.

Such reality necessarily creates a sense of injustice, unfairness, and impotence among the population. We are in a situation in which those who have can get away with violating the laws while the have-not cannot do so.

Investigating, prosecuting cybercrimes is all by itself technically complex as even the most advanced investigative agencies like the FBI or Scotland Yard in England find out time to time. If you add an iota of corruption as it happens regularly in developing countries like Cote d'Ivoire, one must admit that winning the fight against cybercriminality is lost before it began. The infamous Ivorian cybercriminal "Commissaire 5500" once said that if he gets caught with a dozen millions of Francs CFA ($20.000) by a police officer who barely make $400 per month, all he has to do is hand him a few thousand dollars in order to be set free right away.

In that, the kind of corruption brought on by cybercriminality in Cote d'Ivoire and elsewhere in West-Africa, is in no way different from the type of corruption one can witness in narco-states in South America where powerful drug dealers reign supreme over the production and export of cocaine.

In fact, as we have seen elsewhere in this research, sometimes, police officers of their own volition, go patrol money transfer agencies looking to "steal" from those cybercriminals who came to withdraw the money they have extorted from their victims, both local and foreign.

Although, we have not heard or seen the existence of cartels comprising young cybercriminals and members of the law enforcement community, we cautiously suspect the probable existence of such groups, but it will take another research by others to uncover such cartels.

On the other hand, we are aware of some degree of complicity between cybercriminals and employees of money transfer agencies and even some banks and or Internet Service Providers (ISPs).

To compound the issue of the near inexistence of the rule of law in most West-African countries, has been the emergence of Covid 19 over the past two years depriving many in the informal economy of their source of income, however small it can be.

Covid-19 has struck informal workers especially hard in Cote d'Ivoire, causing the number of households considered "extremely poor" to spike four-fold, according to the United Nations Development Program (UNDP)[349] and national authorities.

[349] *In Côte d'Ivoire, pandemic prompts surge in extreme poverty | United Nations Development Programme*. (2020, July 6). Press release. https://www.undp.org/press-releases/cote-divoire-pandemic-prompts-surge-extreme-poverty
The entire Press release: "Abidjan — COVID-19 has struck informal workers especially hard in Cote d'Ivoire, causing the number of households considered "extremely poor" to spike nearly four-fold, according to a new assessment by UNDP and national authorities, which will inform policies and programs to help the country recover.
Three surveys—of households, businesses, and the informal economy—found the West African country reeling from lost jobs and lost business, with many people struggling to keep food on the table and often falling back into extreme poverty they had left behind. More than two-thirds of households, or 71.7 per cent, reported lower income, while 85 percent of informal workers cited lost work and income. Some 1.3 million jobs or about one third of all informal jobs have already been lost as a result of the pandemic and lockdown measures to contain it, nearly quadrupling the number of "extremely poor" households.
The most vulnerable people have been hit hardest. Some 1.37 million households, or 45.2 per cent, that had been just above the poverty line have now fallen below it, while the poorest Ivorians have seen incomes plunge 30 percent. Most say the crisis will affect their ability to meet commitments such as paying off debts, obtaining food regularly, and financing school fees.

The pandemic has exacerbated the financial standing of everyday people but also of the state which lost billions in taxes. For one, Covid-19 has pushed many people to work and shop from home, thus magnifying their online exposure to cybercriminals, but also has made worse the financial conditions of everyday people, hence a greater incentive to corruption in order to survive throughout the pandemic.

In fact, cybercrimes around the world have dramatically increased during the pandemic. An Interpol assessment[350] of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure.

"The COVID-19 crisis is an urgent call to revisit our values and behaviors, and an opportunity to deliver a new era of development," Carol Flore-Smereczniak, UNDP Resident Representative in Cote d'Ivoire, said. "It requires proactive policies that address a whole range of systemic challenges."
UNDP conducted these studies with the National Institute of Statistics, with results validated by the Ministry of Planning and Development. The resulting assessment is one of more than 60 country-level analyses of how the pandemic has impacted the world.
Recommendations aimed at response and recovery include:
- Quickly introducing support to businesses and banks.
- Suspending corporate taxes.
- Suspending import taxes.
- Reimbursing value-added taxes, which disproportionately affect the poor.
- Providing subsidies to the informal sector, then monitoring their impact.
- Considering whether and how to formalize informal businesses, which would afford workers more social protection and safety nets.
- Closely monitoring the health of vulnerable people, such as the elderly.
- Working with the financial sector to support vulnerable households.
- Monitoring and mitigating food shortages, in partnership with trade unions, transport workers, and consumers.
UNPD's work in country
On the ground in Cote d'Ivoire, UNDP is using local drone technology to disinfect cities and building online capacity to connect wholesale distributors to people in need. It has also supported the capital's only help center for survivors of gender-based violence, which tends to spike globally during crises. UNDP has also helped expand capacity and recruited and trained staff for the national emergency call center—which now fields some 7,000 calls daily.
UNDP has provided emergency funding to the hard-hit suburb of Cocody to respond to COVID-19, which will be replicated in other communities, and provided personal protective equipment (PPE) to two university hospitals and eight health care facilities. UNDP is also working to raise public awareness about preventing and responding to gender-based violence and child sexual abuse.
In May, UNDP, supported by Japan, provided 80 motorcycles and a large supply of PPE to the Ivorian National Police, to help address violence related to presidential elections scheduled for October 2020 and respond more effectively to cases of gender-based violence—during a time of significantly increased tension".

[350] Interpol. (2020, August). *Interpol report shows alarming rate of cyberattacks during COVID-19*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption. In one four-month period (January to April) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs (all related to COVID-19) were detected by one of Interpol's private sector partners.

The Secretary General of Interpol revealed that cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.[351]

In light of all these recent developments around the world regarding Covid-19, which also affect African countries, including Cote d'Ivoire, one must recognize the difficulties in the fight against cybercrimes in West-Africa in general and in Cote d'Ivoire in particular.

The central determinant that is the economic and financial situation of Ivorians compounded by the health crisis caused by Covid-19 make the fight against cybercrimes all the more arduous for the Ivorian authorities.

One avenue to explore when trying to solve the issue of cybercrimes in poor countries like Cote d'Ivoire, would be to peel away the Ivorian youth from cybercrime activities, through a robust

[351] Interpol. (2020, August). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*.(Supra note 350) P.227. Portion of the Report: "An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure.
With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.
In one four-month period (January to April) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners.
"The increased online dependency for people around the world, is also creating new opportunities, with many businesses and individuals not ensuring their cyber defenses are up to date.
"The report's findings again underline the need for closer public-private sector cooperation if we are to effectively tackle the threat COVID-19 also poses to our cyber health," concluded the INTERPOL Chief.

national program to train young people in computer-related education with the promise of hiring at the end of their training to become the guardians of the Ivorian digital infrastructure.

The Ivorian authorities must also challenge the youth to innovate in fields such as machine learning, artificial intelligence, and other computer-related fields through the financing of a new generation of techpreneurs who will invent and transform the Ivorian future.

The question is if the country's leaders are interested and really motivated to take this route of hope for the youth. Let us examine the political determinant and its impact on the rule of law and the fight against cybercrimes./.

4-4-3-3: Political determinant

Transparency International (TI)[352], a Non-Governmental Organization (NGO) that fights corruption around the world, defines corruption as "the abuse of entrusted power for private gain." It added that corruption erodes trust, weakens democracy, hampers economic development, and further exacerbates inequality, poverty, social division, and the environmental crisis. Political corruption in Africa is well known and has been extensively documented and debated for decades in academic circles around the world. According to Transparency International (TI), corruption can take many forms[353] such as:

- Public servants demanding or taking money or favors in exchange for services,
- Politicians misusing public money or granting public jobs or contracts to their sponsors, friends, and families,
- Corporations bribing officials to get lucrative deals

Transparency[354] is therefore needed in the public conduct of the state business because as TI describes it, transparency is all about knowing who, why, what, how and how much. It means shedding light on formal and informal rules, plans, processes, and actions.

Further, transparency helps us, the public, to hold all power to account for the common good.

However, the "politics of stomach infrastructure"[355], defined by John Sunday Ojo[356] as "the distribution of money and material stuffs as an alternative approach to woo the electorates in order to garner their political conscience during election" is extremely strong in Africa.

---

[352] Transparency International. (2020, August 10). *What is corruption?* Transparency.Org. Retrieved March 19, 2022, from https://www.transparency.org/en/what-is-corruption

[353] Ibid.

[354] Ibid.

[355] Ojo, J. (2019, August). *Politics of Corruption in Africa*. Global Encyclopedia of Public Administration, Public Policy, and Governance. https://www.researchgate.net/publication/322138202_Politics_of_Corruption_in_Africa

[356] Ibid. "The resurgence of politics of stomach infrastructure has been an antiquate one within Africa's political ecology. It dated back to independence which manifests during regional electioneering campaign in Nigeria. The

In a way, corruption is seen in some parts if not all of Africa, as the natural recourse to survive extreme poverty. To do that, entire sections of the population are willing to monetize their support to the politicians willing and able to pay in cash or through co-optations or interventions to resolve a legal issue for the members of the group. Thus, the emergence of what is known in Africa, as the politics of stomach infrastructure John Ojo talks about which is widely accepted in Cote d'Ivoire. In Tanzania, it is even legalized and called "Takrima," meaning traditional hospitality (See Id. 370 below).

As the preamble of the UN convention on corruption states, corruption represents a threat "…to the stability and security of societies, undermining the institutions of democracy, ethical values and justice and jeopardizing sustainable development and the rule of law." As Samuel Atuobi[357] posits, the existence of widespread corruption, especially in societies beset by mass poverty and extremely high levels of unemployment, has a deeply corrosive effect on trust in government and contributes to crime and political disorder. He went on to argue that:

> *In the political realm, corruption undermines democracy and good governance by flouting or even subverting formal processes. Corruption in legislative bodies reduces accountability and distorts representation in policymaking; corruption in the judiciary compromises the rule of law; and corruption in public administration results in the unequal distribution of services. More generally, corruption erodes*

theoretical platform of stomach infrastructure is situated in political clientelism, considering the effectiveness of material benefits for political support, making it difficult for electorates in a fragile region like Africa to safeguard their vote. The typical system of informal political relationship between voters and political contestants is refers to clientelism. For clientelism to become an effective political strategy in an electoral competition, the political parties must incorporate a vast number of local political agents saddled with responsibility to provide information about voter's political preferences so that they can provide material and monetary packages to local populace in order to get political advantage in electoral competition, linking political agents and the electorates. In similar direction, politics of stomach infrastructure also legalized in Tanzania's electoral act, inculcating what is termed as "Takrima" which means "Traditional Hospitality." The clause allows every political contestant in the country to offer gifts such as clothes, money, food and building materials to the electorate during political campaign. This has been devised as a modus operandi and a stratagem of coaxing and entrapping citizens under the travesty of providing material benefits in exchange for vote by the deceitful politicians."

[357] Atuobi, S. (2007, December). *Corruption and State Instability in West Africa: An Examination of Policy Options*. reliefweb.int. https://reliefweb.int/sites/reliefweb.int/files/resources/9BD8A1F729CEB5B8C125746C0049D740-kaiptc-dec2007.pdf

> *the institutional capacity of government as procedures are disregarded, resources are siphoned off, and public offices are bought and sold.3 At the extreme, unbridled corruption can lead to state fragility and destructive conflict and plunge a state into "unremitting cycle of institutional anarchy and violence.*[358]

The political determinant is so powerful as an inhibitor to the enforcement of the rule of law in Africa, that all researchers agree that it is the root-cause of all other types of corruptions in African societies. This is partially true because in most African societies, the leader, especially a political one, is put on a huge pedestal and is seen as the "owner of land" as we call the president in our dialect, Koulango, spoken in the north-eastern part of Cote d'Ivoire. The chief is venerated as a semi-God in some corners of African societies. Thus, the unlimited power politicians at the helm of an African nation hold in their hands. They can buy any type of social support with publics funds and very few will dare ask the hard questions. However, if you are courageous enough to "ask" those hard questions, your head might be rolling in the bushes if you are not too lucky.

[358] Atuobi, S. (2007, December). *Corruption and State Instability in West Africa.(Supra note 357) P.231.*"For the past two decades, internal conflicts with spill over effect have severely disrupted West African social and economic development. The states of the Mano River Union – Guinea, Liberia, and Sierra Leone – have been embroiled in civil wars that have had negative impact on their neighbours. Low intensity conflict in the Casamance region of Senegal has intermittently engaged The Gambia, Guinea Bissau, and Senegal for the past decade, while the oil rich Bakassi Peninsula has been the source of conflict between Cameroon and Nigeria. More often than not, corruption has played a key role in fomenting and prolonging these conflicts by serving as the basis for grievance against political leaders and violent political change. Internal conflicts in West Africa are commonly financed by the illegal sale of arms or the illicit extraction of high value natural resources such as diamonds, gold, and timber. Weapons trafficked across the sub-region are eventually used by rebel groups and criminals for fighting civil wars, as in the case of Liberia, Sierra Leone, and Cote D'Ivoire, among others, or used for armed robbery. Corruption also represents a threat to peacebuilding in post conflict states in West Africa. In spite of the negative effects of corruption on development, peace and security, anticorruption campaigns in the member states of the Economic Community of West African States (ECOWAS) are often cosmetic and rarely address the fundamental problems. Equally, there is lack of adequate research on the relationship between corruption and state stability, particularly in West Africa. An earlier attempt to place corruption on the ECOWAS agenda is found in the Protocol Relating to the Mechanism for Conflict Prevention, Management, Resolution, Peacekeeping and Security. The Protocol on Democracy and Good Governance11 also recognizes the need to fight corruption. In December 2001, the Protocol on the Fight against Corruption was adopted by ECOWAS member states to help address the negative impact of corruption on the political and economic stability of the sub-region. The adoption of the anti-corruption protocol by ECOWAS thus represents an attempt by the regional body to legalize and institutionalize the fight against corruption".

Corruption in West-Africa is so pervasive that even the great writer Franz Fanon wrote in 1961 about corruption in West-Africa:

> *Scandals are numerous, ministers grow rich, their wives doll themselves up, the members of parliament feather their nests and there is not a soul down to the simple police officers or the customs officer who does not join in the great procession of corruption*[359].

Corruption in Africa take many forms as Atuobi[360] detailed it here:

> *A common form of public sector corruption in West Africa is the appearance of 'ghost names' on the civil service payroll. For instance, in Ghana, the deputy Auditor-General disclosed in March 2002 that more than US $20 million had been paid to about 2,000 ghost names in the previous two years.47 According to a survey Report on National Perception and Attitude towards corruption conducted in 2000 by the National Reform Strategy of Sierra Leone, 92.3 % of respondents considered bribery to be the most corrupt practice. In the survey 94% of respondents considered corruption to be most rampant in government departments.48 In Burkina Faso, a corruption survey identified the police as the most corrupt institution. In Senegal, a survey conducted by 'Forum Civil' identified the traffic police, customs officials, and police as the most corrupt institutions. A similar survey in Ghana conducted by the Centre for Democratic Development-Ghana with the World Bank in 2000 revealed that most Ghanaians considered the Motor Traffic and Transport Unit (MTTU) of the Police Services, the Customs Excise and Preventive Service (CEPS), the Regular Police and the Immigration Service as the most corrupt public institutions. Majority of the respondents said they have had to pay bribes to officials in these institutions on some occasions. 49 Most Ghanaian businesses said they felt reluctant using the law courts to address conflict because of the prevalence of corruption in the judiciary.50 The survey result blamed high level of corruption in Ghana on low salaries, culture of gift giving, absence of or weak corruption reporting system and poor internal management practices.51 Political corruption is also rampant. Most state officials – president, ministers, legislators, governors etc – see political offices as opportunity to make wealth. For instance, in September 2006, the Economic Crimes Commission of Nigeria charged 15 of the 36 states governors of corruption. Most of them were suspected of stealing public funds and money laundering.*

[359] Atuobi, S. (2007, December). *Corruption and State Instability in West Africa. (Supra note 357) P.231.*
[360] Ibid.

Political corruption in Africa has sometimes an external factor as Momoh[361] pointed out that corruption in Africa has internal and external dimension which are interrelated in some respect. These are corrupt practices perpetrated by Africans and those conducted by foreigner via collaboration with corrupt Africans.

Since this research is based on the nexus between the rule of law in general and the fight against cybercrimes, we will not delve into the external factors of corruption in Africa, rather, we analyse the degree of success in the fight against cybercrimes within a corrupt environment in West-Africa and especially in Cote d'Ivoire. The fact of the matter is that political corruption in Cote d'Ivoire is a huge obstacle in the fight against cybercrimes for many reasons. For one, law enforcement like everyone else in the nation, tend to justify their corrupt acts through the prism of the behavior of the political establishment. If those in higher positions within the government, are corrupt, we in law enforcement, are also allowed to find ways to make ends meet. It would be impossible to stamp out corruption in Cote d'Ivoire and in any other country for that matter if those in high positions are allowed to get away with corrupt acts.

[361] Momoh, Z. (2015, March). *Corruption and Governance in Africa*. ResearchGate. https://www.researchgate.net/publication/308792420_CORRUPTION_AND_GOVERNANCE_IN_AFRICA
External dimensions: "This dimension involves corrupt practices indulge by foreigners in collaborate with corrupt Africans in order to engage in various illicit capital flow (Money Laundering) and to bribe government officials in Africa in order to secure contracts. For instance, New African Magazine in 2009 reported that on the 25th of September 2009 a UK owned company called Mabey &Johnson (M&J) whose business was to build bridges in some African states like Ghana, Madagascar, Angola, and Mozambique in which the company pleaded guilty at the Southwark crown court in London for bribing government in these African countries in order to secure contracts. In the same vein, there was an allegation of bribery involving the role of BAE systems and other weapons firms in the South Africa's biggest arm deal (the sale of Hawk and Gripen Warplanes for 1.66 billion pounces) (New Africa, November 2009). However, in Nigeria, between 1994 to 2002, there was an investigation conducted that revealed that Halliburton Co-executive, Albert Jack Stanley pleaded guilty for "orchestrating more than $180 million in bribe to top government officials in order to secure contracts (Osumah, and Aghedo, 2013). The Halliburton corruption fraud has been swept under the carpet because of the personalities that was indicted. This also portrays the elevated level of corruption in Nigeria at the institutional level. Nevertheless, Global Witness reported that some British High Street Banks have facilitated money laundering from Nigeria to the UK between 1999 and 2005. Also, the banks made it possible for Late General Sani Abacha, former Governors Bayelsa state DSP Alamieyeseigh and Chief Joshua Chibi Dariye of Plateau state to launder money (Audu, 2010 in Osumah, and Aghedo, 2013). Lastly, in ability of foreign nations to monitor complex activities embark by their "blue-chip" companies but operate in Africa has contributed to their involvement in money laundering, bribing of host countries government officials and indulge in illicit capital flow."

To successfully fight the scourge of cybercrimes in Cote d'Ivoire and in the rest of Africa for that matter, the authorities at the highest level should give the good example and severely repress cases of corruption within the government.

The issue in African countries when it comes to fighting social ills like cybercriminality, is that the culture of not seeing the long-term effects of such practice on the reputation of the nation, is powerfully entrenched in all areas of government.

In some cases, political leaders, encourage the youth to persist in their illegal practices through inaction, half-baked solutions, or outright involvement in those schemes to defraud innocent victims both local and foreign.

As we have said repeatedly, cybercrimes can be complex in nature, due to the transnational aspect of it but also, due to the anonymization of perpetrators of cybercrimes. To sort this complexity out, law enforcement needs the best tools money can get in order to do their job effectively.

However, due to the corrupt nature of the government, some people in higher position will seek to make some money out of the delivery of these tools desperately needed by law enforcement.

Any refusal to agree with such schemes can delay the procurement process Ad Vitam Aeternam[362].

It is fundamental for the political leaders to understand the benefits of the rule of law and know that it guarantees their own safety and assets. A society based on a strong and fair rule of law benefits everyone and quell the need for some to seek regime change.

[362] Forever, for life.

As Leanne McKay[363] noted, the rule of law guarantees us whatever advantages are contained in the law, such as the guarantee of the right to a fair trial. The rule of law can provide certainty or predictability in our interactions with the state and with other members of society, and it can restrict the actions of government officials.

Actually, there is no universal definition of the rule of law but in 2004, the international community agreed on the following working definition of the rule of law:

> *A principle of governance, in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced, and independently passed on judicially, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of the law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency*[364].

This definition which says all persons, institutions, and entities, public and private, including the state itself are accountable to the rule of law is unfortunately inexistent in most West-African countries, including in Cote d'Ivoire. One can even argue that this definition is a little bit "naïve"

[363] L. McKay. (2015). *Toward A Rule of Law Culture.(Supra note 341) P.218.*"In today's world, states face a plethora of domestic, regional, and international challenges related to justice, security, economics, and politics. These challenges, or "stresses," can increase the risk of violence and instability within a country. Stresses may include, for example, war, terrorism, transnational organized crime, civil unrest, natural disasters, ethnic or religious conflicts, human rights abuses, discrimination, and perceived injustice. When rule of law and its institutions, such as the judiciary and law enforcement agencies, are weak, internal, and external stresses make a country more vulnerable to violence and instability and increase the likelihood of the denial of fundamental rights and freedoms. A strong rule of law, however, can aid a government in more effectively and efficiently providing essential justice and security services for its people in a sustained manner.

[364]Ibid. "This definition contains the core element of rule of law, namely, the notion that everyone is accountable to the law. The definition also "has much to say about how the laws are drafted." These elements are known as the procedural elements of the definition and include, for example, that law-making processes should be transparent and that laws must be publicized, accessible, enforced equally, applied fairly, and passed on judicially by an independent decision-making body. The definition also includes substantive elements; that is, it "contains requirements about the content of laws," such as that laws must be consistent with international human rights norms and standards, and must be clear, precise, and foreseeable (people must be able to foresee the legal consequences of their actions). The UN definition has been criticized for being so full of broad concepts that it is impossible to implement, nineteen and for failing to explicitly acknowledge the role of customary, or nonstate, justice mechanisms that are not recognized within the formal justice system. Scholars, practitioners, organizations, and agencies around the world have yet to adopt this definition unanimously, although many of the definitions share many similarities.

as there is no country on earth where one can find the enforcement of this principle, including in the developed countries. Establishing a strong rule of law is a political exercise put in place by people bent on protecting their own interests.

Leanne McKay[365] suggests that creating a society that is based on a strong rule of law is not a purely technical, law-led exercise involving the reform of laws, strengthened justice institutions, and better-trained legal personnel to operate them, is an inherently political exercise that touches on the fundamental interests and concerns of both political and economic elites and the average citizen.

[365] L. McKay. (2015). *Toward A Rule of Law Culture*.(Supra note 341) P.218. "Where people are marginalized, when they lack access to justice and basic services, and suffer from real or perceived inequalities and injustices, the failure of the state and its institutions to protect their rights, prevent discrimination, and ensure the equality of every person before the law can be a significant driver of instability and conflict. Establishing a strong rule of law that protects everyone from injustice and insecurity requires the genuine willingness of government officials and members of society to hold themselves and one another accountable to the law. However, achieving this willingness on both sides can be a significant challenge. Where governments have shown an unwillingness to protect the rights of all citizens and to abide by rule of law, a lack of trust develops between those who govern and those who are governed. To create a strong rule of law, this relationship of trust must be carefully and intentionally rebuilt. Building trust and confidence between government officials and members of society will take time and patience. The decision of a previously corrupt police officer to act with honesty and self-discipline does not require a new law. It does require a change in attitude and behavior. It is this change that will help to build trust with the public. A rights-respecting, rule of law–abiding government does not materialize on its own. It requires the active engagement of all members of society to uphold these principles and to assist the government in creating a social and institutional rule of law culture. To achieve a society that embodies rule of law, a consensus must first be reached on a shared vision for a state. Identifying and agreeing on that shared vision takes time. It requires an open dialogue involving all elements of society to identify, acknowledge, and effectively respond to what people want—their values and desires, as well as their concerns and objections. The process of reaching this vision is likely to require societies to grapple with difficult issues, such as national identity, and, often, to confront a history of violence and injustice. In many contexts where countries are emerging from conflict or authoritarian rule, a new or revised constitution articulates the rules, shared values, and aspirations on which a society has agreed. The constitution provides a framework for the system of laws that apply in a specific context. Further reforms may be needed to ensure, for example, that laws uphold the rights and freedoms enshrined in the constitution, or to define the roles, mandates, and parameters of rule of law institutions, such as protecting the independence of the judiciary. The legitimacy of justice and security institutions, systems, and the officials within them comes not only from this system of laws but also from ensuring that these three entities operate and act with integrity, have the capacity to provide justice and security services for all, are seen to be credible by upholding the shared values of society, and are transparent, and that mechanisms exist for the public to hold them accountable for their actions. Their legitimacy also derives from upholding, promoting, and protecting the rights of all people and all groups within a society. The idea of inclusiveness—namely, that all people are accountable to and protected by the law—is a critical component of rule of law. There cannot be one universal approach to establishing rule of law. Every country struggle to establish its own rule of law vision based on the historical, political, social, cultural, and legal realities of the national context.

The problem with this view is that it recognizes the need to safeguard the interests of the political and economic elites which in a way, defeats the impartiality of the rule of law.

The rule of law would gain substantial force if it were the fruit of independent agencies within the structure of the state itself. Unfortunately, even that assertion does not hold in the face of corruption in poor countries such as Cote d'Ivoire.

Therefore, it is extremely unlikely that political corruption in West-Africa will disappear anytime soon. The political determinant has a powerful impact on how successful, the fight against cybercrimes will be. The risk that members of the government will seek to take advantage of the cybercrime phenomenon is extremely high.

Historically, most societies that have possessed a sufficient amount of permanent public authority to be deemed a state have also been governed by other principles of authority based on patronage and clientele systems.

As John Mbaku[366] pointed out, in Africa, bureaucrats attempt to increase their level of compensation by lobbying lawmakers and politicians and by engaging in other activities to influence the political system and maximize the benefits accruing to them.

---

[366] Mbaku, J. M. (1996). *Bureaucratic Corruption in Africa: The Futility of Cleanups*. CATO Journal. https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/3186/Vol.pdf?sequence=1&isAllowed
"If bureaucrats discover they can earn more income from providing services to groups seeking state favors than from their regular (public) jobs, they may pay more attention to the demands of such interest groups than to the proper enforcement of state laws and regulations and the effective implementation of national development plans. In societies where civil service compensation levels are low, a significant part of the public employee's total compensation may be derived from engagement in outside activities, resulting in a significant increase in bureaucratic corruption. The rules that regulate socio-political relations in a country have a significant impact on the ability of civil servants to seek and secure (either legally or illegally) outside income. In nondemocratic societies, as has been shown by Mwangi Kimenyi, bureaucrats are less constrained in their employment of public resources to lobby legislators and influence those individuals with direct responsibility for determining levels of compensation for the public sector. In fact, in many African countries, most civil servants are members of the politically dominant group and have considerable influence over the allocation of resources. Under these conditions, civil servants behave like interest groups whose primary objective is to put pressure on the political system in an effort to redistribute wealth to themselves. In countries with poorly constructed, inefficient, and non-self-enforcing constitutional rules, opportunistic behavior (including rent

He went on to say that many civil servants also illegally increase their compensation by providing services to interest groups that seek favors from the government.

Political coalitions seeking ways to subvert the existing rules to redistribute national income and wealth in their favor can achieve their objectives by bribing civil servants whose job is to enforce state regulations and implement national development plans, he added.

The political corruption in Africa, which started since the 1960s is unfortunately far from being over at the beginning of the 21st century. Therefore, the political determinant remains a great inhibitor to the rule of law in most African countries and especially in Cote d'Ivoire./.

seeking) is usually quite pervasive. In such countries, the rules that regulate socio-political interaction, have failed to constrain the government. As a result, state intervention in private exchange is equally pervasive. Excessive regulation of economic activities creates many opportunities for rent seeking, including bureaucratic corruption. Corruption in developing countries is often believed to arise from the clash or conflict between traditional values and the imported norms that accompany modernization and socio-political development. Bureaucratic corruption is seen by some researchers, then, as an unavoidable outcome of modernization and development. David Bayley argues that "corruption, while being tied particularly to the act of bribery, is a general term covering the misuse of authority as a result of considerations of personal gain, which need not be monetary." Herbert Werlin defines political corruption as the "diversion of public resources to non-public purposes." In Africa, many people see corruption as a practical problem involving the "outright theft, embezzlement of funds or other appropriation of state property, nepotism and the granting of favours to personal acquaintances, and the abuse of public authority and position to exact payments and privileges" (Harsch). Joseph Nye argues that corruption involves "behavior which deviates from the normal duties of a public role because of private-regarding (family, close clique), pecuniary or status gain; or violates rules against the exercise of certain types of private-regarding influence".

CHAPTER 5: Summary and Recommendations

5-1: Summary

5-1-1: Rule of Law in West-Africa

The rule of law in West-Africa is in no way different from the rule of law in most poor countries around the world. That being said, the level of corruption in West-Africa, which goes hand in hand with the absence of the rule of law, is such that this region tops the index of corruption time to time.

The fundamentals of a strong and legitimate state based on the rule of law, good governance and democracy as seen in the West, are almost inexistent at this time in African countries in general and in West-Africa in particular. The reasons for this situation can be traced to colonial times, when the traditional African rule of law was set aside and replaced with the kind of rule of law that existed in Europe at the time.

In other words, the African society in general was turned upside down overnight. Some portions of the population tried in a variety of ways to oppose the Pax Europa through wars, boycott etc… Others took advantage of the new normal to advance their own interests to the detriment of the community.

In reality, besides the European model of rule of law tailored to the colonies, the colonists introduced corruption in African societies by favoring one group (tribal) over another whose consequences led to the last genocide of the 20th century in Rwanda in 1994.

European powers to achieve their goals of exploitation would pay money to some African kings or local leaders, in order to pacify those reluctant to accept the colonial rule.

And when that did not work as planned, they resorted to outright repression. It was a tragic de-structuration of African societies that still reverberate to this day in how Africans behave with the law.

This is true whether they are leaders of the nation or everyday citizens. Thus, the emergence of powerful inhibitors to the rule of law in Africa which can be grouped into three categories: economic, social, and political determinants.

In that environment fraught with corruption, tribal interests, it does not really matter how strong are the laws adopted in the land, people and interest groups will always find ways to outsmart the system of checks and balances.

To successfully fight against the scourge of the 21st century, cybercriminality, any nation must have the basics of the rule of in place, such as a detached law enforcement community, a judiciary free of corruption, and those at every level of power to submit willingly to those checks and balances as we see here in the United States of America.

5-1-1-1: Economic, Social and Political determinants

West-African nations are not profoundly different from one another when it comes to the factors that inhibit a fair application of the rule of law. In most cases, the nation is led by either one perpetual ethnic group that hoards all the country's assets into a few hands or there is a constant regime change leading to the instability and fragility of the state itself.

The latter case is the most prominent in West-Africa, dubbed the "coup belt" by international observers. From independence in the 1960s until now, West-Africa has experienced numerous military coups in all but one country (Senegal). When the coup fails, most of the time, it leads to a civil war as we saw at the end of the 80s in Liberia, Sierra-Leone in the 90s and Cote d'Ivoire at the beginning of the 21st century.

In fact, Cote d'Ivoire experienced more than one coup or attempt and two (2) civil wars within one decade. This instability of the state in West-Africa helps feed corruption, thus defeating the conditions of good governance.

Even in countries that have become stable politically (Nigeria, Ghana etc.), corruption of the elites and interest groups has not let down. In this gloomy atmosphere, powerful economic, social, and political groups impose their desiderata on the state, outside of any norms considered essential to the rule of law.

The economic determinant is based on the fact that the strong few in the country hoards the majority of the country's assets and operate a selective distribution to some subgroups and turn them dependent on those at the helm.

Thus, the rule of law is for "others," the poor and non-connected who by reflex, and to survive the extreme poverty in African countries, offer their own services to get a slice of the pie, however small it may be.

The extreme inequalities observed in African societies derive from this system of rent-creation as Weingast posits, leading to a cycle of unending poverty. The social determinant acts as the normalizer of the corruption culture we observe in African countries, especially in West-Africa. This social determinant can even make someone look stupid if he or she does not take advantage of their social, economic, or political position.

Growing up in Cote d'Ivoire, we have heard numerous times, different people condemning one of their own holding an important position, for not stealing enough and fast from the company or the state agency where he or she works. This is the entrenched culture anyone can observed on the streets of West-African cities with law enforcement dealing with road traffics for example.

The political determinant is the most powerful inhibitor to the fair application of the rule of law in West-Africa, as the general populace tend to imitate what is done by national leaders. Unlike western societies in which, in order to make huge money, people tend to go into the private sector, in West-Africa, it is the opposite: if you want to make easy and colossal amount of money, you will go work in the public sector.

Most African politicians seek the political power structure not to advance the interests of the state, to "fix an injustice" against their ethnic groups because they harbour the idea that they have long been excluded from the national pie by other groups.

In most African societies, there is always this perpetual tension between ethnic, financial, and social groups that jockey to supplant the other groups in the control and redistribution of the national wealth.

5-1-1-2: Impacts of the old determinants on the Fight Against Cybercriminality

Cybercrimes, like other more traditional types of crimes, demands the forceful attention of the national authorities in order to successfully eradicate them from society.

To achieve this noble goal, a nation must have a strong culture with regard to the respect and obedience to the rule of law. The complexity of cybercrimes by itself demands even more focus on the part of the authorities.

Unfortunately, West-African countries, plagued by the economic, social, and political determinants that inhibit the rule of law, are struggling to put out the fire of cybercrimes in most West-African countries.

From Abuja (Nigeria) to Accra (Ghana), Dakar (Senegal) and other West-African capitols, the conclusion is the same: while the scourge of cybercrimes takes deep roots within these countries, the different authorities are struggling to win the fight against cybercrimes.

In fact, the situation is getting worse as some cybercriminals are now extradited to the United States for prosecution as was the case with a Ghanaian national in 2021. Some people in some African quarters, not only benefit from cybercrimes, financially and other, they even encourage it because they see the western victims of cybercrimes as “paying back” a portion of what the West “stole” from Africa.

Obviously, the African victims of cybercrimes and they are many, do not think that way, quite the opposite. Cybercrime activities against already poor Africans by other Africans is seen as a recipe for disaster for the victims who sometimes lose all their savings to unscrupulous cybercriminals roaming the streets of Lagos, Accra, Cotonou and beyond.

The political web that metastasizes and permeates the African social corpus is inextricably linked to the weakness of the rule of law for it is based on open corruption, quid pro quo and other shenanigans undertaken by political leaders to control the African masses. Therefore, the rule of law in African countries in general and in West-Africa in particular, is a concept in name only.

This lead most West-African nations to a standstill in terms of good governance, enforcement of the laws on the books, individual freedoms, and a democratic competition to oversee the business of the nation.

In conclusion, the fight against cybercriminality does not have a much greater chance to succeed if those long-term inhibitors (economic, social, political) to the rule of law are not weeded out from West-African countries.

There is a tiny bit of good news in that the two economic giants in the region, Nigeria, and Ghana, have after 2 decades of practice, a solid democratic foundation on which to build a fairer society in the coming decades.

It would be extremely beneficial for the whole region, if those two countries can teach the other countries, the intricacies of a society trying to achieve democratic norms. It is obviously far from being perfect in these two countries, but the political aspect is encouraging, and Cote d'Ivoire should learn from them.

Cote d'Ivoire being a prominent member of West-African states community is not better than the others when it comes to enforcing the rule of law in a fair, just and rigorous manner.

In fact, it is unfortunately, one of the most corrupt countries in West-Africa, compounded by multiple social disruptions and two civil wars within the last decade.

5-1-2: Rule of Law in Cote d'Ivoire

Cote d'Ivoire like most African countries was colonized by France at the end of the 19th century until 1960, when it became an independent country on August the 7th of that year. Before the arrival of the French, Cote d'Ivoire was a grouping of kingdoms regulated by traditional laws and customs.

These traditional laws were strictly respected by every member of the community and based on the premise that the elders cannot be wrong in any way, shape, or form. Therefore, violating the customs and other restrictions put in place by them was seen as highly destructive for the community as a whole.

The Ivorian kingdoms also practised slavery which made impossible for some former slaves to have the same rights as their former masters. The social order was thus respected by everyone and, people would stay in "their lane." All this social construct will disappear overnight with the arrival of the Europeans colonists and the introduction of rules of law imported from Europe.

The implementation of these European rules of law turned the Ivorian societies upside down. The local populations had to learn a new set of rules, foreign to them, that put everyone on an equal footing and in some cases, made former slaves the new "masters" of their former masters.

The French, by operating on a system of preferences among the myriad of tribal groups, introduced a system of corruption in Ivorian societies by favouring some groups over others, using money as a power to convince some kings to go along with their projects to exploit the land. These episodes of quid pro quo introduced by them have persisted to this day. It is no doubt one of the force multipliers of the quasi-inexistence of the rule of law in African societies and particularly in Cote d'Ivoire.

5-1-2-1: Economic, Social and Political determinants

Just as we saw how the economic, social, and political determinants have acted to inhibit the rule of law in most West-African countries, those same determinants exist in Cote d'Ivoire, notwithstanding it relative development compared to many other African countries.

In fact, it made things even more complex, in that powerful economic, ethnic, and foreign groups compete to get the bigger slice of the pie. The Ivorian social construct is in no way different from its West-African counterparts, except that over the past few years, in light of the two civil wars and numerous coup attempts, people want to make it big and fast because no one knows what the near future hold.

Therefore, everyone is in a perpetual rush to secure as many assets as they can get from the system. Thus, those social, economic, and political forces stand in the way of a just enforcement of the laws of the land.

They have permeated the Ivorian society to such a degree, that even national exams are not corruption-free. The reality today in Cote d'Ivoire, just as in other West-African nations, is that everything is a "deal" that must bring in some revenue.

No section of the nation is immune from this sad reality. Therefore, enforcing the laws against traditional crimes as well as cybercrimes, which involve millions of dollars each year, is fraught with lapses, quid pro quo, and sometimes outright undue influence from the powerful.

In conclusion, one must recognize that the economic, social, and political determinants impact negatively the fight against cybercriminality both in Cote d'Ivoire and in the rest of West-Africa.

5-1-2-2: Impacts of the old determinants on the Fight Against Cybercriminality….

The fight against cybercriminality in Cote d'Ivoire is strongly impacted by the economic, social, and power structure of the country. As we have seen over and over, what is going on in West-African nations, in terms of the health of the rule of law is in no way different from what has been going on in Cote d'Ivoire.

Cote d'Ivoire, just like other African nations in the western part of the continent, is plagued by social and political instability, especially over the past two (2) decades. The passing of the founder of Cote d'Ivoire, President Felix Houphouet Boigny in 1993, has left a big hole in the Ivorian public discourse which led to the formation of three political entities among the three biggest ethnic groups in the nation.

The power struggle that begun after 1993 would reach its maximum apex in 1999 with the first military coup in the history of Cote d'Ivoire. Unfortunately, it would not be the last coup, rather, it would give rise to multiple coups attempts that later morphed into two devastating civil wars. Although the health of the rule of law in Cote d'Ivoire, was not excellent pre-political instability, it worsened with the new instability paradigm.

The civil wars will in fact show the failure of the rule of law in Cote d'Ivoire, by creating a new class of rich warlords involved in a myriad of traffics (gold, diamond, coffee, cocoa etc…). To make things worse, these "nouveaux riches" would show off their riches, thus giving ideas to the Ivorian youth on the possibility to get immensely rich and faster.

The pervasive culture deriving from this state of affairs in Cote d'Ivoire at the beginning of the 21st century will later give rise to the phenomenon known as "Brouteurs" who specialized in cybercrimes, witchcraft, and other sordid rituals to become rich as fast as possible.

The social and political changes in Cote d'Ivoire over the past two decades, have forcibly weakened the rule of law in the country. Therefore, and to give some answers to the questions asked in the introductory chapter, we have to recognize that:

1- The rule of law in Cote d'Ivoire is not strong enough to facilitate the successful fight against cybercriminality. More must be done to win the fight.
2- The Ivorian law enforcement authorities are not well-equipped, nor skilled enough even if they are "motivated" to safeguard the reputation of Cote d'Ivoire around the world.
3- To win the "war on cybercrimes," Cote d'Ivoire needs strong cooperation with more advanced nations like France, the European Union, and the United States on a yearly basis.
4- The fight against cybercriminality can help strengthen the rule of law in Cote d'Ivoire, but only if the economic, social, and political inhibitors are purged from the public discourse.

5-2: Recommendations

5-2-1: West-Africa

West-Africa through the regional body, ECOWAS has been doing some fantastic work to stamp out the scourge of cybercrimes inside its member-states. Some of the legal frameworks adopted by ECOWAS earlier on, have had some influence on other regions of Africa and even at the African Union level. Here are a few recommendations West-African countries through ECOWAS can put to good use for the benefit of West-African populations:

West-African countries through ECOWAS should adopt a number of directives with regard to the fair implementation of the rule of law in West-Africa. One directive would focus on strengthening the judiciary in each country by funding the hiring and training of the personnel at each ministry of justice.

ECOWAS should ask its international partners (UN,EU, Council of Europe, United States) for technical and financial assistance to tackle cybercrimes more effectively in West Africa.

ECOWAS should also ask each member state to dedicate a substantial amount of funds to the reform of the justice system through hiring and training more legal personnel, judges, and magistrates.

ECOWAS must find practical ways to strengthen the judicial cooperation between member-states. In order to succeed in the interstate cooperation aspect, we think the language barrier between Francophones and Anglophones should “disappear” one way or another at the law enforcement level. Each country should train a new crop of police officers in the opposite language who will intern in one of the countries speaking a different language. For example, Nigeria could train a few police officers in French and send them for an internship in Cote d’Ivoire where they will work

with the Platform for the fight against cybercrimes (PLCC), while Cote d'Ivoire sends officers to Accra which send officers to Dakar (Senegal) etc… Within a noticeably short time, we would have a network of Police officers who can work anywhere in West-Africa on cybercrime cases that involve multiple countries.

The other recommendation would be for every country in the region to commit to fighting the inhibitors to the rule of law such as special interest groups that operate some sort of balkanization of the nation in terms of economic, social, and political interests./.

5-2-2: Cote d'Ivoire

Cote d'Ivoire is a vibrant country with a young population and is one of the most advanced countries in West-Africa. The opportunities to make it an emerging economy in the coming decades are endless. However, to achieve its development goals in the coming years, the country's authorities must stamp out the scourge of corruption which weaken the rule of law.

Democracy, good governance, and a solid civil society are the foundations for an economic success that benefit the vast majority of the population.

The Ivorian authorities should take drastic measures to fight corruption at the highest level of government to give an example for the general population to follow. One avenue in the fight against corruption would be to revive a policy set in place by the previous Gbagbo Administration which consisted in hiring members of financial agencies through a national exam as opposed to choosing someone close to the authorities.

The mandate of these civil servants in the highest positions should be limited so as to avoid any culture of entrenchment which always lead to corruption.

Those guilty of alleged corruption at the highest level of government should face the weight of justice, irrespective of their personal connections in government.

To fight and win the war against corruption, the Ivorian government should make a number of legal reforms focus on the repression of any corrupt actions by civil servants and the public in general.

Once high-profile corruption cases are extensively broadcasted in the media, it will have the effect of seeding fear in anyone tempted to engage in corrupt acts.

Cote d'Ivoire should ask its international partners (UN,EU, Council of Europe, France, United States) for technical and financial assistance to tackle cybercrimes more effectively in the country. Such request could be done through ECOWAS and even through the African Union.

The different cyber laws against cybercrimes adopted more than a decade ago, should be updated to reflect the new reality of cybercrimes in Cote d'Ivoire. For example, those laws must be made to inflict the maximum jail time and fine onto those guilty of cybercrimes activities. The government has promised to double the fines and jail time contained in the 2013 laws against cybercrimes. We think the government should go further, by targeting not only cyber laws but also by adopting new laws against corruption in general with stiff penalties for the guilty ones.

To successfully fight the scourge of the 21st century, cybercriminality, the authorities could initiate the training at the national level of young people who are interested in computer science. Here, the objective would be to train scores of young men and women in fields such as machine learning, Artificial intelligence, cloud computing etc… and hire them to work in specialized units to advance the goals of becoming an emerging country in coming decades.

To do that, the Ivorian authorities must be bold, ambitious, and ready to finance this national project. Once young people who know how to use a computer learn that they can have a career in computer science, some of them will be peeled away from committing cybercrimes which can lead them to jail.

Once again, the trick is for the government to produce a sizable project in the field of information and communication technologies addressed to the Ivorian youth.

It means that Cote d'Ivoire must have the ambition to train the next generation of Artificial intelligence specialists who will help solve some of the issues specific to Cote d'Ivoire but also to other African countries.

The education of the youth must become a national priority as opposed to spending taxpayer money on Herod-like infrastructures.

One other avenue to peel away young people from committing cybercrimes, would be to institute national or regional awards for those young people who excel in computer science. That being said, the authorities should not stop at the awards: the hiring of the winners by the Administration but also the private sector, will show the youth that there is a future outside of cybercrimes.

The Ivorian law enforcement agencies should get all the equipment and training needed to do their jobs. Law enforcement officers should also be well paid to motivate them in their work.

The economic, social, and political inhibitors to the rule of law should be dealt with by the authorities if they want to succeed at their jobs and gain the trust of the Ivorian people./.

Bibliography

1 M'Begniga, Abdoulaye & Guang, Ma. (2017). African Customary Law and Modern Law from Western: An Overview on Their Roles and Impacts in African Societies. 5. 188-192.

2 Mutua, Makau, Africa and the Rule of Law (July 7, 2016). SUR 23 - v.13 n.23, 159 - 173, 2016, Available at SSRN: https://ssrn.com/abstract=2838309.

3 Joireman, S. (2001). Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy. The Journal of Modern African Studies, 39(4), 571-596. Retrieved January 22, 2021, from http://www.jstor.org/stable/3557341

4 John W. Harbeson and Donald Rothchild, eds., Africa in world politics: reforming political order, 4th ed. (Boulder, Colorado: Westview Press, 2008).

5 Raef, Meeuwisse. Cybersecurity for beginners. London, UK: Cyber Simplicity Ltd, 2017. P. 3.

6 Paul, Day. Cyber Attack: The truth about digital crime, cyberwarfare, and government snooping. London, UK: Carlton Publishing Group, 2014.

7 Dr. Michael McGuire. Into the Web of Profit: Understanding the Growth of the Cybercrime Economy. Bromium Inc. *2018*

8 Center for Strategic and International Studies. Economic impact of cybercrime. 2018 https://www.csis.org/analysis/economic-impact-cybercrime *(accessed on 02/03/19)*

9 Andrews, Atta-Asamoah. Understanding the West African Cybercrime process. Institute for security studies: African Security Review Vol 18. No 4.

10 *Africa*. (2020, September 15). United Nations. https://www.un.org/en/sections/issues-depth/africa/index.html

11 Council of Europe. (2018). Budapest Convention and related standards. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

12 McLeod, S. A. (2014, Feb 05). *Case study method*. Retrieved from https://www.simplypsychology.org/case-study.html

13 Bingham, T. (2011). The Rule of Law (Reprint ed.). Penguin UK

14 Choi, N. (2019, August 27). Rule of law. Encyclopedia Britannica. https://www.britannica.com/topic/rule-of-law *(Accessed on 01/19/2020)*

15 University of Southern California. (2020, March 19). Brief History of Jim Crow Laws | Online LLM Degree. Online International LLM Degree Program. https://onlinellm.usc.edu/a-brief-history-of-jim-crow-laws/ *(Accessed on 01/29/2021).*

16 American Bar Association. (2019). Rule of Law. ABA. https://www.americanbar.org/groups/public_education/resources/rule-of-law/ *(Accessed on 02/07/2020)*

17 United Nations. (2020). Human Rights. UN. https://www.un.org/en/sections/issues-depth/human-rights/ *(Accessed on 02/23/2019).*

18 N.A. Curott, Foreign Aid, the Rule of Law, and Economic Development in Africa, 11 U. BOTS. L.J. 3, 14 (2010).

19 United Nations Office on Drugs and Crime report. Transnational organized crime in the West African Region, P.4.

20 Heyl, C. (2019, July 29). The Judiciary and the Rule of Law in Africa. *Oxford Research Encyclopedia of Politics.* Retrieved 31 Jan. 2021, from https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1352.

21 Kshetri N. (2013) Cybercrime and Cybersecurity in Sub-Saharan African Economies. In: Cybercrime and Cybersecurity in the Global South. International Political Economy. Palgrave Macmillan, London. https://doi.org/10.1057/9781137021946_8

22 Brian Harley "A Global Convention on Cybercrime?" March 23, 2010. The Columbia Science and Technology Law Review. Volume XX (2010-2011). http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/ (Accessed on 05/09/19)

23 Antonio, F. (2018). *Library â€ ¢ ICT Policy Africa*. A.U. https://ictpolicyafrica.org/

24 Council of Europe. (2018). *Budapest Convention and related standards*. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

25 GDPR.eu. (2019, February 19). General Data Protection Regulation (GDPR) Compliance Guidelines. https://gdpr.eu/

26 Human Rights Watch Briefing Paper. (2004). *Côte d'Ivoire Accountability for Serious Human Rights Crimes Key to Resolving Crisis*. H.R.W. https://www.hrw.org/legacy/backgrounder/africa/cote1004/accountability.pdf

27 *Ubi societas, ibi ius*. "Wherever there is society, there is law." A maxim meaning that law may be found in all forms of stable ... (2011). Oxford Reference. https://www.oxfordreference.com/view/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-2028?rskey=8TGbxr&result=2029

28 Mbambi, V. K. (2005). Originally African rights in recent codification movements: the case of French-speaking sub-Saharan African countries. Les Cahiers de droit, 46 (1-2), 315–338.https://doi.org/10.7202/043841ar (Accessed on 02/12/2021).

29 *Africa: Laws and Legal Systems*. (2016). Laws and Legal Systems. https://geography.name/laws-and-legal-systems/ (Accessed on 02/17/2021).

30 The African usual way to identify Europeans instead of the country of origin.

31 Thierry Verhelst. (1968). *Safeguarding African Customary Law: Judicial and Legislative Processes for its Adaptation and Integration*. African Studies Center University of California, Los Angeles, California. https://escholarship.org/content/qt33g2v27d/qt33g2v27d_noSplash_42d5da862de9136b469c2414312669d6.pdf

32 Matala-Tala, L. (2013). The ineffectiveness of positive law in sub-Saharan Africa [1]. Civitas Europa, 2 (2), 239-260.https://doi.org/10.3917/civit.031.0239 (Accessed on 02/18/2021).

33 The United Nations Democracy Fund-UNDEF-. (2016). *UDF-IVC-11-417: Promotion of democratic dialogue and social cohesion in western Côte d'Ivoire*.https://www.un.org/democracyfund/sites/www.un.org.democracyfund/files/cote_divoire_-_udf-11-417-ivc_-_evaluation_report.pdf (Accessed on 02/18/2021).

34 Moyrand Alain. Reflections on the introduction of the rule of law in French-speaking black Africa. In: International review of comparative law. Vol. 43 N°4, October-December 1991. pp. 853-878; doi: https://doi.org/10.3406/ridc.1991.4401 https://www.persee.fr/doc/ridc_0035-3337_1991_num_43_4_4401

35 Chantal VLÉÏ-YOROBA, "Family law and family realities: the case of Côte d'Ivoire since independence," Clio. History ,women and societies [Online], 6 | 1997, posted on January 01, 2005, Accessed February 19, 2021. URL: http://journals.openedition.org/clio/383 ; DOI : https://doi.org/10.4000/clio.383 .

36 Granger Roger. Tradition as a limit to legal reforms. In: International review of comparative law. Flight. 31 N ° 1, January-March 1979. pp. 37-125;doi: https://doi.org/10.3406/ridc.1979.3348 https://www.persee.fr/doc/ridc_0035-3337_1979_num_31_1_3348 (Accessed on 02/24/2021).

37 Kotto, R. (2019, January 14). Chez nous pays: Discover the inter-ethnic alliances in Côte d'Ivoire | Life Magazine. Lifemag-Ci. https://lifemag-ci.com/chez-nous-pays-decouvrez-les-alliances-inter-ethniques-en-cote-divoire/ (Accessed on 02/24/2021).

*Ethnic group from neighbouring Ghana.

38 UNESCO announces the creation of a mobile application for interethnic alliances in Côte d'Ivoire. (2020). Abidjan.Net. https://news.abidjan.net/h/682520.html (Accessed on 02/25/2021).

39 Community here refers to ethnic communities living in urban areas like Abidjan, the commercial hub.

40 *Culture*. (2020). The Merriam-Webster.Com Dictionary. https://www.merriam-webster.com/dictionary/culture (Accessed on 02/27/2021).

41 Stability pacts and confidence building in the process of social cohesion. (2011).https://gerflint.fr/Base/Afriqueouest3/amoa2.pdf (Accessed on 02/27/2021).

42 *Legal pluralism in land matters in West Africa: the case of Côte d'Ivoire. (2016).* Sylvia Soro, Daniel Lopes, Seynabou Samb. https://www.legitimus.ca/static/uploaded/Files/Documents/Rapports/Rapports2/Le-pluralisme-juridique-en-matiere-fonciere-en-Afrique-de-l%E2%80%99Ouest---le-cas-de-la-Cote-d%E2%80%99Ivoire.pdf (Accessed on 03/01/2021).

43 Degni-Segui, R. (1995). Access to justice and its obstacles. *Law and Politics in Africa, Asia, and Latin America, 28*(4), 449-467. Retrieved March 4, 2021, from http://www.jstor.org/stable/43110616.

44 United Nations. (1948, December). *The Universal Declaration of Human Rights*. un.org. https://www.un.org/en/universal-declaration-human-rights/ (Accessed on 03/03/2021).

45 United Nations Human Rights. (1966, December). *International Covenant on Civil and Political Rights*. ohchr.org. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed on 03/03/2021).

46 Cote d'Ivoire Constitution, Art. 6: "The right of everyone to free and equal access to justice is protected and guaranteed. Everyone has the right to a fair trial and to judgment rendered within a reasonable period as determined by law. The State promotes the development of local justice."

47 *Cote d'Ivoire | Data*. (2020). The World Bank. https://data.worldbank.org/country/cote-divoire

48 UNESCO Institute for Statistics. (2020). *Côte d'Ivoire | UNESCO UIS*. Sustainable Development Goals. http://uis.unesco.org/en/country/ci (Accessed on 03/03/2021).

49 USAID. (2020). *Increasing Access to Justice*. U.S. Agency for International Development. https://www.usaid.gov/cote-divoire/fact-sheets/increasing-access-justice (Accessed on 03/03/2021).

50 *Child-friendly legal aid in Africa. (2011).* https://www.unodc.org/documents/justice-and-prison-reform/Child_Friendly_Legal_Aid_in_Africa.UNICEF.UNDP.UNODC.fr.pdf (Accessed on 03/12/2021).

51 *Cote d'Ivoire 2019 Human Rights Report*. (2019). US Embassy. https://ci.usembassy.gov/wp-content/uploads/sites/29/COTE-DIVOIRE-2019-HUMAN-RIGHTS-REPORT.pdf (Accessed on 03/11/2021).

51 Picture: “Commissaire 5500”, famous cybercriminal living free in Abidjan, Cote d’Ivoire.

52 https://en.wikipedia.org/wiki/Ivory_Coast (Accessed on 01/14/2020)

53 Boddy-Evans, Alistair. "A Very Short History of Côte D'Ivoire." ThoughtCo, Feb. 11, 2020, www.thoughtco.com/very-short-history-of-cote-divoire-43647.

54 https://www.legallanguage.com/legal-articles/ivory-coast-history-facts/ (Accessed on 01/12/2020).

55 Source: US Library of Congress. http://countrystudies.us/ivory-coast/3.htm (Accessed on 1/29/2020)

56 https://en.wikipedia.org/wiki/History_of_Ivory_Coast (Accessed on 02/07/2020)

57 J.C Berthelemy, F. Bourguignon. “Growth and Crisis in Cote d’Ivoire.” May 1996. World Bank. Comparative Macroeconomic Studies.

58 Robert E. Handloff, ed. *Côte d’Ivoire: A Country Study*. Washington: GPO for the Library of Congress, 1988. http://countrystudies.us/ivory-coast/3.htm

59 Laurent Bigot. as cited in “Ivory Coast: in fact, who won the presidential election of 2010?”. Le Monde Afrique. May 27th, 2016. https://www.lemonde.fr/afrique/article/2016/05/27/cote-d-ivoire-mais-qui-a-gagne-la-presidentielle-de-2010_4927642_3212.html (Accessed on 06/23/2020).

60 Voanews.com. Africa. “Rights Group Decry Trafficking of Nigerian Women in Ivory Coast”. August 26,2010. https://www.voanews.com/africa/rights-group-decrys-trafficking-nigerian-women-ivory-coast

61 United Nations Office on Drugs and Crime. “Transnational Organized Crime in the West African Region.” United Nations, New York. 2005.

62 Ryan Flores, Bakuei Matsukawa et. al. *“Cybercrime in West-Africa: poised for an underground market.”* Trend Micro, Interpol joint research paper. 2017. www.trendmicro.com , www.interpol.int .

63 Stephen Ellis interviews with law enforcement officers in Abidjan, 1997.

64 Morie Lengor, as cited in “United Nations Transnational Organized Crime Assessment Form: Sierra Leone,” April 2004.

65 Alain Sissoko as cited in, “United Nations Transnational Organized Crime Assessment Form: Côte d’Ivoire,” April 2004.

66 Etannibi E.O. Alemika, as cited in "United Nations Transnational Organized Crime Assessment Form: Nigeria," April 2004,

67 Etannibi E.O. Alemika, as cited in "United Nations Transnational Organized Crime Assessment Form: Nigeria," April 2004,

68 http://www.gartner.com/it-glossary/

69 The Mobile Economy West-Africa 2019. www.gsmaintelligence.com/research .

70 Mutsa Chironga, Hilary De Grandis, Yassir Zouaoui. *Mobile financial services in Africa: Winning the battle for the customer*. September 2017. Article. https://www.mckinsey.com/industries/financial-services/our-insights/mobile-financial-services-in-africa-winning-the-battle-for-the-customer (Accessed on 07/05/19).

71 http://www.think-progress.com/africa/performance-and-productivity/power-to-the-people-the-impact-of-digitisation-in-africa/ (Accessed on 07/05/19).

72 Longe, O. B., Chiemeke, S. C, Onifade, O. F. W., Balogun, F. M., Longe, F. A. & Otti, V. U. (2007). Exposure of children and teenagers to Internet pornography In Southwestern Nigeria: Concerns, trends & implications. Journal of Information Technology Impact, 7(3), 195-212. Retrieved from http://www.jiti.net/v07/jiti.v7n3.195-212.pdf

73 https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (Accessed on 12/23/19)

74 Longe, O. B., Chiemeke, S. C, Onifade, O. F. W., Balogun, F. M., Longe, F. A. & Otti, V. U. (2007). Exposure of children and teenagers to Internet pornography In Southwestern Nigeria: Concerns, trends & implications. Journal of Information Technology Impact, 7(3), 195-212. Retrieved from http://www.jiti.net/v07/jiti.v7n3.195-212.pdf

75 https://en.wikipedia.org/wiki/Ghana (Accessed on 1/9/2020)

76 https://www.nbcbayarea.com/news/national-international/76-year-old-new-jersey-woman-tricked-into-giving-away-125000-to-online-boyfriend/1961429/ (Accessed on 1/12/20).

77 https://abc7.com/fbi-serves-arrest-search-warrants-in-south-bay-connected-to-international-scams/5485625/ (Accessed on 1/12/20).

78 https://cybersecurity.gov.gh/ (Accessed on 1/14/20)

79 Wikipedia contributors. (2021, March 29). *Phishing*. Wikipedia. https://en.wikipedia.org/wiki/Phishing

80 G Urbas and KR Choo, Resource materials on technology-enabled crime, AIC, Canberra, 2008, p.85; Symantec Corporation, Symantec Report on the Underground Economy July 07 – June 08, Symantec Corporation, November 2009, p.19.

81 Meharchandani, D. (2020, December 7). *Staggering Phishing Statistics in 2020*. Security Boulevard. https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/#:%7E:text=A%20single%20spear%20phishing%20attack,the%20malicious%20link%20or%20attachment.&text=81%25%20of%20all%20mobile%20phishing%20attacks%20were%20launched%20outside%20of%20email.

82 Sari, O. (2021, March 10). *The Biggest Data Breaches in the first half of 2020 - Keepnet Labs*. Anti-Phishing Solution and Security Awareness Training - Keepnet Labs. https://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020/

83 Google Inc. (2014). *Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild*. http://intellivoire.net/wp-content/uploads/2014/11/google_hijacking_study_2014.pdf (Accessed on 03/29/2021).

84 *What Email Phishing Scams Do and How to*. (2020). © Copyright 2004 - 2021 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-phishing#:%7E:text=Email%20Phishing%20scams%20are%20carried,passwords%20and%20credit%20card%20numbers. (Accessed on 04/09/2021).

85 *Banking & Financial Services Cyber Threat Landscape Report*. (2019). https://wow.intsights.com/rs/071-ZWD-900/images/Banking%20%26%20Financial%20Services%20Cyber%20Threat%20Landscape%20Report.pdf (Accessed on 04/09/2021).

86 U.S. Embassy in Cote d'Ivoire. (2015, December 7). *419 Scams | U.S. Embassy in Cote d'Ivoire*. https://ci.usembassy.gov/embassy/embassy/sections-offices/419-scams/?_ga=2.105688195.122874908.1583284762-452227721.1583284762

87 *Romance Scams*. (2020, April 16). Federal Bureau of Investigation. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams (Accessed on 03/22/2021).

88 *Romance scams take record dollars in 2020*. (2021, February 10). Federal Trade Commission. https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020 (Accessed on 03/22/2021).

89 *What You Need to Know About Romance Scams*. (2021, March 4). Consumer Information. https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams (Accessed on 03/22/2021)

90 Testimonial: 3 months of love and dirty water. (2017, April 2). [Romance Scams]. ArnaqueInternet.com. https://arnaqueinternet.com/racontez-votre-histoire/arnaques-aux-sentiments/3-mois-d-amour-et-d-eau-sale/ (Accessed on 03/22/2021).

91 Federal Bureau of Investigation. “Scams and Frauds from A to Z.” San Bernardino, CA. August 4th, 2017.

92 Finn Brunton. “The long, weird history of the Nigerian e-mail scam.” Globe Correspondent, May 19, 2013, 12:00 a.m. https://www.bostonglobe.com/ideas/2013/05/18/the-long-weird-history-nigerian-mail-scam/C8bIhwQSVoygYtrlxsJTlJ/story.html (Accessed on 09/09/2020).

93 https://ci.usembassy.gov/embassy/embassy/sections-offices/419-scams/ (Accessed on 09/23/2020).

94 www.aducademy.com

95 https://www.lexico.com/en/definition/malware (Accessed on 02/13/2020).

96 See Cybercrime and Cybersecurity: Trends in Africa. 2016. Symantec/African Union.

97 https://www.symantec.com/blogs/threat-intelligence/african-financial-attacks (Accessed on 03/12/2019).

98 Infocyte Inc. (2018). *The Threat of Malware in Africa*. https://www.infocyte.com/wp-content/uploads/security_brief-malware_in_africa.pdf (Accessed on 04/12/2021).

99 *Fake Dating Apps Found as Top Source of Malware in Africa - Security News - Trend Micro ZA-EN*. (2020). Trend Micro. https://www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/fake-dating-apps-found-as-top-source-of-malware-in-africa (Accessed on 04/14/2021).

100 *Thousands of Cheap Android Phones in Africa Were Pre-Installed with Malware*. (2020). Pcmag.com. https://www.pcmag.com/news/thousands-of-cheap-android-phones-in-africa-were-pre-installed-with-malware (Accessed on 04/12/2021).

101 scidev.net. (2020, October 8). *Cyberattack surge highlights Africa security risk*. Sub-Saharan Africa. https://www.scidev.net/sub-saharan-africa/news/cyberattack-surge-highlights-africa-security-risk/ (Accessed on 04/12/2021).

102 *What is Sextortion?* (2016, May 23). Federal Bureau of Investigation. https://www.fbi.gov/video-repository/newss-what-is-sextortion/view (Accessed on 04/16/2021).

103 Sommerlad, N. (2017, April 3). “Sextortion” gangs’ extortion 30 teenagers a day by luring them into webcam sex acts using fake women’s profiles. *Mirror*. https://www.mirror.co.uk/news/uk-news/cyber-sex-gangs-blackmail-30-9972341 (Accessed on 04/16/2021).

104 Reavy, P. (2019, April 10). Utah family sharing sextortion suicide story likely saved some lives, police say. *Deseret News*. https://www.deseret.com/2019/4/10/20670612/utah-family-

sharing-sextortion-suicide-story-likely-saved-some-lives-police-say#davis-county-sheriffs-detective-john-peirce-works-in-his-office-at-the-davis-county-justice-center-in-farmington-on-monday-april-1-2019-peirce-worked-on-the-tevan-tobler-case (Accessed on 04/16/2021).

105 Cybercrime and Cybersecurity: Trends in Africa. 2016. Symantec/African Union

106 *Insights*. (2020, August 6). Intralinks. https://www.intralinks.com/insights#:%7E:text=Run%20anti%2Dvirus%20software%2C%20and,and%20operating%20system%20%E2%80%94%20updated%20too.

107 Rogers, P. (2019, April 19). *British cybercriminal sentenced for disrupting Liberian telecoms provider*. Intelligent CIO Africa. https://www.intelligentcio.com/africa/2019/01/22/british-cybercriminal-sentenced-for-disrupting-liberian-telecoms-provider/ (Accessed on 1/23/2020).

108 Article 3 of the Ivorian Penal Code states: "Is punished (...), anyone with the intention of cause a situation of terror or to intimidate the population, or to promote a religious political cause or ideological, or to force the
government, organization or institution to initiate an initiative or act according to certain principles, commits or threatens to commit an act that: carries injury to life; cause of violence serious to people; causes serious damage to property, natural resources, to the environment or cultural heritage; put in danger the life of one or more people; creates a serious risk to health or safety of the public or any other party public ; exposes the public to a dangerous, radioactive or novice, a toxic product or an agent microbiological or other agent or toxin organic; interrupts, disrupts, damages, or destroys a system IT or service provision directly linked to an infrastructure of communication, banking and financial, transport systems public or key infrastructure; disrupts the provision of services emergency services such as the police, civil protection and medical services; endangers public safety or national security; creates or is likely to create a crisis situation within populations or insurgency general".

109 Human Rights Voices. UN 101: There is no UN definition of terrorism. http://www.eyeontheun.org/facts.asp?1=1&p=61 (Accessed on 10/14/19).

110 National Institute of Justice (2017). Terrorism. https://www.nij.gov/topics/crime/terrorism/Pages/welcome.aspx (Accessed on 10/12/2019)

111 22 U.S Code Sec 2656f.

112 Terrorism [definition]. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=5407

113 Janine Kremling, Amanda M. Sharp Parker. "Cyberspace, Cybersecurity and Cybercrime." Los Angeles, USA: SAGE Publications Inc. 2017 P. 128.

114 Marjie T. Britz. "Computer Forensics and Cybercrime: An Introduction." Pearson. Third Edition.

115 Grabosky, P. (2015). *Cybercrime (Keynotes Criminology Criminal Justice)* (1st ed.). Oxford University Press.

116 Haggard, S., & Lindsey, J. R. (2015). North Korea and the Sony hack: Exporting instability through Cyberspace. *Asia Pacific Issues from the East-West Center, 117, 1-8*

117 Janine Kremling, Amanda M. Sharp Parker. "Cyberspace, Cybersecurity and Cybercrime." Los Angeles, USA: SAGE Publications Inc. 2017 P. 116.

118 Thomas, D. and Loader, B. (two thousand). Introduction – Cybercrime: Law enforcement, security, and surveillance in the information age. In D. Thomas and B. Loader (eds) Cybercrime: Law enforcement, security, and surveillance in the information age. London: Routledge

119 Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) Crime and the internet. London: Routledge.

120 Majid Yar. The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology 2005; two; 407. http://euc.sagepub.com/cgi/content/abstract/2/4/407 (Accessed on 11/1/19).

121 https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed on 11/05/19).

122 Felson, M. (1998). Crime and everyday life, 2nd edn. Thousand Oaks, CA: Pine Forge Press.

123 Grabosky, P. and Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies.

124 Beavon, D., Brantingham, P. L. and Brantingham, P. J. (1994). The influence of street networks on the patterning of property offenses. In R. V. Clarke (ed.) Crime prevention studies, Vol II, 149–63. New York: Willow Tree Press.

125 Smith, C., McLaughlin, M. and Osborne, K. (1997). Conduct control on Usenet. Journal of Computer-Mediated Communication 2; URL (consulted 13 May 2005): http://www.ascusc.org/jcmc/vol2/issue4/smith.html.

126 Cohen, L. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review 44, 588–608.

127 Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004). Burglary victimization in England and Wales, the Unites States and The Netherlands: A cross-national comparative test of routine activities and lifestyle theories. British Journal of Criminology 44, 66–91.

128 United Nations. (2021). *Côte d'Ivoire Population (2021) - Worldometer*. https://www.worldometers.info/world-population/cote-d-ivoire-population/ (Accessed on 04/20/2021).

129 *Côte d'Ivoire | UNESCO UIS*. (2020). Côte d'Ivoire. http://uis.unesco.org/en/country/ci (Accessed on 04/20/2021).

130 Net Offensive. (2020, July 27). ⇒ Who are the Internet grazers and crooks?https://www.netoffensive.blog/e-reputation/donnees-personnelles/sextorsion/arnaque-webcam/les-brouteurs/ (Accessed on 04/22/2021).

131 N'Guessan, A. (2014, November 28). THE PRACTICE OF CYBERCRIME IN SCHOOLS AND UNIVERSITY IN CÔTE D'IVOIRE. CASE OF PUPILS AND STUDENTS IN THE DISTRICT OF ABIDJAN (pdf) | Paperity. https://paperity.org/p/59114531/la-pratique-de-la-cybercriminalite-en-milieux-scolaire-et-universitaire-de-cote-divoire (Accessed on 04/22/2021).

132 Idriss, F. B. (2017, October 14). Cyber-fraud, the 501 blows of Ivorian grazers. The opposite of FBIYAY. https://visavis.mondoblog.org/cyber-delinquance-les-501-coups-des-brouteurs-ivoiriens/ (Accessed on 04/22/2021).

133 Bogui, J. (2010). Cybercrime, a threat to development: Internet frauds in Côte d'Ivoire. Contemporary Africa, 2 (2), 155-170. https://doi.org/10.3917/afco.234.0155 (Accessed on 04/29/2021).

134 *Flutterwave, PayPal partner to allow African businesses to receive payments*. (2021). Financial Nigeria International Limited. http://www.financialnigeria.com/flutterwave-paypal-partner-to-allow-african-businesses-to-receive-payments-news-2342.html#:%7E:text=Flutterwave%2C%20Nigerian%20and%20U.S.%2Dbased,users%20globally%20through%20Flutterwave's%20platform. (Accessed on 04/29/2021).

135 Mary Aiken, Ciaran Mc Mahon, Ciaran Haughton, Laura O'Neill & Edward O'Carroll (2015): A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online, Contemporary Social Science, DOI: 10.1080/21582041.2015.1117648. http://dx.doi.org/10.1080/21582041.2015.1117648 (Accessed on 11/11/19).

136 https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

137 David S. Wall. Cybercrime and The Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime (Revised Feb. 2011). Criminology, SASS, Durham University, 32 Old Elvet, Durham.

138 Paul, Day. *Cyber Attack*: *The truth about digital crime, cyber warfare, and government snooping.* London, UK: Carlton Publishing Group, 2014.

139 Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems, 6*(1), 1–12. https://doi.org/10.5897/jiis2015.0089 (Accessed on 05/18/21).

140 Irwin, L. (2018, July 16). *Online anonymity has allowed cybercrime to thrive*. IT Governance Blog En. https://www.itgovernance.eu/blog/en/online-anonymity-has-allowed-cyber-crime-to-thrive (Accessed on 05/18/21).

141 GSMA Intelligence. (2019). *The Mobile Economy Sub-Saharan Africa 2019*. https://data.gsmaintelligence.com/research/research/research-2019/the-mobile-economy-sub-saharan-africa-2019

142 Medugno, R. (2014, March 28). *Africa: A New Safe Harbor for Cybercriminals?* Trend Micro, Inc. https://blog.trendmicro.com/africa-a-new-safe-harbor-for-cybercriminals/

143 ISSAfrica.org. (2015, January 20). *The AU's cybercrime response: A positive start, but substantial challenges ahead*. ISS Africa. https://issafrica.org/research/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead

144 Marco, G. (2009) Understanding Cybercrime: A Guide for Developing Countries. Geneva: ITU, p. 84.

145 Rudnick, L. et al. (2015) Towards Cyber Stability: A User-Centred Tool for Policy Makers. Geneva: United Nations Institute for Disarmament Research, p. 7.

146 Trend Micro, & Kharouni, L. (2013). *Africa, a new safe harbor for cybercriminals?* https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf

147 Orji, U. J. (2018, September 17). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? | Orji | Masaryk University Journal of Law and Technology. https://journals.muni.cz/mujlt/article/view/8666/9255

148 See Article 32 AU Convention on Cybersecurity and Personal Data Protection

149 See African Union (2008) Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report. Addis Ababa, Ethiopia: African Union.

150 See *Oliver Tambo Declaration*. (2009, November). https://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf

151 Ball, K. M. (2017). Introductory Note to African Union Convention on Cyber Security and Personal Data Protection. *International Legal Materials, 56*(1), 164–192. https://www.jstor.org/stable/90020562

152 See AU Convention on Cybersecurity and Personal Data Protection. Part I – Objectives.

153 Ball, K. M. (2017). Introductory Note to African Union Convention on Cyber Security and Personal Data Protection.

154 See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art.25. al.2

155 See AU Convention on Cybersecurity and Personal Data Protection. Chapter III.25 al.3.

156 See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art. 28 al.1

157 See AU Convention on Cybersecurity and Personal Data Protection. Chapter III. Art.32.

158 Signé, L., & Signé, K. (2021, April 6). *How African states can improve their cybersecurity*. Brookings. https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/

159 See Art.1 of the Fight against cybercriminality Act (Law No 2013- 451.)

160 See Art. 4 of the Act. (Law No 2013- 451.)

161 See Art. 8 of the Act. (Law No 2013- 451.)

162 See Art. 9 of the Act. (Law No 2013- 451.)

163 See Art. 13 of the Act. (Law No 2013- 451.)

164 *18 U.S. Code § 1029 - Fraud and related activity in connection with access devices*. (2020). LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1029

165 *ngcert | Home*. (2018). Nigeria Cert. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

166 John Mukum Mbaku, *The Rule of Law and the Exploitation of Children in Africa*, 42 Hastings Int'l & Comp. L. Rev. 287 (2019). Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol42/iss2/2

167 Teacher, Law. (November 2013). Patent and Intellectual Property Issues in Africa. Retrieved from https://www.lawteacher.net/free-law-essays/international-law/patent-and-intellectual-property-issues-in-africa-international-law-essay.php?vref=1 .

168 Y. Li, X. Zhang, F. Lu, Q. Zhang, and Y. Wang, "Internet addiction among elementary and middle school students in China: a nationally representative sample study," Cyberpsychology Behav Soc Netw Another, vol. 17, no. 2, pp. 111–116, 2014.

169 S. L. Gencer and M. Koc, "Internet Abuse among Teenagers and Its Relations to Internet Usage Patterns and Demographics," Educ. Technol. Soc., vol. 15, no. 2, pp. 25–36, 2012.

170 https://popia.co.za/

171 Cathy-Eitel Nzume, CIPP/US. *Slowly but surely, data protection regulations expand throughout Africa*. (2021, April). IAPP. https://iapp.org/news/a/slowly-but-surely-data-protection-regulations-expand-throughout-africa/

172 Joao, T. Privacy / Data protection Law: How much disclosure does growth need? Africa 2.0: A brave new (digital) world. Annual Conference, African Bar Association. Port-Harcourt, Nigeria. 2017. https://www.afribar.org/portHarcourt2017/papers/JoaoTracaPaperPrivacyABAfinal.pdf

173 *Data Protection in Africa: A Look at OGP Member Progress*. (2021, August 11). Open Government Partnership. Retrieved 2021, from https://www.opengovpartnership.org/documents/data-protection-in-africa-a-look-at-ogp-member-progress/

174 Protection Authority. (2016). Decision- No.2016-0215- on Authorization of Data Processing by the Company Citibank Cote d'Ivoire P.L.C. Retrieved December 25, 2021, from https://www.artci.ci/images/stories/pdfenglish/decisions_conseil_reg_english/decision_2016_0216_english.pdf

175 *The legal framework principles guiding the handling of personal data in Côte d'Ivoire*. (2019). Oxford Business Group. https://oxfordbusinessgroup.com/analysis/authorised-use-four-principles-guiding-handling-personal-data

176 See Economic Organization of West-African States. (2010). *Supplementary Act on Electronic Transactions within ECOWAS*. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

177 Smedinghoff, Thomas J., The Legal Challenges of Implementing Electronic Transactions (September 28, 2008). Uniform Commercial Code Law Journal, Vol. 41, No. 3, 2008.

178 Varghese, J. (2021). *Ecommerce Security: Importance, Issues & Protection Measures*. https://www.getastra.com/blog/knowledge-base/ecommerce-security/

179 See Article 36, Law No. 2013-456, 30 July 2013.

180 Council of Europe. (2000). *Who we are*? The Council of Europe in Brief. https://www.coe.int/en/web/about-us/who-we-are?l=sq

181 National Research Council (US) Institute for Laboratory Animal Research. The Development of Science-based Guidelines for Laboratory Animal Care: Proceedings of the November 2003

International Workshop. Washington (DC): National Academies Press (US); 2004. The Council of Europe: What Is It? Available from: https://www.ncbi.nlm.nih.gov/books/NBK25399/

182 EU. (2003). *EUR-Lex - 31995L0046 - EN - EUR-Lex*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1995/46/oj

183 Council of Europe. (n.d.). *What are the benefits and impact of the Convention on Cybercrime?* Cybercrime. https://www.coe.int/en/web/cybercrime/home

184 Greenleaf, Graham, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108 (October 19, 2011). International Data Privacy Law, Vol. 2, Issue 2, 2012, UNSW Law Research Paper No. 2011-39, Edinburgh School of Law Research Paper No. 2012/12, Available at SSRN: https://ssrn.com/abstract=1960299

185 *The Budapest Convention on Cybercrime: a framework for capacity building – Global Forum on Cyber Expertise*. (n.d.). Thegfce.Org. Retrieved January 12, 2022, from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/

186 Council of Europe. (2020). *The Budapest Convention on Cybercrime: benefits and impact in practice*. coe.int. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

187 EU, CE, AU Commission. (2021). *Second African Forum on cybercrime to take place on 28 and 29 June online*. https://www.coe.int/en/web/human-rights-rule-of-law/-/second-african-forum-on-cybercrime-to-take-place-on-28-and-29-june-online

188 Deutsche Welle (www.dw.com). (2019). *Abidjan strengthens its system against cybercrime*. DW.COM. https://www.dw.com/fr/la-c%C3%B4te-divoire-renforce-son-dispositif-contre-la-cybercriminalit%C3%A9/a-50706017

189 Wolford, B. (2019, February 13). *What is GDPR, the EU's new data protection law?* GDPR.Eu. Retrieved January 19, 2022, from https://gdpr.eu/what-is-gdpr/

190 UCLA. (2021). *In developing countries, no quick fix for strengthening police–civilian relations*. Newsroom.ucla.edu. https://newsroom.ucla.edu/releases/community-policing-developing-nations

191 *Cyber Crime Investigation: Making a Safer Internet Space*. (2021, September 8). Maryville Online. Retrieved January 19, 2022, from https://online.maryville.edu/blog/cyber-crime-investigation/

192 United Nations Office of Drugs and Crimes-UNODC-. (2014). *About the PLCC-Platform Against Cyber Crimes*. unodc.org. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Cote_DIvoire.pdf

193 Self, B. (2016, March 30). *The Difficulties of Litigating Cyber Crime*. Law Enforcement Cyber Center. Retrieved February 22, 2022, from https://www.iacpcybercenter.org/the-difficulties-of-litigating-cyber-crime/

194 Grimes, R. A. (2016, December 6). *Why it is so hard to prosecute cyber criminals*. CSO Online. Retrieved March 1, 2022, from https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

195 Ehouman, A. (2021, December 22). *Côte d'Ivoire records an estimated 50% resolution rate for cybercrime offenses (Ministry)*. Ivorian Press Agency-AIP. Retrieved March 1, 2022, from https://www.aip.ci/aip-la-cote-divoire-enregistre-un-taux-de-resolution-dinfractions-en-lien-avec-la-cybercriminalite-estime-a-50-ministere/

196 Afp, J. A. A. (2019, April 2). *Côte d'Ivoire: nearly 100 cybercriminals were arrested in 2018*. JeuneAfrique.com. Retrieved March 1, 2022, from https://www.jeuneafrique.com/757600/societe/cote-divoire-pres-de-100-cybercriminels-ont-ete-interpelles-en-2018/

197 Kouade, L. (2017, August 4). *Côte d'Ivoire: fight against cybercrime, the participatory role of Internet users*. Ivoire Intellect. Retrieved March 1, 2022, from https://ivoireintellect.mondoblog.org/cote-divoire-lutte-contre-cybercriminalite-role-participatif-internautes/

198 Pinto, P. (2021, September 8). *The Ivorian government toughens penalties for cybercrime*. RFI. Retrieved March 20, 2022, from https://www.rfi.fr/fr/afrique/20210908-le-gouvernement-ivoirien-durcit-les-peines-en-mati%C3%A8re-de-cybercriminalit%C3%A9 The article:

199 Sample, B. (2020, June 5). *Federal Cyber Crime | Cyber Crime Lawyer | 802–444-4357*. Brandon Sample Attorney. Retrieved March 21, 2022, from https://brandonsample.com/federal-cyber-crimes/

200 Susan W. Brenner & Joseph J. Schwerha IV, Transnational Evidence Gathering and Local Prosecution of International Cybercrime, 20 J. Marshall J. Computer & Info. L. 347 (2002)

201 Granville, J. (2003). The Transnational Dimension of Cyber Crime and Terrorism. By Abraham D. Sofaer and Seymour E. Goodman (Stanford, CA: Hoover Institution Press, 2001, 292 pp. $24.95 pb). *British Journal of Criminology*, *43*(2), 452–453. https://doi.org/10.1093/bjc/43.2.452.

202 Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Tex. L. Rev. 553 (1997-1998) Available at: http://ir.lawnet.fordham.edu/faculty_scholarship/42

203 The FBI in Abidjan to note the arrest of the gang of cyber crooks who have committed frauds of 900 million FCFA. (2013, June 25). Edith Brou Island. Retrieved March 10, 2022, from https://lactuwebdedith.wordpress.com/2013/06/25/le-fbi-a-abidjan-pour-constater-larrestation-du-gang-de-cyberescrocs-auteur-descroqueries-de-pres-de-900-millions-de-fcfa/

204 Ajayi, E. (2016, July 25). *Challenges to enforcement of cyber-crimes laws and policy*. Journal of Internet and Information Systems. Retrieved March 10, 2022, from https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210

205 Maras, M. (2016). *Cybercriminology* (1st ed.). Oxford University Press.

206 K. (2019, March). *Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations*. UNODC.ORG. Retrieved March 12, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html

207 Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.

208 S, S. (2017, August 12). *Difference Between Culture and Society (with Comparison Chart)*. Key Differences. Retrieved March 14, 2022, from https://keydifferences.com/difference-between-culture-and-society.html

209 Weingast, B. (2009, February). *Why are developing countries so resistant to the rule of law?* cadmus.eui.eu. https://cadmus.eui.eu/bitstream/handle/1814/11173/MWP_LS_2009_02.pdf?sequence=1&isAllowed=y

210 L. McKay. (2015). *Toward A Rule of Law Culture. Exploring Effective Responses to Justice and Security Challenges*. usip.org. https://www.usip.org/sites/default/files/Toward-a-Rule-of-Law-Culture_Practical-Guide_0.pdf

211 *Côte d'Ivoire*. (2021). World Bank. Retrieved March 18, 2022, from https://www.worldbank.org/en/country/cotedivoire

212 African Development Bank. (2011). *Income inequality in Africa*. ADB. https://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Revised-Income%20inequality%20in%20Africa_LTS-rev.pdf

213 *In Côte d'Ivoire, pandemic prompts surge in extreme poverty | United Nations Development Programme*. (2020, July 6). [Press release]. https://www.undp.org/press-releases/cote-divoire-pandemic-prompts-surge-extreme-poverty

214 Interpol. (2020, August). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

215 Transparency International. (2020, August 10). *What is corruption?* Transparency.Org. Retrieved March 19, 2022, from https://www.transparency.org/en/what-is-corruption

216 Ojo, J. (2019, August). *Politics of Corruption in Africa*. Global Encyclopedia of Public Administration, Public Policy, and Governance. https://www.researchgate.net/publication/322138202_Politics_of_Corruption_in_Africa

217 Atuobi, S. (2007, December). *Corruption and State Instability in West Africa: An Examination of Policy Options*. reliefweb.int. https://reliefweb.int/sites/reliefweb.int/files/resources/9BD8A1F729CEB5B8C125746C0049D740-kaiptc-dec2007.pdf

218 Momoh, Z. (2015, March). *Corruption and Governance in Africa*. ResearchGate. https://www.researchgate.net/publication/308792420_CORRUPTION_AND_GOVERNANCE_IN_AFRICA

219 Mbaku, J. M. (1996). *Bureaucratic Corruption in Africa: The Futility of Cleanups*. CATO Journal. https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/3186/Vol.pdf?sequence=1&isAllowed