Neo-Economy and Militating Effects of Africa's Profile on Cybercrime

Benjamin Okorie Ajah[1] & Onyejebu Dominic Chukwuemeka[2]
University of Nigeria, Nigeria

Abstract
The neo-economy includes all businesses that wholly exist or make critical use of the internet. They operate in all parts of the world and are very developed in some parts and tender in other parts. In Africa, the neo-economy is likely the best thing that has occurred in the continent since the independence era. The opportunities of this economy in Africa are however drained by the infamous profile of Africa in cybercrime. This article is anchored on the containment theory and adopted secondary sources of data such as journal articles, newspaper publications and policy briefs to discuss how this infamous profile has hindered the successes of businesses in the neo-economy and key actions that could be taken to re-image "Africa equal to cybercrime" profile in the global community. The article recommends the need for African leaders to reach consensuses on meaning of cybercrime, effects, and roles each nation must play to reach an agreed result. Also, parents need to balance euphoria in their children with trainings and preparations for the harsh environments in the real world.

Keywords: Cybercrime, Militating Effects, Millennials, Profile, Neo-Economy.

Introduction

In preliminary conversation with the Queen, moments before a major anti-corruption summit in London, David Cameron pronounced Nigeria and Afghanistan as "fantastically corrupt" (Ajah & Okoro, 2017; BBC, 2016). To significant number of people in Britain, United States, and other developed countries – it is not just Nigeria or Afghanistan that is corrupt, it is all of Africa and most other economically downsized nations in East Europe, South America, and Asia. An average Westerner believes that all Africans are corrupt and fraudulent (Chinweze, Chukwuemeka, & Egbegi, 2019; Nwune, Ajah, Egbegi, &

[1] Lecturer II, Social Sciences Unit, School of General Studies, University of Nigeria, Enugu Campus, Nigeria. Email: okorie.ajah@unn.edu.ng (Corresponding author)
[2] Lecturer II, Social Sciences Unit, School of General Studies, University of Nigeria, Enugu Campus, Nigeria. Email: divinemercy_f@yahoo.com

Onyejegbu, 2019; Conversation, 2017). In a modern global setting where people are more connected than ever in history, this epithet of corruption and fraud spreads swiftly and do not only apply to people jumping queues or giving privileges to cronies, it is mostly pronounced in the domains of fraudulent activities perpetrated through the internet. These kinds of activities constitute what is known as cybercrime.

Cybercrime includes the regular crimes that are widely known, like forgery, cheating, falsification, fraudulent representation of facts or impersonation – only that they are now carried out through the use of computer and internet (Chinweze, Chukwuemeka, & Egbegi, 2019; Abdul-Rasheed Ishowo, Muhammed, & Abdullateef, 2016; Jumoke, 2015). Africa is profoundly labeled corrupt and fraudulent in this regard (Adanikin, 2018). In response to questions at Quora.com on countries with highest number of internet scammers, Pablo Djankowicz specifically mentioned most countries in sub-Saharan Africa as most active in cybercrime in the world (Pablo, 2017). Biko Agozino of Virginia Tech University noted that "there is a long-standing demonization of Nigeria as being full of criminals" (Agozino, 2003). This narrative convincingly applies to not only Nigeria but all of Africa.

What is interesting is that cybercrime is neither a peculiar problem to Africa nor to any specific continent. Every country and continent have straits of cybercriminals and suffers dents of losses in the hands of its citizen-cybercriminals (Adewole, Isiaka, & Olayemi, 2011). The unique appellation of Africa as full of corruption and criminals is however promulgated by the many challenges that face the continent and the emotional dimensions of styles of crimes perpetrated from the region (Adewole, Isiaka, & Olayemi, 2011; Ajayi, 2016). It is important to note that the term "cybercrime" is often used in misleading contexts. While cybercrime includes all forms of criminal activities carried-out through the internet like cyber espionage, cyber stalking, revenge porn, forgery, hacking or stealing of data, Africa is exclusively vested in cyber fraud (Abdul-Rasheed Ishowo, Muhammed, & Abdullateef, 2016). Cyber fraud is a type of cybercrime that involves the use of deception to tout and defraud people on the internet (Jumoke, 2015; AL-Rawashdeh, Abu-Errub, Areiqat, & Dbbaghieh, 2012). It requires less technological skills but sufficient social skills to attract and misdirect victims. According to Al-Shalam (2006), Africa is rather vested in cyber fraud while developed countries in the West are vested in other kinds of cybercrimes like cyber stalking, hacking, revenge porn, and cyber espionage. In the real sense of things, Africa is not the most active continent in cybercrime – China, United States (US), and United Kingdom (UK) have always come before African countries. US Federal Bureau of Investigation (FBI) and its Internet Crime Complaint Center have consistently ranked Nigeria 'third" behind US and UK in cybercrimes (Chinweze, Chukwuemeka, & Egbegi, 2019).

Africa is however more designated as a "continent of cybercriminals" in the public domain than any of the Western or Asian countries (Das & Nayak, 2013). This is so for two reasons; African countries have since suffered at the hands of bad governance and victims of African fraudsters do not only lose their monies, they also suffer from emotional entanglements. First, the impacts of consistent bad leadership across African countries since independence like in the economy and healthcare of African citizens, and the ensuing narratives covering the continent paint to the world "a miserably poor and useless continent where the leaders heartlessly harm and destroy their own people (Ajah &

Okoro, 2017)." With this narrative clouding every mention of Africa to non-Africans, it is easy to conveniently append everything bad to the continent. Second, the primary goal of every African cyber fraudster is financial benefit. They are considerably unsophisticated, keen for quick access to victims' cash, and sometimes even annoying in a unique annoying manner. They fit the narrative of "miserably poor Africa" and often conjecture their own stories of how miserable their lives and homes are – just to convince and misdirect their victims (Ayofe & Irwin, 2010; Bamrara, Singh & Bhatt, 2013).

These "pity-seeking" conjectures often successfully seduce victims and part them with their life-savings. This is always painful because the method does not only lure and harm the emotions of victims – it also costs them savings that took very long to build. Danquah and Longe (2011) noted that because it is easy to attribute everything bad to Africa in addition to the unique emotions and pains associated with methods of cyber fraudsters from Africa, most non-Africans unconsciously consider Africa as most fraudulent of all continents – even when US and UK are evidently ranked higher than any African country.

Africans have reacted to this global attribution of corruption and cybercrime but these reactions have been rather conflicting (Chinweze, Chukwuemeka, & Egbegi, 2019; Danquah & Longe, 2011). After David Cameron's public declaration of Nigeria as "fantastically corrupt," the Nigerian president went on to tell News Channels that he agreed with Cameron and would demand repatriation of funds looted from Nigeria back to Nigeria (Olalekan & Kamarudeen, 2016). Opposition parties in Nigeria vehemently rejected Cameron's assertions and reprimanded the president for espousing such notions (Affe, 2010). The actual confliction in response exuded itself in Nigerians' remarks on social media. Nigerians could not agree on the meanings of Cameron's assertion and their implications for the country. With this failure to reach consensus, the chant of Africa as a continent of corruption and cybercriminals yet endured. These conflictions are proofs that Africans have no consensus on meaning of cybercrime, size of its threats or methods of addressing the threats (Danquah & Longe, 2011). The implications of this inability of Africans to agree on meanings and actions are many – but the graveness of impact is most on the neo-economy.

Many scholars have studied cybercrime in Africa and made valid contributions on impacts and viable rectification measures (Das & Nayak, 2013; Desai & Patel, 2013; Folashade & Abimbola, 2013). What however has not been achieved is a detailed study on how cybercrime affects success of businesses in the neo-economy. This gap is what this paper intends to fill.

The article is divided into four sections. The first section that started with 'Pathology of Crime and Cybercrime in Modern Africa' discusses brief genealogy of crime in Africa, coming of internet, emergence of cybercrime and methodologies of cybercrime across the continent. The second section introduces the neo-economy, its economic successes and opportunities in the continent. The third section discusses 'Impact of Africa's cybercrime profile on neo-economies' and the theoretical framework supporting this study. The fourth and last section discusses strategies to rectify Africa's cybercrime profile and mitigate effects of cybercrime.

1. Pathology of Crime and Cybercrime in Modern Africa

Crimes and criminal tendencies are not novel. People of all ages have experienced their shares of what such social factor entails. In modern Africa however, cyber frauds are unique but are underscored by preexisting foundations set from the old Africa.

1.1. Earlier Africans

They were the first generations. The primitive ones; they lived in small groups in unsophisticated societies where everyone knew everyone and trust was based on this knowledge (Khan Academy, 2019). Crimes like stealing existed but no sophisticated arts like defrauding, impersonation or forgery existed. As time passed, African communities grew. More sophisticated patterns of trade emerged. Egyptian Pharaohs organized large populations, collected taxes, and invented more advanced systems of trade and governance. As at the first points of contact with Europeans, trade systems were still very basic in Africa – and only unsophisticated crimes existed (Lawpadi, 2019; Khan Academy, 2019).

Khan Academy (2019) notes that the coming of Europeans during the colonial era brought changes to Africa in trades, methods and perceptions. The old level of trust still strongly existed in trades but new methods of doing farming and trading were introduced. Seeing how their colonial masters lived, Africans began to imagine new lifestyles for themselves. The battle for resources and favor of their masters ensued, creating divisions within clans and often within families. People switched religious faiths and often value systems (Khan Academy, 2019). Fathers turned on sons and sons turned on fathers. Trading systems changed and general consensus on "right and wrong" changed as well, but criminal methods were still basic. In late periods of colonialism, methods of crime upgraded especially with ascension of few Africans to political positions – but these methods still lacked much sophistication and popularity compare to modern era.

At the early hours of independence, a new Africa emerged. Hopes were high, Africans abroad migrated home to build their homelands and the euphoria was unimaginable. Most countries still lacked strong, educated work force – education was prized and graduates were often begged to take jobs. Africans became the presidents of African countries and finally lived like their colonial masters. This also created a new form of imagination in the minds of most Africans. A belief that everything is now possible; anyone could be anything. Anyone could be the president of Uganda, Kenya or Ghana. People went to schools with their hearts filled with dreams of the future – including a sense of guaranteed future of grandeur. It did work out for many (Khan Academy, 2019). With the huge lack of educated skills in public service and industries, most graduates were quickly absorbed with reasonable salaries. In the course, Africans also learnt sophistication. Educations abroad broadened their views of the world. This was further supported by widespread emergence of universities and other tertiary institutions in Africa. Since jobs were readily available for graduates and many were satisfied with their salaries, crimes were still not as popular as in recent times (Ajah, Nwokeoma & Okpan, 2017). Most criminal activities were only noticeable within ruling elites who carelessly handled states' resources for personal gains

1.2. Millennials and Birth of Cybercrime

Most African countries received independence around 1955 – 1970. As at 1981 – 1997 when the millennials were born, people born during the independence era were the new adults (Folashade & Abimbola, 2013). They were the products of the high hopes and euphoria of independence – the old breeds. Along with their own expectations of the future, they transferred this euphoria to the younger generation, the millennials. Millennials were taught from early age that school education means guaranteed success. Just like the independence generation, they were taught that graduating from school means guaranteed jobs and comfortable lives. According to Ajah and Okoro (2017), young children from poor homes or who faced certain socioeconomic challenges were promised better lives and brighter futures if they managed to learn to read and write. It became a religion, every hardship or mere bad luck experienced by young millennials while growing up were promised to fade away over time – in a better world guaranteed in the future (Ajah & Okoro, 2017; Gercke, 2013).

Mothers taught their sons that everything is possible and they could be anything, even the "president of the world." Most children grew-up imagining a future where they have breakfast in London, lunch in Berlin, and dinner in Washington. It was an era of dreaming and millennials were busy dreaming while the work was not done. Most performed terribly in schools, others had personal cultures that were not pro-productivity. Nonetheless, a new euphoria of "non-encumbrance" grew and this time – fueled by narratives from parents and relatives from the early post-colonial Africa (Gercke, 2013). In every moment of hardship or inconvenience in their families, parents often told their young millennials that they will fix the challenges when they grow up. This created a sense of responsibility to solve their family problems and take-up their parents' roles as soon as they can. These beliefs, euphoria and sense of responsibilities were not matched with work. Young millennials worked less hard than their parents, lived more carelessly, and simply stayed back and dreamt.

At the dawn of the twenty-first century, the dreamed future of millennials had begun. The oldest millennials were 20years old at the time. They were migrating to adulthood. The dreamed futures were not coming to reality (Froggio & Agnew, 2007). An old clique of leaders had already established themselves and a system that makes it difficult for youngsters with little network and funding to near political positions – regardless how creative or thoughtful the youngsters might be. Public service systems were already crowded and private companies were few and had limited spaces for teeming number of school graduates. The reality became direct opposite of what most millennials had imagined (Frank & Odunayo, 2013).

Internet was finding its way into the lifestyles of Africa at the time. As at 1996, Ghana had already secured a permanent internet connection – Nigeria followed in 1997. It was a new system that had the potentials to connect the world. It was costly at first but consistent improvements and competition lowered the prices. Right now, anyone could own a gadget and internet connection for as low as US$100 or less (Chinweze, Chukwuemeka, & Egbegi, 2019). Bringing the world to one "public auditorium" called internet has as much complications as it does have opportunities and benefits. Despite the spate of bad leadership in the continent, the dawn of twenty-first century came with news of democracy and demise of military dictatorship. Some westerners saw the opportunities

for investments in new business systems in this new Africa like purchase of properties, purchase of oil wells and promotion of existing solutions. Most leveraged the internet, which is the most cost-effective means to discover and learn about distant locations. The smart and often educated millennials whose "imagined futures" have been shattered by ceiling realities saw Western interests in investments as ways to make quick money and realize their dreams by selling falsehood to the foreigners who sought real business opportunities (Ajah & Okoro, 2017).

It quickly established as a pattern, young millennials started seeking and contacting foreigners on the internet with "false" business opportunities in calculated efforts to defraud them – and cyber fraud began. Because governance in African countries increasingly failed to institute accepted laws and systems that enabled millennials to work and achieve their dreams, cyber fraud that was started by a handful of people grew to hundreds of thousands and millions of people - and it gradually became a reality that 'Africa equals cyber fraud.'

1.3. The Internet and Cyber Crime

No one knows exactly when and for what purpose internet was created. Certainly, it was created in United States at the supervision of the military (Ian, 2004). Internet has become the single most connected and important information sharing facility in the world. A PR perspective would probably brandish that internet was created to link the world. It has globalized cultures and innovations, and enabled old and new businesses to succeed exceedingly through data management, information sharing and enhanced decision-making processes.

The Internet is a network made-up of many computers and smart devices for easy movement of data from one device to another (Ibikunle, 2005). Different people have perceived and reacted to the creation of internet based on their different interests and how it best serves them. Security agencies have mounted surveillance and other security apparatus through the internet. Businesses have integrated their processes for efficient data storage and easier access to information for decision making (Ibrahim, 2016). Most businesses also reach their customers through the internet. The biggest benefit of the internet in twenty-first century is that everyone is now connected with everyone.

Imhof (2010) maintained that criminals and common fraudsters have also leveraged the internet in searching and misdirecting their victims, hence cybercrime. Cybercrime includes all forms of crimes perpetrated through the use of computer and internet. Crime is not new, it is cybercrime that is new (Abdul-Rasheed Ishowo, Muhammed & Abdullateef, 2016). The emergence of internet demanded and established new forms of social behaviors that had no existence before the internet. People used to express themselves in face-to-face interactions or simply write, but same results could now be achieved with a phone call between two people that are far apart (Innovative Dynamic Networks (IND), 2016). A new form of habit and social paradigm that enables people to achieve same conversational effects as in real-time face-to-face interactions on the phone evolved. Crime also evolved with new methods and social paradigms that enabled it to settle and thrive on the internet.

2. Methodologies of Cybercrime in Africa

A certain social paradigm always takes effect when huge changes occur that disrupt existing systemic models like changes from socialism to capitalism or dictatorship to democracy. Same paradigm occasionally happens with leadership changes as well (International Cyber Security Protection Alliance (ICSPA), 2016). It occurred in 1776 after America's independence when slaves and free men comprising artists, carpenters and all kinds of talents migrated from all-around the world to America. It occurred in Europe after the formation of Eurozone and hundreds of foreign companies stormed the continent hoping to leverage the opportunities of a single large market (International Telecommunication Union (ITU), 2009). In early twenty-first century, it occurred in Africa – for the second time, the first being the independence euphoria. The early 2000s brought a new Africa where most African countries were just migrating from military dictatorships to modern democracies. This wave, which is common with such social paradigms, invited much euphoria on new kinds of opportunities in Africa (Jackson & Robert, 2016). Throughout the late hours of 20th century and first decade of 21st century, the world looked to Africa for new opportunities expected of the changing social paradigms. The penetration of internet through the continent created new ways of seeking these opportunities. It was at this time that local fraudsters embraced the opportunity of the internet to go global and created a new version of fraud called cyber fraud (Jaishankar, 2007).

According to Jansen and Leukfeldt (2016) cyber fraud includes all use of falsehood on the internet to gain a dishonest advantage. It is a type of cybercrime and is less diverse than cybercrime. Cybercrime includes all forms of criminal activities carried out on the internet. This includes hacking, cyber espionage, SIM swap, cyber fraud, and many more. Africa is most vested in cyber fraud. More sophisticated cybercrime activities also exist in Africa especially cyber-hacking of all sorts. In 2017, 50 graduating students from Makerere University Uganda were removed from graduating list in accusation of hacking into the University's system to change their grades (Abdi, 2016).

The bank systems are also often hit through direct hacking, malware planting, and many other more sophisticated means. Experts have estimated that over 80% of personal computers in Africa are infected with viruses and other malicious software that aid hacking and data loss. There are also rumors of a very gigantic network of malware-infested laptops called "botnet" that has the capacity to take down the whole internet (Franz-Stefan, 2010). Some of these sophisticated methods of cybercrime are manufactured and carried out in Africa while some are manufactured outside the continent but used in Africa – nonetheless, they all threaten African and global cyber security from Africa. It is important to know that this paper addresses how the epithet of Africa as home of cybercriminals and fraudsters has affected the success of the neo-economy in Africa – and it is not intended to address all spheres of cybercrime like the more sophisticated methods of cybercrime. This is because every modern nation faces the challenge of cybercrime and have them manufactured and used locally, but not all nations have such renowned epithet of cyber fraudsters like African nations. This unique personality in cyber fraud is what this paper address.

Methodologies of cyber fraud have evolved over time to match the changing social narratives between Africa and Africans and Africa and the rest of the world. In the early

2000s, Africa was newly opened to the world and both businesses and individuals scouted for big opportunities in the continent. Because the Western and European businesses thrived on trust and agreements, foreigners from both regions easily placed faith in dealing with business opportunities from Africa (Chinweze, Chukwuemeka, & Egbegi, 2019). At the time, the model of cyber fraud was to forge documents and sell hypothetical or fake products to foreigners through the internet. They would search, study and send messages to target victims, bearing news of "unique" opportunities to buy items or make investments with guaranteed profits (Prince, 2019). Some of these messages are often too good to be true or so fashionably constituted that red flags are hard to detect. For instance, contacted for purchase of bullions of gold which turned out to be fake, buyers reported receiving emails like;

> "I am Kwassi Mensah from the family of his royal highness NANA APAI MENSAH of the Ashanti Kingdom in Ghana. As part of our royalty, we, the royal family is entitle to some % of the total gold mined in the Ashanti kingdom, in view of this, we have in stock 280kg of a Alluvial Gold Dust 22 Karats, we are looking for a serious buyer" (David, 2012).

Or like this;

> "We are group of miners located in Africa presently in tarkwa Ghana. We are the best in local mining in the history of mining in Ghana, we can supply up to 100kg per month, and we do CIF with no upfront payments needed by our LMO which is the local mining organization, all transaction to be closed via our UK Partners" (David, 2012).
>
> "Alliance Brokers UK or GMM "Ghana ministry of Mines. Our AU is noted for its prolific purity of 96.7%- 98.9% Purity and can be refined up to 23 carat plus, 100% POP of merchandise will be provided to seller while buyer provides POF and transaction to be closed via Alliance Brokers. We are ready to work with any mandate/Broker with a qualified certified Buyer with legal rights to Buy AU gold from Ghana/Africa." (David, 2012:).

Such seemingly genuine business opportunities go on to become scams to steal and defraud people. For people that lack adequate knowledge of Africa, this method often works. This can be considered to be an 'Investment Opportunity' method.

After a while, the scammers resorted to a complicated begging approach. In this method, they always approached as victims of some injustice or illness and hold huge opportunities of money or love if helped. An instance is a recent email I received from one Mrs. Marianne Jeanne. She writes …

> "My Greetings
> I am Mrs. Marianne Jeanne; I have decided to donate what I have to you /Churches/ Motherless babies/Less privileged/Widows' because I am dying and diagnosed for cancer for about 2 years ago. I have been touched by God Almighty to donate from what I have inherited from my late husband to you for good work

> of God Almighty. I have asked Almighty God to forgive me and believe he has, because he is a Merciful God I will be going in for an operation surgery soon.
>
> I decided to will/donate the sum of (€ 8.5 million Euros) to you for the good work of God Almighty, and also to help the motherless and less privilege and also forth assistance of the widows. At the moment I cannot take any telephone calls right now due to the fact that my relatives (that have squandered the funds gave them for this purpose before) are around me and my health status also. I have adjusted my will and my lawyer is aware.
>
> I wish you all the best and May the good Lord bless you abundantly, and please use the funds judiciously and always extend the good work to others. As soon as you get back to me, I shall give you info on what I need from you, then you will contact the bank and tell them I have willed those properties to you by quoting my personal file routing and account information. And I have also notified the bank that I am willing that properties to you for a good, effective and prudent work. I know I don't know you but I have been directed to do this by God Almighty.
>
> I Have all my Hospital document which i can send to you as prove to what am tell you and my seriousness to this.
>
> Reply to my private E-mail address (mariannejeanne849@gmail.com)
>
> If you are interested in carrying out this task, get back to me for more details on this noble project of mine.
>
> Yours Faithfully,
> Mrs. Marianne Jeanne."

In most cases, these requests seem so convincing that "soft-minded" people become convinced and fall victim. This method can be considered as 'Pity-Seeking' method.

Another model that has been massively used involves fabricated love narratives paraded on social media and dating sites. This approach has mostly affected women in the ranges of +50years old. In a particular case, Maria Grette, a 62-year-old Swede was approached and cajoled into love by a 58-year-old Danish man named Johnny who lived in England (BBC News, 2016). Maria was lonely and narrated Johnny as a man with a unique sense of romance more than she has ever experienced in any man. In the course of their relationship, Maria was emotionally cajoled to transfer thousands of dollars to Johnny to help treat his son's sickness. This would have been a perfect love story - only that Johnny was actually a 24-year-old Nigerian who graduated without a job. Maria lost considerable amount of money to the boy and only abated after she has lost enough amount of money that awoke her suspicion. This 'Love Affair' method affects even the most intelligent people.

These constitute cyber fraud and have established a narrative for Africa among natives of other continents. These constructs that utilize the looks of truth and emotional entanglements - love, pity – all came together to uniquely position Africa at the center of cybercrime in public domain even when other continents actually lead in cybercrime

activities. It is as though Africans are all criminals, fraudsters, and shameless internet scammers.

3. The Neo-Economy

Primeval economies in Africa were based on subsistence farming. During their time, people also exchanged goods for goods and practiced diverse methods of basic trading. Upon contact with the Indians, Arabs, and Europeans, trades and trading systems became more sophisticated – but still involved physical exchange of goods with money. Colonialism further opened Africa to the world. During which Europeans toured the continent and left no economic potential stone unturned. Specialties were discovered – cocoa for Ghana, groundnut for Nigeria, rubber for Congo, and specific produce or crops for certain countries (Ajah & Okoro, 2017). Africans were taught how to sign contracts, make partnerships, setup businesses, govern, and do many things that made trading more sophisticated and efficient. African economies became dependent on agriculture and trade of agricultural products. At the twilight of colonialism and reign of independence, natural resources like Gold, Crude Oil, Diamond, and others came to limelight. This added more products to trading and further diversified African economies into agriculture, trading, and natural resources (Sahara Reporters, 2018). The advent of the internet only brought new systems for trading, communication and information sharing. These new systems quickly became industries of their own. They form the neo-economies.

3.1. Economic Success of the Neo-Economies

While Africa experienced economic evolutions, other regions witnessed same growth particularly in America, Europe, and Asia. These regions had the original epiphanies and led the changes in neo-economies. As at the time Ghana struggled to secure first permanent internet connection in Africa in 1995, Americans were already shopping on Amazon and internet in China was already established that the Chinese started shopping online 4yrs later. All the businesses or economic activities that exist solely on the internet or have internet/related technologies at its core operations make up the new economy. This includes businesses like Amazon, Alibaba, Microsoft, Facebook, Instagram, Jumia, and others.

These neo-economy businesses have achieved profound successes more than is possible with simple trade. For Africa, they have improved conditions of living in healthcare, shelter, finance, farming, and education. With companies like LifeBank, Prediagn or Medsaf – Africans are guaranteed of ubiquitous access to blood, clinical record, and total elimination of fake drugs. These are challenges in healthcare system that most African governments have battled without success. The neo-economy has also shown to grow faster and create new jobs for Africans unlike traditional businesses. Cellulant, a Kenyan FinTech company founded in 2004 grew from zero employees to over 321 employees as in 2017 (Cellulant, 2018). Yoco, a South African company founded in 2015 grew from zero to 114 employees in 4yrs (Yoco, 2018). The neo-economy has also greased governments' tax coffers and contributed hugely to infrastructural development and net GDP of African countries. Most importantly – it gives young millennials a new chance, an opportunity for them to gainfully employ creativity in solving societal problems and achieve the unlimited possibilities they earlier imagined.

3.2. Opportunities in the New Economy

The biggest opportunity in the neo-economy is the chance to improve lives and conditions of living in Africa. These improvements will manifest in better health technologies and recipes, new methods of sheltering, creation of new jobs, enhancement of governance systems, establishment and maintenance of infrastructures, and profound proliferation in innovations and decrease in crime – including cybercrime (Onwuama, Ajah, Asadu, Ebimgbo, Odi & Okpara, 2019).

It is undoubtedly possible for the neo-economies to elevate living conditions in Africa to the standards of Europe or North America – and strike a socioeconomic balance in world order. Maximizing the opportunities of the neo-economies can come from trust and acceptance, support and encouragement, financial investments, and growth of an informed or tech-savvy public.

3.3. How Africa's Cybercrime Profile Affects Success of the Neo-Economy

Two foundational things companies and businesses of the neo-economy require to innovate, survive, and grow are trust and financial investments. Trust connotes a high-level confidence that these businesses and companies can be truthful, useful, and should be given trials to prove their relevance (Timothy, 2018). This trust is expected of customers and partners. With trust from African users in the market, neo-economy businesses can reach their target users at ease, help solve users' pain-points and generate revenues to scale the businesses (Tan, 2009). But when trust is exculpated, target users consider the businesses to be fraudulent by default. Then stay away from such businesses and stick to old manual processes – even when the neo-economy businesses offer better values to them. In such scenarios, neo-economy businesses find it hard to sell, scale or even survive. The businesses eventually die-off and great opportunities become lost.

Another key need of neo-economy business is financial investments. New economy businesses are highly scalable and must scale to survive in global competition. Most often than not, the businesses do not have sufficient funding to scale and meet their targets – and would need external financial partners to invest and help them build (Timothy, 2018; Ajah & Okoro, 2017). At the current state of development, African countries have very few citizens who understand the neo-economy and have funds to invest in them. The greatest numbers of people that understand the neo-economy are outside Africa. They live, work and hold citizenships in Europe, Asia, and North America. These are the people that have also grown to believe Africa as home of criminals and cyber fraudsters. They consider every African as poor, criminal-minded and cyber fraudster by default. This epithet of fraudsters and criminals have made it extremely difficult for businesses in the new economy to raise the funds required to innovate, survive and fully embrace market opportunities.

The biggest consequences of Africa's huge profile in cyber fraud are these lacks of trust and support required from local African markets for neo-economy businesses to succeed – and the extreme reluctance of foreign investors to trust and invest in African neo-economy businesses due to belief that all opportunities or businesses from Africa are fraud (Chinweze, Chukwuemeka, & Egbegi, 2019).

Key result of these is that Africa loses the opportunities of the neo-economy era while same economy makes peoples' lives better and thrive in other regions of the world. A

result that will trigger cataclysmic levels of capital flight from Africa, massive migration problems to Europe or North America, widespread poverty and diseases in Africa, and a vicious cycle of crime across the continent.

3.4. Theoretical Framework: Containment theory

Containment theory was developed by Walter Reckless in 1961. This theory suggests that individuals are pushed and pulled into crime. Pushes are elements that pressure individuals to engage in delinquency while pulls draw individuals away from accepted forms of behavior. The theory states that pushes and pulls are buffered by inner and outer containments. The inner containment includes self-concept, goal orientation, frustration tolerance, and norm commitment and retention (i.e. elements within the individual's self). The outer containment includes social environment in which the individual resides and reflects socialization within the community (i.e. elements outside one's self) (Cardwell, 2013).

Containment theory asserts that there is an ordering to these elements, with factors of inner containment being developed to address the onset of deviant pushes and factors of outer containment serving as secondary reinforcement mechanisms and buffers against deviant pulls. According to Reckless, we should expect to see factors of inner containment exhibit a strong and primary influence on decision making over the factors of outer containment (Kennedy, 2015).

A situation that may push an individual towards a deviant act is one in which the individual feels some type of pressure to engage in order to escape or improve their current situation (Lilly, Cullen & Ball, 2007). As the individual is self-interested, the presence of the negative situation is pushing them toward a socially undesirable act because they see this act as a way to alleviate their current pain. The only thing keeping the individual from engaging in the undesirable behavior is the presence of strong factors of inner or outer containments (Kennedy, 2015).

In this context, most African millennials are pushed to cyber fraud by the failures of their imagined futures to come true as they had imagined. These failures make them seek alternatives to bring their dreams to reality and mostly resort to cyber fraud as a quick, but desperate means. The millennials are also pulled to cyber fraud by lack of societal laws and systems that allow them to express their creativities and get rewarded for doing so. This is seen in how tight the leadership cults in African countries are, allowing only a handful of people into leadership positions and keeping the young and innovative millennials out of leadership systems. With increasing popularity of Africa's personality in cyber fraud, a new pull is created that affects the neo-economy and likely the future of Africa. This new pull builds a vicious cycle of cybercrime in Africa by targeting the foundation of modern economies in Africa – the neo-economy.

4. How to Placate African Cyber Fraud Narratives

Of all the factors that render Africa incapable of repairing its global profile on cyber fraud, the inability of African leaders to agree on most things has had the most impact. Ensuring security of internet users is never effective with lone-ranger cyber-security efforts. It demands understanding, consensus, and both political and socioeconomic arrangements between nations to be largely effective. Africa lacks this consensus, a kind of

understanding and agreement on meanings, scopes, and defined roles of individual nations in ensuring collective safety of internet users. This kind of arrangement is not similar to the usual random police arrests, reactive legislations or unconnected internet protocols. There is a need for broader, continental strategy where every arrest, legislation, media education, and internet protocol within every nation is part of this larger strategy and achieves predetermined goals for the individual nation and for Africa as a continent. These consensuses have to exist for Africans to take collective approach and have a chance in changing the fraudulent narratives of Africans in public domain.

Parents need not stop giving their children the feelings of limitless possibilities, but the children also need to be taught that realizations of perfect lives are often difficult or delayed. That people can graduate from schools, stay years without jobs or even have difficulties to feed. That bad governance might reign and the citizens would need to endure, act to elect/institute better governance. They need to know and be prepared for the realities of the harsh world. By balancing the information that cultivates euphoria in millennials with preparation for harsh realities, African youths will be better prepared to embrace the future and be less engaged in cyber fraud.

Conclusion

The internet has brought the world to one "public hall," a place where everyone is connected to everyone. This is the foundation of the future and most businesses have already taken every element of their existence to the internet. These businesses constitute a new form of economy called the neo-economy. The neo-economy proves to benefit humanity greatly especially in making human lives better. In Africa, the neo-economy is young and will not succeed if financial investors from developed countries in Europe, Asia, and North America do not embrace business opportunities and invest their money in Africa's neo-economy. This reluctance to invest was created by Africa's infamous profile in cyber fraud. This paper studied the pathology of crime and cyber fraud in Africa – and found euphoria planted in millennials by post-independence Africans and lack of generally accepted laws and systems as main causes of cyber fraud in the continent.

To salvage Africa's fraudulent profile in the global community, African leaders need to reach consensuses on meaning of cyber fraud, effects and roles each nation must play to reach an agreed goal. Parents need to also balance euphoria in their children with trainings and preparations for the harsh environments in the real world.

Conclusively, Africa is neither a country nor equal to cyber fraud; it is a continent with good people and genuine business opportunities that require considerable due diligence, just like every other business opportunity in every other continent. Africa houses thousands of technological companies in the neo-economy and these companies are open for investment.

References

Abdi, L. F. (2018). *Cybercrime is costing Africa's businesses billions.* Quartz News. Retrieved from https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions.

Abdul-Rasheed Ishowo, S. L., Muhammed, L. A. & Abdullateef, Y. R. (2016). Cybercrime and Nigeria's external image: A critical assessment. *Africology: The Journal of Pan African Studies*, *9*(6), 119-132.

Adanikin, O. (2018, May 3). Cybercrooks attempt to steal $3.9m from maritime sector. The Nations Newspaper, Thursday, pp 12.

Adewole, K. S., Isiaka, R. M. & Olayemi, R. T. (2011). An inquiry into the awareness level of cyber security policy and measures in Nigeria. *Journal of Science and Advanced Technology, 1*(7), 91-96.

Affe, M. (2010, June 15). Online shopping portal decries prevalence of internet fraud. *The Punch Newspaper*, Tue, pp. 25.

Ajah, B. O., & Okoro, I. T. (2017). Diagnosis and Prognosis of the Nigerian Recession. IOSR Journal of Humanities and Social Science, *22*(8), 41-48

Ajah, B. O., Nwokeoma, B. N. & Okpan, S. O. (2017). Socio-Economic Implication of Kidnapping and Hostage Taking in Southern Nigeria. *Journal of Law and Judicial System, 6*(2), 51-59.

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

AL-Rawashdeh, B. S., Abu-Errub, A. M., Areiqat, A.Y. & Dbbaghieh, M. (2012). Information technology role in reducing e-banking services risk in Jordanian banking sector. *Journal of Computer Science, 8*(3), 374-381.

Al-Shalam, A. (2006). *Cyber crime fear and victimization: An analysis of a national survey*. Ph.D dissertation submitted to Mississippi State University.

Ayofe, A. N., & Irwin, B. (2010). Cyber security: Challenges and the way forward. *GESJ: Computer Science and Telecommunications, 6*(29), 56-69.

Bamrara, A., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. *International Journal of Cyber Criminology, 7*(1), 49–61

BBC News. (2016). *I went to Nigeria to meet the man who scammed me.* Retrieved from https://www.bbc.com/news/world-africa-37632259,

BBC News. (2016). *Is Nigeria 'fantastically corrupt', as Cameron claims?.* Retrieved from https://www.bbc.com/news/av/uk-politics-36263809/is-nigeria-fantastically-corrupt-as-cameron-claims.

Biko, A. (2003*). Counter-Colonial Criminology: A Critique of Imperialist Reason.* Retrieved from https://www.press.uchicago.edu/ucp/books/book/distributed/C/bo21637229.html.

Cardwell, S. M. (2013). *Reckless reevaluated: containment theory and its ability to explain desistance among serious adolescent offender.* A thesis submitted to the graduate faculty of The University of Alabama at Birmingham, in partial fulfillment of the requirements for the degree of Master of Science in Criminal Justice.

Cellulant. (2018). *About Us*. Retrieved from: https://www.linkedin.com/company/cellulant/?originalSubdomain=ng.

Chinweze, U. C., Chukwuemeka, O. D., Egbegi, F. R. (2019). An exploratory study of cybercrime in the contemporary Nigeria value system. *European Journal of Social Sciences Studies*, *4*(3), 131 -141.

Conversation. (2017). *The view that '419' makes Nigeria a global cybercrime player is misplaced.* Retrieved from https://theconversation.com/the-view-that-419-makes-nigeria-a-global-cybercrime-player-is-misplaced-73791.

Danquah, P., & Longe, O. B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact, 11*(3),169-182.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies.* 6(2), 142-153.

David, L. (2012). *How to avoid being caught in a common gold scam*. Retrieved from: http://www.mining.com/how-to-avoid-being-caught-in-a-common-gold-scam/

Desai, P. N., & Patel, A. M. (2013). Cyber crime against person. *International Journal of Innovations in Engineering and Technology*, *2*(3), 198-201.

Folashade B. O. & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98- 114.

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in science, engineering and education, 1*(1), 1-11

Franz-Stefan, G. (2010). *Africa's Cyber WMD*. Foreign Policy. Retrieved from https://foreignpolicy.com/2010/03/24/africas-cyber-wmd.

Froggio, G. & Agnew, R. (2007). The relationship between crime and objective versus subjective strains. *Journal of Criminal Justice*, *35*, 81-87.

Gercke, M. (2013). Training on cybercrime and discussion of the draft bill, special training on cybercrime. 2nd Workshop on Transposition of SADC Cyber security. Model Laws in National Laws for Namibia Windhoek, Namibia. Retrieved from http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/Special%20Training%20on%20Cybercrime%20%281%29.pdf.

Ian, P. (2004). *The beginnings of the Internet. Net History*. Retrieved from http://www.nethistory.info/History%20of%20the%20Internet/beginnings.html.

Ibikunle, A. (2005). *Investigation of computer crime in information technology industry*. (Unpublished Master's Thesis). Ladoke Akintola University of Technology, Ogbomoso, Oyo State.

Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. In: *Cybercrime and computer forensic (ICCCF),* IEEE International Conference on (pp. 1-9). Vancouver: IEEE.

Imhof (2010). *Cybercrime and telecommunication law*. Rochester Institute of Technology USA.

Innovative Dynamic Networks (IND) (2016). United Nations' definition of cybercrime. Accessed online from: Retrieved from *https://idn-wi.com/united-nations-definition-cybercrime.*

International Cyber Security Protection Alliance (ICSPA) (2016). The International Cyber Security Protection Alliance (ICSPA). A study on the impact of cybercrime on businesses in Canada. Online available at: *www.icspa.org*

International Telecommunication Union (ITU), (2009). *Understanding cybercrime: A guide for developing countries.* Switzerland. ITU publication

Jackson T. C. B. J. & Robert W. E. (2016). Cybercrime and the challenges of socio-economic development in Nigeria. *JORIND, 14*(2), 42-49.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6.

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A Qualitative Analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91.

Jumoke, A. L. (2015, March 5). SMEs hardest hit by cybercrime, as 60% of Nigerian businesses suffer attacks. *Business Day Report*, P3.

Kennedy, J. P. (2015*). Losing control: a test of containment theory and ethical decision making. International Journal of Criminal Justice Sciences*, *10*(1), 48-64.

Khan Academy. (2019). Organizing Paleothic Societies. Retrieved from https://www.khanacademy.org/humanities/world-history/world-history-beginnings/origin-humans-early-societies/v/organizing-paleolithic-societies-video.

Khan Academy. (2019). Peopling the Earth. Retrieved from https://www.khanacademy.org/humanities/world-history/world-history-beginnings/origin-humans-early-societies/v/peopling-the-earth.

Lawpadi. (2019). 10 things to know about Nigeria's cybercrime act 2015. Retrieved from https://lawpadi.com/10-things-to-know-about-nigerias-cybercrime-act-2015.

Lilly, R., Cullen, F. T., & Ball, R. A. (2007). *Criminological theory: context and consequences* (4th ed.). Thousand Oaks, CA: Sage.

Nwune, E. C., Ajah, B. O., Egbegi, F. R., & Onyejegbu, D. C. (2019). Across the Wall: the Perception of Rehabilitation, Reformation and Reintegration Programmes in Anambra State Prison Command. *Journal of Law and Judicial System*, *2*(2), 13-22.

Olalekan, A., & Kamarudeen, O. (2016). *Buhari agrees with Cameron that Nigeria is 'fantastically corrupt'.* Punch News. Retrieved from https://punchng.com/buhari-agrees-cameron-nigeria-fantastically-corrupt-2.

Onwuama, K. C., Ajah, B. O., Asadu, N., Ebimgbo, S. O., Odii, A., & Okpara, O. P. (2019). Public perception of police performance in crimes control in Anambra State of Nigeria. *African Journal of Law and Criminology*, *9*(1), 17-26.

Pablo, D. R. (2017). *Which country has the most scammers?*. Quora News. Retrieved from https://www.quora.com/Which-country-has-the-most-scammers.

Prince, O. (2019, 3rd April). Cyber attack: 60% of Nigerian businesses attacked in 2018. *Vanguard Newspaper,* p51.

Sahara reporters (2018). Nigeria overtakes India as country with highest number of extremely poor people in the world. Sahara News. Retrieved from

http://saharareporters.com/2018/06/25/nigeria-overtakes-india-country-highest-number-extremely-poor-people-world.

Tan, W, K. (2009). What does Locke Mean by "Trust," and Why is it so Important to him? Retrieved from https://www.e-ir.info/2009/12/02/what-does-locke-mean-by-%E2%80%9Ctrust%E2%80%9D-and-why-is-it-so-important-to-him.

Timothy, O. (2018). Nigeria Struggles Against Unemployment, Extreme Poverty. VOA News. Retrieved from https://www.voanews.com/a/nigeria-struggles-against-unemployment-extreme-poverty/4684351.html

Yoco. (2018). *Company Details*. Retrieved from https://www.linkedin.com/company/yoco/?originalSubdomain=ng.