ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Cyber-Security in Nigeria. *A Case Study of Surveillance and Prevention of Digital Crime by Lorliam*. A Review beyond Mere Digital Surveillance

James Chike Nwankwo

Professor, Department of Statistics Nnamdi Azikiwe University, Awka, Nigeria

ABSTRACT

This article explores the technological sophistication associated with cyber related crimes and how it has significantly raked in trillions for the actors involved. This is a review of Lorliam's stance on digital surveillance software. Comparative arguments are presented as to the Nigerian, African, US and European postulations as to these cyber related crimes. Statistics shows the shift in cyber-attack trends from the usual spamming to the use of ransomewares and cloud. This article entails a presentation of new perspectives to cyber-crime activities and argues in favor of its recognition as a stand-alone economy with state actors as supports.

***Corresponding author**

James Chike Nwankwo, Professor, Department of Statistics Nnamdi Azikiwe University, Awka, Nigeria. E-mail: jamescul36@gmail.com

Received: July 21, 2022; **Accepted:** August 11, 2022; **Published:** August 19, 2022

Introduction

With the seemingly rise in cyber related crimes in Nigeria, it might be necessary to examine the true motivation behind the perpetration of cyber-crimes against individuals and corporate bodies.Lorliam's stance cites the critical need to implement sophisticated digital surveillance software in order to help law enforcement agencies in Nigeria detect and prevent cyber related crimes. But, considering the various collaborators and communal actors who are deeply rooted in not just the force but also in government, can Lorliam's postulation be the right move against all odds? Although, it is agreeable that the Nigerian cyberspace needs close monitoring and a high level of reactiveness, the reluctance and complacent attitudes of the agencies involved are sabotaging any significant lead. Lorliam further proposes an independent technological infrastructure that can counter the increase in cyber-criminal activities. The structure proposed according to Lorliam should include a roadmap surveillance that caters for passive and active forensic investigations. Passive in the sense that investigative procedures should be followed duly in the event of a cyber-activity occurrence and active in the sense of getting through to cyber-crime perpetrators in real time. While these are quite logical assertions which are not different from what other scholars have clamoured for, it may be time to import a different perspective in order to win the war against cyber-crime in Nigeria.

Other studies have been conducted as regards the financial and economic downturn of cyber-crimes, the increase in sophistication of cyber-threats [2]; on increased globalized threat of ransomeware CISA [3]; the increasing sophistication of cyber-attacks means stronger strategies are needed in financial organizations, Platt [5]; curtailing cyber-attacks in Africa, Ajao [1], it is logical to hypothesize that the increase in cyber-crimes may not just be as a result of sophistication or usual compromise which is visible in countries where corruption thrives. Most especially, with the presence of not just non-state actors but state actors who are benefactors. For instance, reports shared by Hanafi [6], emphasizes how fraudulent persons in Nigeria bribe both the police and soldiers in order to evade arrest. This report is validated by Oludare [7] who specifically notes that the Economic and Financial Crimes Commission (EFCC) which was set up to tackle crimes related to corruption and cyber are at the fore of bribery. This is a clear case of compromise and complacency because these beneficiaries appear to be comfortable with the status quo so far the bribery is steady. But from a more intense assessment, there could be existence of more than the normal compromise or sophistication that causes an increase in cyber-crime perpetration. Hence, the ultimate goal of this essay is to cite Lorliam's approach as secondary and provide a different perspective through which Lorliam's approach can become effective when applied. In addition, this review provides most suitable explanation with respect to the increase in cyber-crimes especially in a developing country like Nigeria where poverty and recession is a dire call to multiple streams of revenue for cash flow.

Cyber Related Crimes in Africa

There is no doubt that the cyber related crimes has been on the increase in Africa. Especially when the standard of living is seemingly increasing. In South Africa alone, it is estimated on business tech in 2021 that there are 230 million threats in total. This is not so surprising considering the discovery made by Interpol as documented by on Business tech in 2021. This discovery explains that South Africa losses R2.2 billion yearly. This same report is

validated by Dolley [8] where it claims that South Africa has become increasingly vulnerable to ransomeware attacks.

The top five threats identified in South Africa are, online scam, digital extortion, business email compromise, ransomeware, botnets. Amongst these threats, the business email compromise appears to be quite popular in Africa. The likes of Hushpuppi and Invictus were arrested based on scams that involved this sort of threat. But that is not to say that others are not as popular as well. In recent times, Nigeria has witnessed a high rate of online scam [9]. It was observed that during the pandemic, internet fraudsters went on a scamming spree to dislodge unsuspecting individuals and corporate entities. The International Criminal Police Organisation (INTERPOL) was said to have thwarted a $1.6 million face masks scam [9]. This fraudulent activity involved Germany, Ireland and the Netherlands. More importantly is that the transferred amount of about $544,000 meant for the procurement of the essential medical items was traced to Nigeria [9].

However, countries like Ghana are not left out of this as in 2016; their financial institutions were noted to have encountered more than 400,000 incidents with respect to malware, 44 million linked to spam emails and 280,000 related to botnets [10]. The millions of cyber-attacks witnessed against this financial institution highlights the desperate attempt to bypass the information security.

Another report worthy of mentioning here is that which was made known in 2016 by the African Union Commission (AUC) and the cyber security firm Symantec. The report states that only 30 out of the 54 countries of Africa, did not have precise legal frameworks to tackle cyber related crimes. As stated in the introduction of this study, law enforcement agents in some countries would rather demand their own share of the stolen funds than take major actions against the perpetrators. Kshetri reference as regards the reportage of government officials in Nigeria who claim to be unaware of cybercrimes within the country and even described it as Western propaganda seems to be valid. More so, it seemed more likely that the Nigerian elites at that time were more interested in using the EFCC as a witch hunting agent against political dissidents. In addition, some top ranking state officials were reported to have been involved in cybercrimes .Unfortunately, there are recent revelations that shows that there are Nigerian elites who are still in the fraudulent cyber business.

Channels Tv in 2021 reported that Abidemi Rufai, who served alongside Ogun State Governor in Nigeria as Senior Special Assistant on Special Duties was arrested in the US over $350,000 employment fraud. Rufai who was said to have used multiple and unidentifiable e-mail addresses and as well stole the identities of over a hundred (100) Washington residents. This stolen identities were then used to file claims with Employment Security Department (ESD) in order to partake in the pandemic-related unemployment benefits. This is once again a case of business email compromise[21].

Cyber-Crimes in Nigeria: An Institute of Mere Compromise or Sophistication

Cyber related crimes in Nigeria has over the years grown due to factors that can most likely be not just compromise but sophistication just as Lorliam has claimed. For example, the 2021 report by cyber authorities in the US, UK and Australia showed that a number of agencies like the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency, National Security Agency and Cyber Security Centre in 2021, detected an increase in cyber-attack sophistication in the US, UK and Australia. Noteworthy, is the increased rate at which ransomwares were used against dire infrastructure organizations globally. Similarly, Microsoft in its 2020 digital defense report reveals that the persons involved in cyber threat have swiftly improved in their sophistication over the past year. Microsoft notes that they use strategies that make it more difficult for them to be identified and as well threaten even the tech savviest. What is more is that the new techniques have increased the chances of getting utmost access to high-value targets, cyber-crime syndicates that have businesses as their targets have relocated their organization to the cloud in order to disguise their identities among legitimate services. Also, these same cyber-crime actors have assembled new ways that search the internet for vulnerable systems. That is technological systems that are susceptible to ransomware. This in fact begs the question whether the security outfits that were set up in Nigeria to tackle such illicit activities have the necessary expertise and resources to defend the security systems which Lorliam proposed. And even if they do, can they put it into use without undue interference from the elites. One can as well postulate that even the developed countries like the US, UK and Australia have access to the best resources yet cannot prevent such attacks from occurring. But at least regular arrests are being made in the aforementioned countries and jail terms served appropriately without compromise or so it seems. The same cannot really be said about the Nigerian situation. Instead, there seems to be a bigger accomplice that shields the culprits from the law. An interesting validation of this is the FBI's indictment of the renowned super cop, Abba Kyari in the Hushpuppi case [18] or the Instagram affluent celebrity known popularly as Mompha arrested twice by EFCC.

However, in a twist of events, the Superintendent of Police termed the FBI tip on Abba Kyari as being misled but clamoured calls by the US and Nigerians, release of FBI's overwhelming evidence led to a review of the case [11]. The interest in reviewing the case must have stemmed from the need to maintain a transparent stance. This reaffirms the conviction on compromise beyond sophistication. In fact, Busari and Princewill [18] further reported that evidence reveals that Abba kyari enjoyed proceeds of the cyber-crime activity carried out by Hushpuppi to the tune of which makes him an accomplice. Since the police investigation has found him guilty and the Nigerian court demands he be reprimanded in prison, why then has he not been extradited to the US to answer for his part in Hushpupi's cyber-crime activity till this moment? Sahara reporters in their February 15, 2022 report states that according to the United States Department of Justice only the Nigerian government can offer reasons for the delay in the extradition of the 'super cop' Abba Kyari. The report further notes that extradition involves a lot of processes and that the case is a quite cumbersome one considering that he is wanted for some other drug trafficking related crime. Princewill [4] reports that he is to face charges on cocaine smuggling. Unfortunately, all these might be delay tactics in order to ensure he is not extradited to the US. What is more is that this might be an indication that there are some other higher forces involved in the Hushpuppi circle.

Cyber-Criminality, the New Economy

Studies like that of Lorliam that have explored the negative impacts of cyber-crimes on the Nigerian economy may be missing some integral factors that can lead to negligence or aiding and abetting such illicit activities. What is more is that Ismail [12] posits that a total of $1.5 trillion is made from global cybercrime making it one of the largest growing economies in the world. The implication for this is that there are possibilities that state actors may look to it as not just a source of power but as a means of revenue. Todd

[13] in quoting Mieke Eoyang, the deputy assistant secretary of defense for cyber policy states that the line between state actors and cyber criminals has become blurry, as it is no longer easy to identify who is precisely behind cyber-attacks. This is a validation that there are state actors who benefit from these sort of attacks. The argument remains whether these state actors are all in for the money or power. Mieke Eoyang is further quoted as saying that there are governments who leverage on cyber-crimes in order to shield them from prosecution.

Furthermore, Odejobi [14] reports that Hushpupi had claimed that Mompha an affluent instagram celebrity helps politicians in Nigeria to launder money. This was said to have been uttered during an altercation between the two parties. The same information was also revealed by Ikeji [15] with a screen shot as proof. If this is the case then it might be plausible to note that asides the power which the state actors can wield in this regard, it is possible some percentage is charged by the government as leverage in exchange for protection and freedom. Perhaps another angle to this is to examine the situation in developing countries like Nigeria.

In Nigeria, when cyber criminals are charged to court and found guilty their properties are confiscated so also the money in their accounts. But what happens to these confiscated items? Yusuf [16]reports that the EFCC does not keep such properties or recovered monies but returns it to the individuals, state or federal government. By implication, the funds are not really returned to the victims who are most likely abroad. This act in a way confirms the active role which state actors play in the progression of cyber fraud. Bromium's independent (2018) study is parallel to the above postulation. This study examined the interconnected dynamics of cybercrime and reveals that cybercrime is a booming venture which has resulted in trillion dollars illicit profits being acquired, laundered, spent and reinvested by cybercrime fraudsters. The interesting idea shared in this study is the term used 'illicit profits'. This is one of the few studies that terms this endeavor as profit. Another comprehensive study by same Bromium [17] reveals that up to $200 billion is generated each year in illegal cybercrime profits. This includes monies laundered. According to Oludare [17], Nigeria losses 127 billion naira to cyber-crime annually. With the increase in cyber-crimes it is most likely that this number would or might have increased. That is to say out of the global $1.5 trillion, Nigeria loses over $350 million which is quite a significant amount that can make a meaningful change in infrastructures and general welfare of the masses [22-23].

Conclusion

There is no doubt about Lorliam's proposition being one of the appropriate moves that should be taken in order to curb cyber insecurity. What is more important is to consider the 'big players' or entities who are beneficiaries and can thwart the efforts being put in place to tackle this level of insecurity. For instance, when an individual or corporate establishment is duped by a cyber-crime ring, it becomes a case of loss to the scammed but profit not just to the scammer but his/her immediate environment. This is so because the money made from this criminal activity could be spent on car purchase, house, clothes, food, health, investment, offsetting necessary bills, and most notably bribery to government agencies which includes the likes of EFCC, Nigerian Police Force (NPF). Besides, Nigerians in the act of cyber-crime have been observed to be extravagant in their spending.The famous business mail hacker known as Hushpuppy comes to mind here. According to Ratliff [19], he is a Gucci master that has a knack for extravagance. He lived in a penthouse apartment at the Palazzo Versace Dubai, with a private pool and had a luxury collection which includes a private jet, Rolls-Royces, Ferraris, Hermes, Fendi, Luis Vuitton and of course Gucci. Moreover, he most possibly has properties in Nigeria, sends money to his relatives in Nigeria and owns business ventures. Same can be said for Invictus Obi, whose properties and investments in Nigeria were seized by the federal government when he was indicted for business email cyber-crime in the US. Therefore, it might be necessary to come to terms with this institution as a profit generating one and identifying the benefactors first before deciding appropriate measures to tackle it.

References

1. Kshetri N (2019) Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management 22: 77-81.
2. Burt T (2020) Microsoft report shows increasing sophistication of cyber threats , Microsoft report shows increasing sophistication of cyber threats - Microsoft On the Issues.
3. Cybersecurity Authorities in the United States, Australia, and the United Kingdom (2022) 2021 Trends Show Increased Globalized Threat of Ransomware , https://www.cisa.gov/uscert/ncas/current-activity/2022/02/09/2021-trends-show-increased-globalizedthreatransomware#:~:text=CISA%20encourages%20users%20and%20administrators,and%20-this%20Privacy%20%26%20Use%20policy.
4. Princewill N (2022) Nigeria hero 'supercop' arrested in cocaine smuggling case , Nigeria hero 'supercop' arrested in cocaine smuggling case - CNN.
5. Platt A (2018) The increasing sophistication of cyber-attacks means stronger strategies are needed in financial organizations ITProPortal , The increasing sophistication of cyber-attacks means stronger strategies are needed in financial organisations | ITProPortal.
6. Hanafi A (2021) Scammers joining police to cover tracks – Sources , How Yahoo boys befriend, bribe policemen, soldiers to evade justice (punchng.com).
7. Oludare I (2020) EFCC Police promoting internet frauds in Nigeria – NANS alleges , EFCC, Police promoting internet frauds in Nigeria - NANS alleges - Daily Post Nigeria.
8. Dolley C (2021) Cyberattacks : South Africa, you've been hacked , South Africa now has the third-highest number of cyberc... (dailymaverick.co.za).
9. Olakoyenikan S (2020) Online coronavirus scams spread in Nigeria amid lockdowns , Online coronavirus scams spread in Nigeria amid lockdowns | Fact Check (afp.com).
10. GNA (2018) Bank of Ghana launches Cyber Security Directive for Financial Institutions. BusinessGhana. Retrieved from Bank of Ghana launches Cyber Security Directive for Financial Institutions - BusinessGhana https://www.ghanaweb.com/GhanaHomePage/business/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions-695006.
11. Ravens N G (2021) Nigeria Police to review super cop Abba Kyari's indictment Ravens , Nigeria Police to review super cop Abba Kyari's indictment - Ravens (ravensng.com).
12. Ismail N (2018) Global cybercrime economy generates over $1.5TN, according to new study. Information Age. Retrieved from Global cybercrime economy generates over $1.5 trillion (information-age.com).
13. Todd L C (2021) In Cyber Differentiating Between State Actors, Criminals Is a Blur US Department of Defense , In Cyber, Differentiating Between State Actors, Criminals Is a Blur > U.S. Department of Defense > Defense Department News .
14. Odejobi M (2017) Hushpuppi reveals that Mompha helps politicians launder money and he is a Whistleblower for

EFCC , https://www.legit.ng/1132482-hushpuppi-reveals-mompha-helps-politicians-launder-money-a-whistleblower-efc.html.

15. Ikeji L (2017) Hushpuppi alleges that Mompha helps Nigerian Politicians to launder money & is a whistle-blower for the EFCC , Hushpuppi alleges that Mompha helps Nigerian Politicians to launder money & is a whistle-blower for the EFCC (lindaikejisblog.com).
16. Yusuf O (2019) EFCC reveals what happens to money properties seized from fraudsters , https://www.legit.ng/1262673-efcc-reveals-money-properties-seized-fraudsters.html .
17. Bromium INC (2018) Up To $200 Billion in Illegal Cybercrime Profits is Laundered Each Year, Comprehensive Research Study Reveals. Into the Web of Profit , Up To $200 Billion In Illegal Cybercrime Profits Is Laundered Each Year, Comprehensive Research Study Reveals | Hp Wolf Security (Bromium.Com).
18. Busari S and Princewill N (2021) FBI investigating Nigeria's 'super cop' in Instagram influencer HushPuppi fraud case, Abba Kyari: FBI investigating Nigeria's 'super cop' in Instagram influencer HushPuppi fraud case - CNN .
19. Ajao, G. (2018, May 09). Curtailing cyber-attacks in Africa. TechDotAfrica. Curtailing the prevalence of cyber-attack in Africa (tech.africa)
20. Ratliff E (2021) The Fall of the Billionaire Gucci Master BloombergUK , Instagram Influencer Hushpuppi's Rise Was Allegedly Fueled by Cyber Scams (bloomberg.com).
21. Channels Television (2021) Dapo Abiodun's Aide, Abidemi Rufai Arrested In US Over $350,000 Fraud, Dapo Abiodun's Aide, Abidemi Rufai Arrested In US Over $350,000 Fraud – Channels Television (channelstv.com) .
22. Oludare R (2017) Nigeria loses N127b yearly to cybercrimes TheGuardian , Nigeria loses N127b yearly to cybercrimes' | The Guardian Nigeria News - Nigeria and World News – Technology-The Guardian Nigeria News – Nigeria and World News.
23. Staff Writer (2021) South Africa under cyber-attack: Interpol reveals top threats in South Africa BusinessTech. Retrieved from South Africa under cyber attack: Interpol reveals top threats in South Africa (businesstech.co.za).