John Adinya Odey, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 11, Issue 10, (Series-II) October 2021, pp. 01-14

RESEARCH ARTICLE OPEN ACCESS

The Potential Impact of Cryptojacking on Nigeria's Critical National Infrastructure: A Study of Power And Energy Infrastructure.

John Adinya Odey[1], Agber Terdoofan[2] andBamidele Ola[3]
[1]*Department of Computer Science, University of Calabar, Calabar, Nigeria.*
[2]*Department of Intelligence and Cyber Security, Nigeria Defense Academy, Kaduna, Nigeria.*
[3]*Department of Computer Information Sciences, University of the Cumberlands, USA.*

ABSTRACT
Cryptomining is a decentralized computational process employed to acquire new coins, validate transactions, and add them to a Blockchain ledger. Their use of cryptography to verify the transfer of assets and secure financial transactions has brought new challenges in cryptomining. One of such challenges is cryptojacking, a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) computing power by cybercriminals to generate cryptocurrency. This paper examines Nigeria's precarious digital landscape, especially regarding critical national infrastructures, to determine how proactive it can be shielded from crypto-jacking attacks on the power and energy infrastructure. A descriptive approach was adopted in this study and implemented by comparative and qualitative content analysis of texts from policy documents using the R statistical software on the study population of three countries: the United States of America (USA), United Kingdom (UK), and Nigeria. The result of this study serves as a template on how the Nigerian cyber security stakeholders and key policymakers in government can effectively navigate this emerging but potentially devastating new age threat that could cause the nation major setbacks.
Keywords: Cryptocurrency, Cryptojacking, Cryptomining, Critical National Infrastructure (CNI).

Date of Submission: 30-09-2021 Date of Acceptance: 13-10-2021

I. INTRODUCTION

Since the emergence of Bitcoin as the first decentralized currency in 2009, there has been a slew of other digital currencies created. Their use of cryptography to verify the transfer of assets and secure financial transactions has made the popularity of cryptocurrencies ever on the rise, and this increasing demand has in turn brought about new challenges, including cryptomining. Cryptomining in and of itself is a computational process employed to acquire new coins, validate transactions, and add them to a decentralized blockchain ledger. This ledger is protected by very complex cryptographic functions that cannot easily be decrypted and is the means through which cryptocurrency is centralized and distributed. While cryptomining is a free-for-all venture by all standards, it is only profitable when carried out with specialized, high-powered machinery. This also is inclusive of large amounts of electricity needed to power equipment running at full scale. Therefore, it is difficult for underpowered mining operations to operate at a profit as the heavy investments in infrastructure needed far outweigh what is garnered through mining. Therefore, it is pertinent that to be any good as a cryptominers, one should have access to a steady and enormous source of electricity and processing power to boot. To address this challenge, miners should invest larger and larger sums of money into acquiring and setting up high-performance machines needed to generate the hashes to validate transactions (Krishnan, Saketh, & Tej, 2015).

1.1 THE MENACE OF CRYPTO-JACKING

As the cost to mine cryptocurrencies becomes prohibitive, various organizations do ask some internet users to allow the mining of cryptocurrency using their computing resources in exchange for eliminating advertisements. However, some miners with dubious intents are now simply stealing or "hijacking" the necessary computing power from an unsuspecting public. In-browser mining scripts now allow crypto-jackers to use the computing power of anyone who visits an infected website; malware can now be spread through malicious links, advertisements, email attachments,

public Wi-Fi, fake apps, and system backdoors (Marshmclennan, 2018). Some resources represent strong targets of interest for cryptojacking. These include critical infrastructures that generate or consume significant amounts of power (electrical). These companies rely heavily on cloud services and users of Internet of Things (IoT) devices, which allow miners to quickly aggregate computing resources and power from a group of hijacked devices to mine cryptocurrency.

As mining cryptocurrencies requires a lot of processing power and electricity, thus generating enormous amounts of heat, there are serious concerns about the legality of crypto-mining and the trading or use of cryptocurrencies; thus leading to bans in certain countries and restrictions in others or moratoriums. According to (Hanibal Goitom, 2018, Said, Ahmed 2019), some countries like Algeria, Iraq, Morocco, Egypt, Bolivia, Morocco, Nepal, Pakistan, and the United Arab Emirates (UAE) have made laws to enable absolute bans on the use of cryptocurrencies. At the same time, countries like Bahrain, Bangladesh, Colombia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia, and Taiwan have inferred bans. China as at 2018, placed a ban on initial coin offerings and in 2021, has shut down crypto-mining operations and halted virtual currency trading. Iceland is currently allows crypto-mining due to the availability of cheap electricity in the region. Plattsburg, a town in uptown New York placed an 18-month moratorium on crypto-mining to cut down electricity consumption (Oberhous, 2018). As cryptocurrencies experience an increase in popularity, so do more concerns (legal and otherwise) arise over the mining operations involved to keep the industry flourishing.

For Nigeria, it has been new technological dawn since internet access became affordable. There has been a significant increase in the number of software engineers, developers, and the numbers are still on the rise. This has, in turn, informed so many businesses (start-ups included) to take their businesses online. The Nigerian digital space is home to most new-age businesses, from mobile to web applications to chat-bots and several other technological tools. The Federal Capital Territory (FCT) and Lagos State are two (2) of Nigeria's major ICT hubs, with most businesses in both cities becoming IT powered. A concentration of web-based crypto-jacking in these cities alone, even if targeting only mobile phones and laptops, would surely cost a fortune in financial losses for both businesses and individuals alike. On the part of Critical National Infrastructure (CNI), Nigeria has primarily kept its operations manual and is not IT-driven. However, the energy (electrical) sector is very susceptible to cryptojacking. Nigeria's electricity is hydro and gas-powered. According to (USAID, 2019) in Nigeria's Power-Africa fact sheet there are currently thirty-eight power stations (hydro and thermal) in Nigeria with a production capacity of about 12,522MW of electricity. However, the country can primarily generate about 3,384MW, a grossly inadequate amount for a country with a 186 million population. Therefore, these figures make it terrifying to ideate the devastation that a crypto-jacking attack on the power stations could cause. The probability of such attacks should not for any reason be ignored because as some countries are clamping down on crypto-mining activities on their territories, these miners spread out, pouncing on more porous and vulnerable regions in which to operate.

In light of these, this work seeks to explore and bring to fore the potential impacts of crypto-jacking attacks on a country such as Nigeria.

II. LITERATURE REVIEW

Classic cryptocurrencies such as Bitcoin and Ether build on proof of work (PoW) CPU-bound functions; this means mining efficiency mainly depends on the available computing power. Graphics processing units (GPUs) and application-specific integrated circuits (ASICs), thus, provide better mining performances for such demanding computations than basic CPUs. As a consequence, profitably mining such currencies is quite infeasible with regular desktop and mobile computing systems. As a remedy, Altcoin (such as Monero) has been developed to use memory-bound functions for constructing computational puzzles. This intensive memory access bounds the run-time of the function and moves the overall mining performance from the computing resources to the available memory access performance (Musch et al., 2018). Browser-based or In-browser mining is the most common method usually employed by attackers.

According to (Saad, Khormali & Moheisen, 2018), In-browser crypto-jacking is done by injecting a JavaScript code into a website, allowing for the hijacking of the processing power of a visitor's device in order to mine a specific cryptocurrency. Upon visiting a website infected with crypto-jacking code, a javaScript is automatically executed in the host computer, starting a mining activity, thus becoming part of a crypto-jacking mining pool. This pressure on a device's resources (processors and memory) can cause malfunctions and ultimately crash the device. It is important to note that there are multiple vectors where various entities can inject mining scripts into a website's codebase (Eskandari et al, 2018).

Another area of the overwhelming impact of crypto-mining is in energy consumption. As of July 2019, Vincent (2019) reports that Bitcoin consumes more energy than Switzerland's entire nation. (Page, 2018) acknowledges that crypto-mining activities consume vast amounts of electricity, solving required computational problems. (Krause, M.J., Tolaymat, T, 2018) observed that energy costs of four cryptocurrencies (Bitcoin, Ethereum, Monero, and Litecoin) for 30 months were responsible for 3-15 million tonnes of CO2 emissions. (Mora et al., 2018) warned that Bitcoin could single-handedly drive two degrees Celsius of global warming within the next three decades due to carbon dioxide emissions related to its energy consumption. In May of 2018, Plattsburg residents voted to place an 18-month moratorium on all crypto--mining activities in the area because in January and February of that year, the city went over its cheap power quota for the period due to a cold winter and, the city blames it also on cryptocurrency activities within the area (Oberhous, 2018). Instances such as these are becoming rampant across several towns in the USA and other countries, thus begging the question of serious legislation concerning crypto-mines.

The effects of crypto-jacking are far-reaching tentacles that are also felt none too slightly in enterprise environments. Crypto-jackers are increasingly beginning to bundle miners in exploit kits and other more traditional malware delivery methods away from in-browser mining. Criminals are targeting mobile apps on official app stores like Google Play as a way to broaden their crypto-jacking reach. These apps get infected with coin-mining malware to build up the number of devices silently mining currency for them. The same method gets applied to conventional banking Trojans and other malware. When these kinds of attacks are thus carried out at scale against an enterprise's whole collection of endpoint assets, the performance impact will add up quickly (Chickowski, 2018).

Cryptojacked machines also attempt to infect neighboring machines, generating large amounts of traffic that can overload victim computer networks. (Eitzman et al., 2018) also noted that in the case of operational technology (OT) networks, the consequences could be a lot more severe. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS) environments rely on low-bandwidth hardware and networks as even the slightest increase in CPU load, or the network could leave critical infrastructures unresponsive, impeding operators from interacting with the controlled process in real-time.

Cloud infrastructures are not left out of the crypto-jacking rampage either. Sheridan (2018) states that attackers now have unprecedented access to high-powered public cloud computing resources as crypto-jacking activities have gone mainstream. Major corporations such as Tesla, Gemalto, and Aviva have unfortunately been caught in this web. She notes that this trend is partly because the bar to enter the world of cryptomining is low, and the payoff is relatively high.

The first-ever reported instance of a crypto-jacking attack specifically targeting a nation's critical infrastructure was in 2018, at a water facility in Europe. The incident was found and reported by a security outfit called Radiflow (Radiflow,2018). As at the time of reporting in February 2018, Radiflow had determined that the cryptocurrency mining software was on the water utility's network for approximately three weeks before it was detected. There was also limited evidence to ascertain if the malware had spread from the initial point of infection to other systems on the utility's networks (Kerner, 2018). Interestingly, Radiflow would not name what particular facility had been affected but somewhat ambiguously stated the utility was 'situated in Europe.' This practice of not reporting security incidents is relatively common and significantly impedes advancements in security engineering. For such attacks on Critical National Infrastructure (CNI), one would argue that perhaps the secrecy is due to how central CNI are to a nation's functionality, and as such, it would be unwise to broadcast to the world and, in effect, would-be enemies just how vulnerable to attacks a nation is (Simmons, 2019). In (Stu Sjouwerman, 2019), a survey of professionals using industrial control systems (ICS) and operational technology (OT) finds 90 percent of respondents say their environment has been damaged by at least one cyber-attack for two years, with 62 percent experiencing even more attacks. The people who manage critical systems such as manufacturing plants and transportation almost unanimously stated that they are fighting-off cyber-attacks regularly," (Ponemon Institute, 2018)

It is of great concern that attacks on CNI are becoming more commonplace globally, with China and Russia being fingered as the most likely offenders, especially against the United States of America (Ranger S., 2019). While China presents a persistent cyber-espionage threat and a growing attack threat to US core military and critical infrastructure systems, Russian intelligence and security services continuously target US information systems, as well as the networks of NATO and its allies for technical information, military plans, and insight into US governments' policies (Ranger S., 2019). Interestingly, China, which dominates 70 percent of the world's crypto-mining operations, is

also home to the world's largest crypto-mining hub (Huang, 2019).

The WannaCry and NotPetya ransomware (Forrest, C. 2018). attacks of 2017 were eye-openers for the world. Ransomware attacks in 2018 (Fischer, D., 2018) did not have such an impact; however, Davis (2019) states that 70 percent of such attacks targeted small businesses. The same 2018 however, saw the re-branding of ransomware worms to contain crypto-jacking mining scripts (Cardona, 2018) as in an instance, United Kingdom (UK) government computers had been infected with a mining virus through an app that reads websites aloud to the blind.

In Nigeria (Deloitte, 2019) stated that many Nigerian companies and organizations suffered a spate of data breaches and ransomware attacks, which caused the loss of billions of Naira in the year under review, though grossly under-reported. The report also stated that many organizations also experienced crypto-jacking because it is a cheaper alternative to ransomware that requires much less technical skills. Sanni (2019) captures the position of the Nigerian government to cryptocurrencies and crypto mining as ambiguous, unlike in countries like Morocco and Algeria. Mordi (2019) noted that Nigeria does not even make the list of Statista's 2017 world's largest consumer losses through cybercrime. This is due to a culture of gross under-reporting of these crimes by both individuals and organizations. Poor cyber security awareness amongst the populace, inadequate professionals to appropriately handle the issues are also factors why Nigerians do not bother reporting these crimes. Given that statistical evidence of cybercrimes in Nigeria is all but non-existent, it would be quite daunting to say for sure whether or not a crime such as crypto-jacking which flies under the radar, leaving barely any traces save for a grossly under-performing device; maybe a crashed one – is actually being carried out.

Another issue worthy of note is Nigeria's epileptic power supply. In 2019, the national grid collapsed six times in the first four months, despite huge investments made in the power sector (Okafor, 2019). As at the time of gathering data for this report, the national grid collapsed yet again on 16th January 2020, plunging the nation into her first blackout of the year; a rather depressing phenomenon as 2019 had seen over ten of such collapses (Wahab B., 2019, Wahab, B., 2020). With the non-investigative approach towards issues usually adopted in the country, it is not yet clear if the collapses result from poor management or cyber-attacks on the nation's critical infrastructure. The latter possibility should be a great cause for worry.

III. METHODOLOGY

A descriptive approach was used. Data from secondary data sources that included web articles, journal publications, national government publications, and national laws were collated, organized, and analyzed. The comparative and qualitative content analysis of texts from policy and strategies documents (ONSA, 2021, CISA, 2019, and JCNSS, 2018.) of the study population consisting of three countries; United States of America (USA), United Kingdom (UK), and Nigeria were done. The R statistical software was used for the implementation to qualify existing and emerging characteristics and concepts that would showcase the impact of cryptojacking on the CNI of each of the sample countries in terms of preparedness and policy robustness. The keyword 'Protection' was matched with such other related words as 'protect', 'security', 'secure', 'preparedness', 'safe', 'restrict', 'safety', 'safeguard' and 'regulate'. A dendrogram was drawn for each country using this data. Also, Text Maps of each country was plotted using scales of 'good' and 'bad' word to show the level of cybersecurity preparedness in the country.

IV. RESULTS AND DISCUSSION

The results are a product of descriptive analysis by qualitatively analysing the security strategies of the sampled countries using the R statistical tool. To achieve this, certain specialized packages were installed in R Studio: *Magrittr, devtools and wordVectors.* wordVectors was particularly necessary to train the program in recognizing the required word patterns. The various libraries of these packages were called prior to commencement of analysis, during which the dendrograms and word maps were plotted accordingly.

4.1. COMPARATIVE ANALYSIS

The results from analyzing the various strategies and policy documents (ONSA, 2021, CISA, 2019, and JCNSS, 2018.) of Nigeria, USA and UK respectively are as shown in the figures below, along with the accompanying discussions for the obtained results.

4.1.1 The Strategies and Policy document of theUnited Kingdom (UK)-*(JCNSS, 2018)*

Figure 4.1 below shows the results from training the program to recognize the text as vectors, and creating the vector model for the key word. It also shows some words in the text observed to have the closest proximity to the key word ‘Protection’.

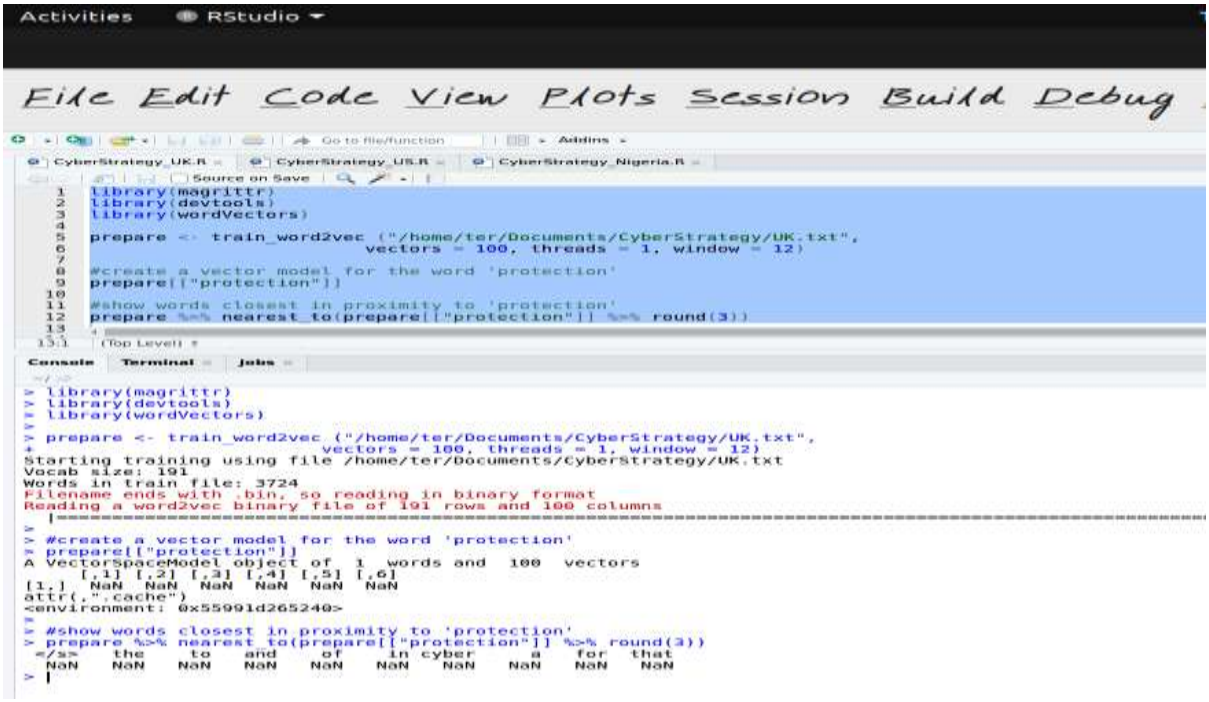

Figure 4.1: Creation of Vector Model for the key word.

Figure 4.2 is a depiction of all the words in the text (JCNSS, 2018) that best describe 'Protection' as a concept. It shows a total sample of 50 words.

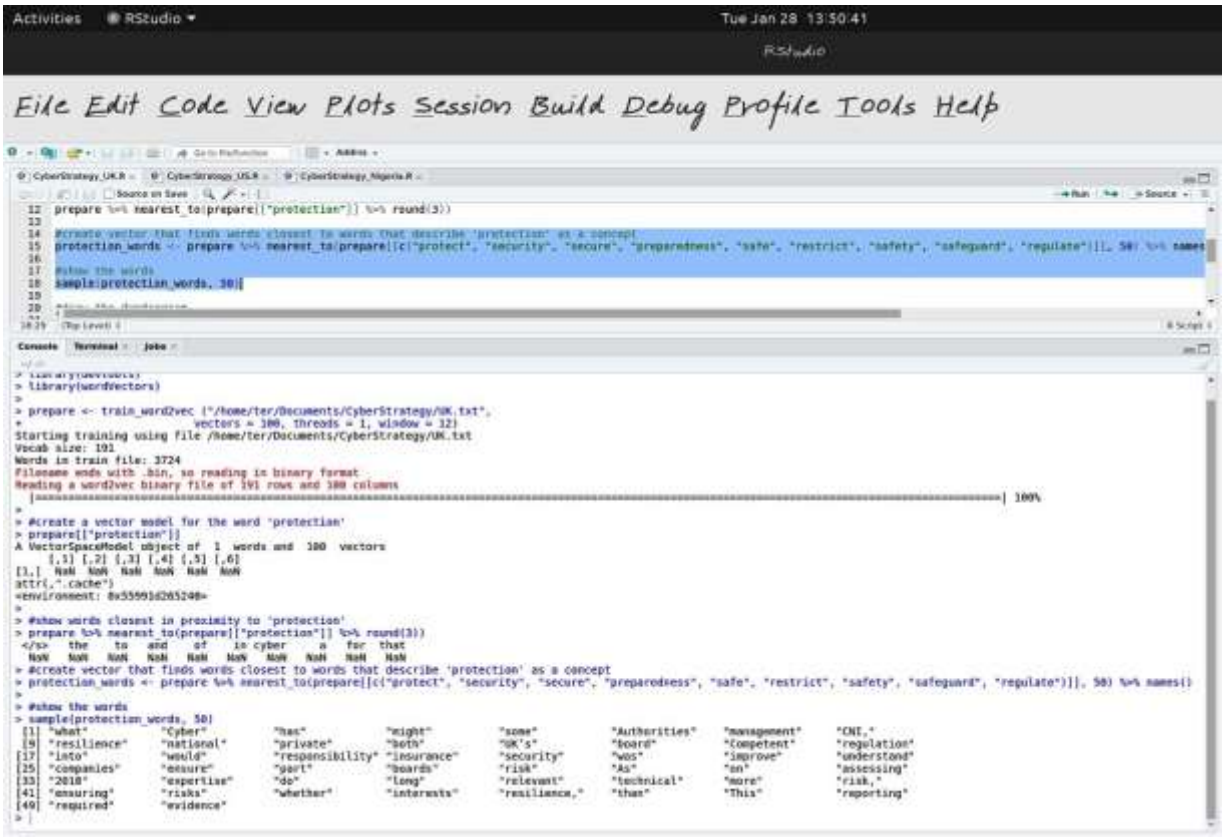

Figure 4.2: Sample of words that best describe the concept of 'Protection'

Figure 4.3: Cluster dendrogram of 50 words closest to a protection vector in JCNSS, 2018

Figure 4.3 shows the dendrogram as plotted using the fifty words of concept description. It is important to note the relationships between 'required', 'security', 'resilience' and 'responsibility'. This implies that to ensure CNI **security** and **resilience** in CNI infrastructures and possibly policies, the **responsibility** needs to be taken up and seriously. Other interesting word clusters pertaining to CNI protection are 'competent', regulation' and 'authorities', as well as 'assessing', 'risk' and 'management'.

Finally, Figure 4.4 is the word map for important connotations in the analyzed text. It shows that 'reporting' cybercrime incidences, 'competence', 'insurance' and other such words in the *good_score* region of the map are very key and important concepts in the protection of UK's CNI.

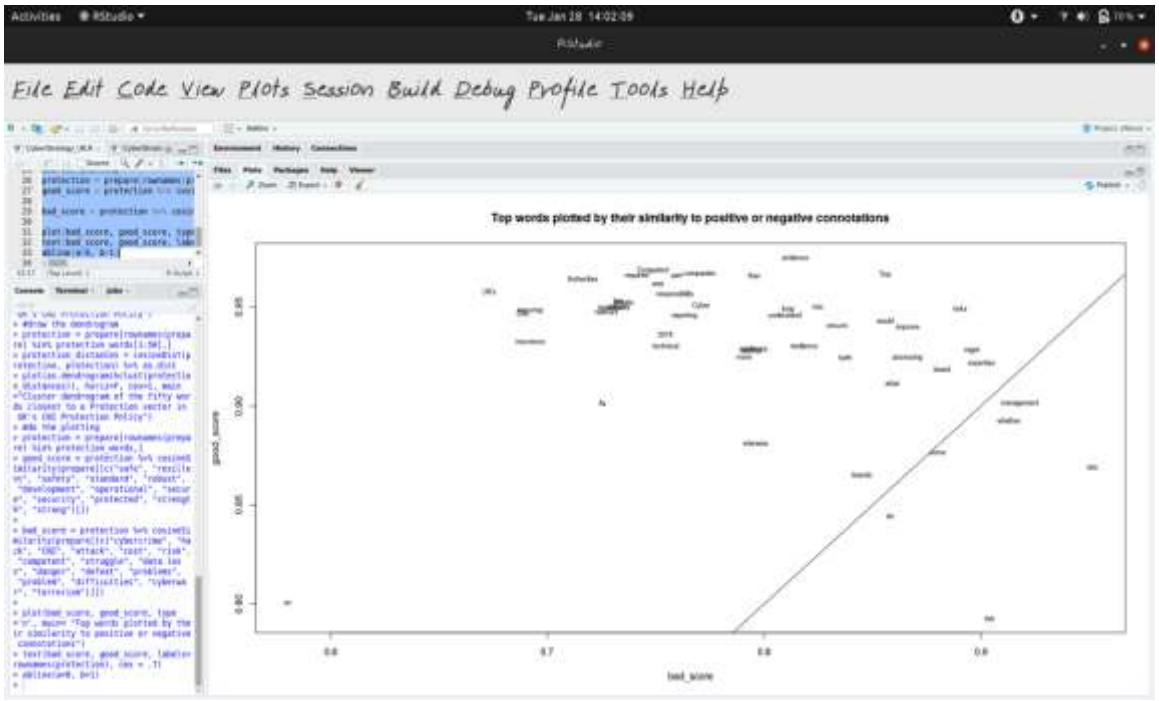

Figure 4.4: Word Map of positive and negative connotations in the reviewed text

4.1.2 The Strategies and Policy document of the United States of America(USA) -*CISA, 2019*

Figure 4.5 shows, results from training the program to recognize the text as vectors, and creating the vector model for the key word.

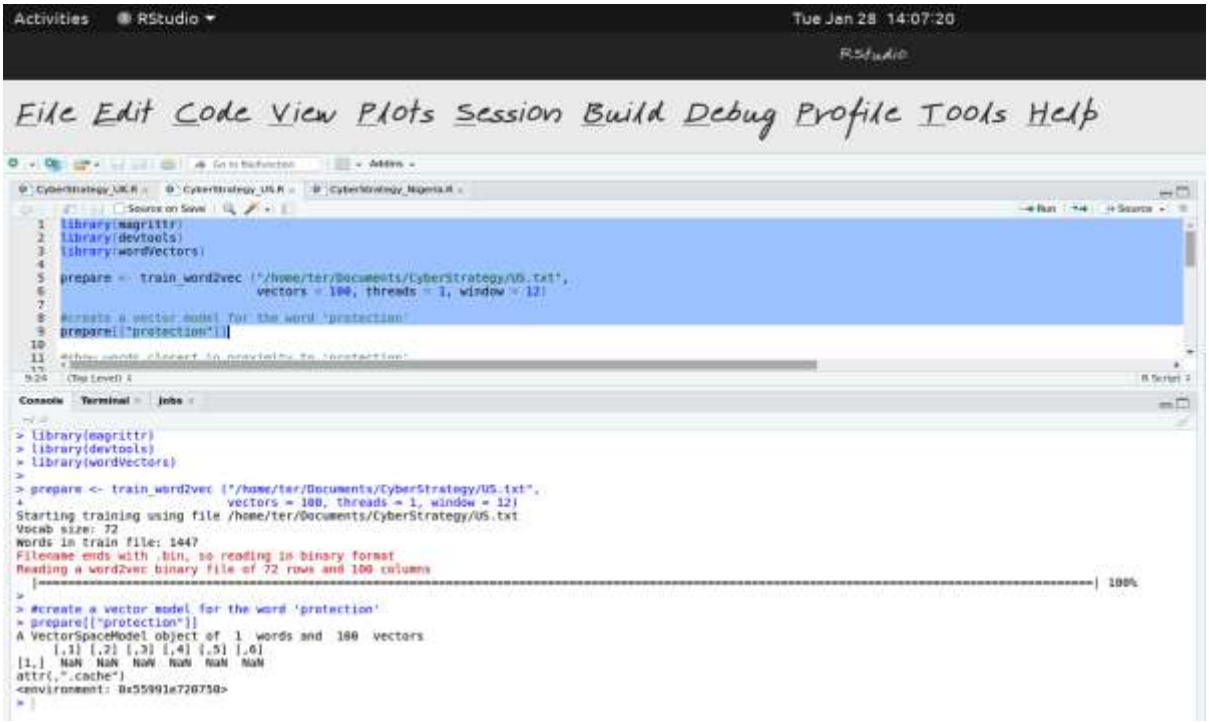

Figure 4.5: Creation of Vector Model for key word

Figure 4.6 is a depiction of the words in the text both nearest to 'Protection' as is used, and the fifty words closest to same 'Protection' as a concept. The relationship between these words is best shown in the dendrogram shown in Figure 4.7.

Figure 4.6: Cluster of words that best conceptualize 'Protection' of US CNI

Figure 4.7, the plotted dendrogram for the conceptual explanations, shows that information sharing across industries is key to protecting the various CNI in the country. Noteworthy too is that the US recognizes the role of the private sector in CNI protection and resilience as can be seen in the figure; this means it is a job not just left for/to the government.

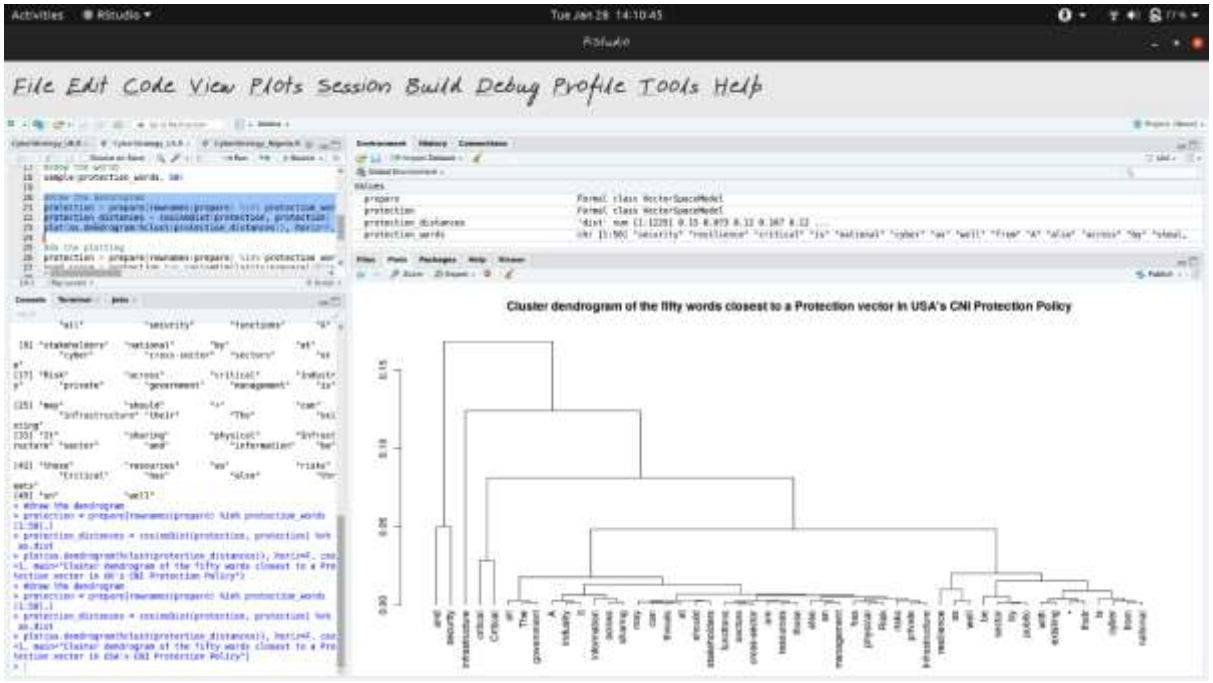

Figure 4.7: Dendrogram for cluster of 'Protection' concepts

Figure 4.8 is the text Word Map. It shows that stakeholders (government & private), the physical aspects of infrastructure (not just the digital) as well as critical information seem to be under constant threat and have a 'bad name', so to speak, in the security and safety of CNI in America.

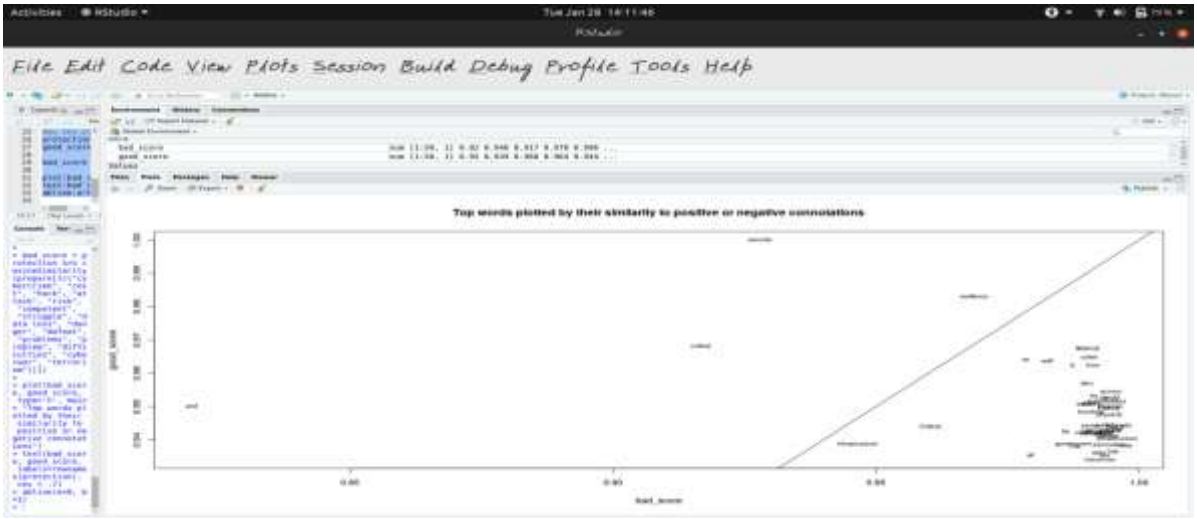

Figure 4.8: Word Map of analyzed text with emphasis on CNI protection in America

4.1.3 The Strategies and Policy document of Nigeria – *(ONSA, 2021)*

The analyses for Nigeria are shown in Figures 4.9 – 4.13.In Figure 4.9 as with the last 2 countries, is a representation of the Vector Model.

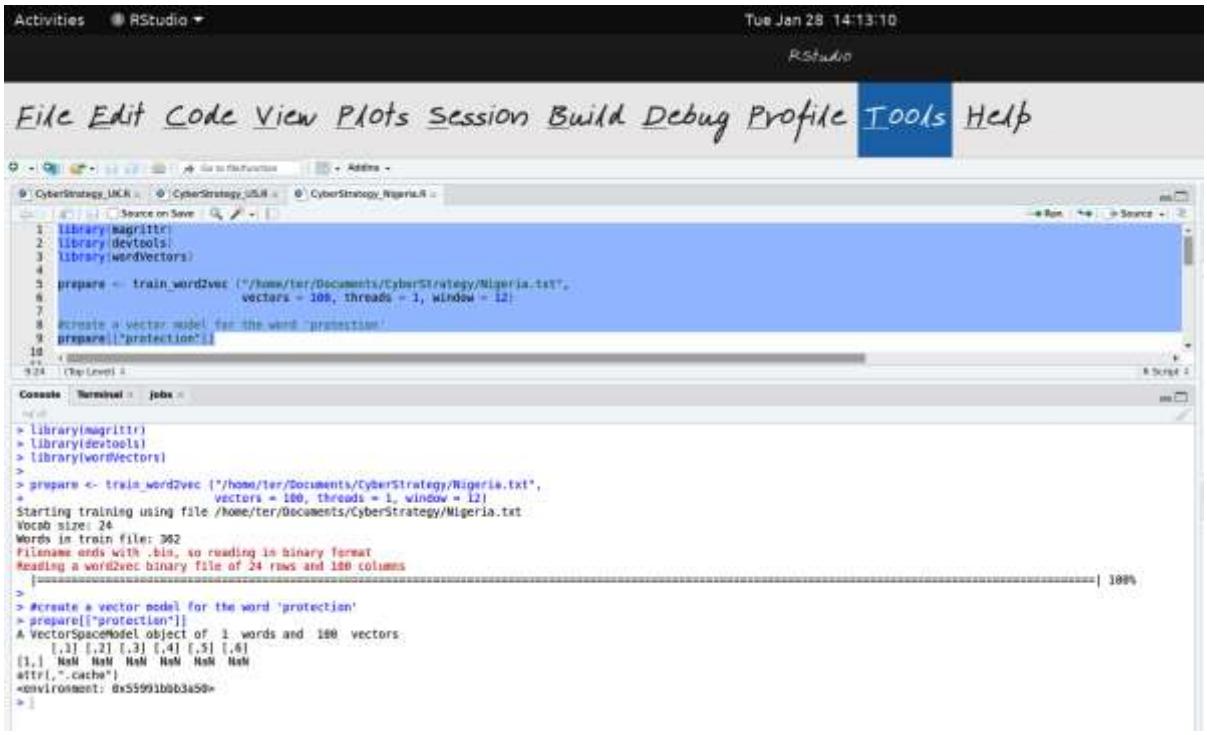

Figure 4.9: Creation of Vector Model for key word

In Figure 4.10 is where it gets interesting. The UK and USA were each analyzed with a 50-word cluster, drawn from words that best conceptualized the theory of 'Protection' of CNI as is insinuated in the strategy document. Nigeria however, could not meet the 50-word mark in all the analyzed text.

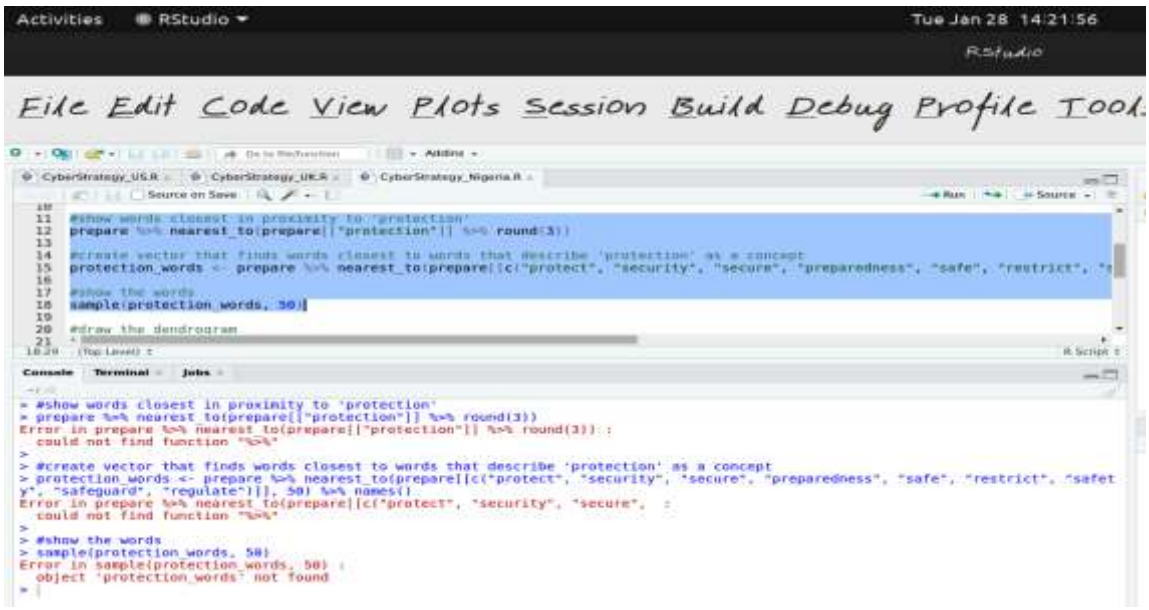

Figure 4.10: Insufficient connotations for 50-word count in conceptualizing 'Protection'

Figure 4.11 was where the word count was scaled down from 50 to 20. The program could then be run at the 20-word count. This means in all the analyzed text, only 20 words could connote protection of CNI in Nigeria as closely as possible.

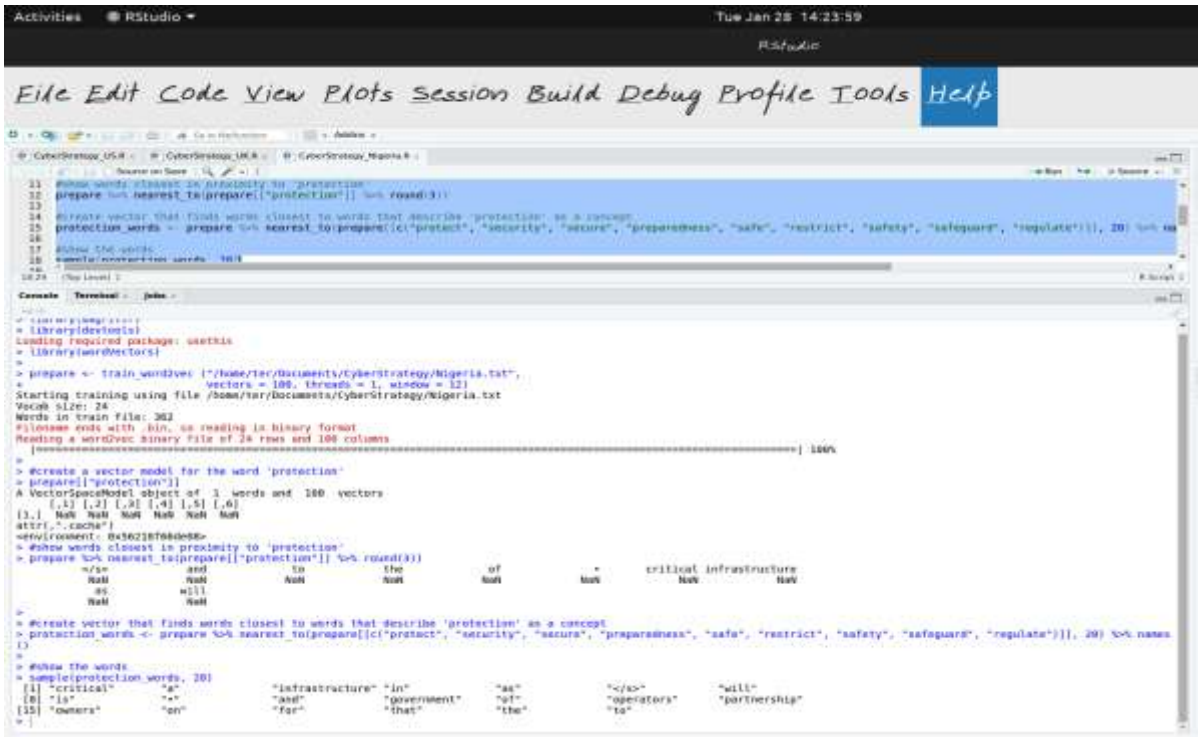

Figure 4.11: Accepted 20-word cluster of connotations for 'Protection'

Figure 4.12 is the plotted dendrogram for the word clusters identified in Nigeria's strategy document as regards CNI protection.

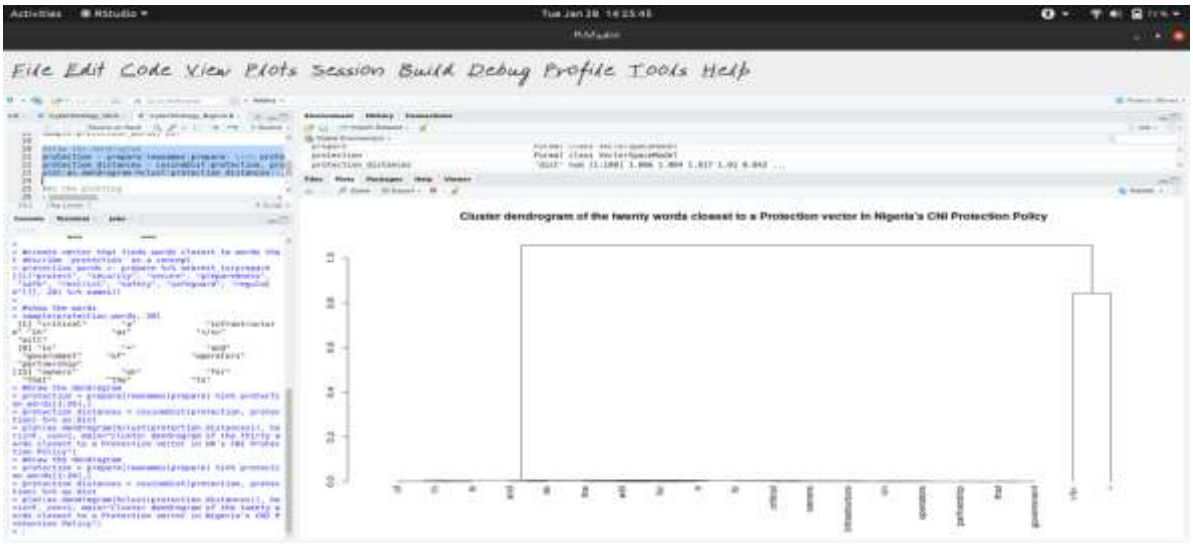

Figure 4.12: Dendrogram of identified word clusters for 'Protection' of Nigeria's CNI

In Figure 4.13 the Word Map of the textual analyses, is an all-empty field.

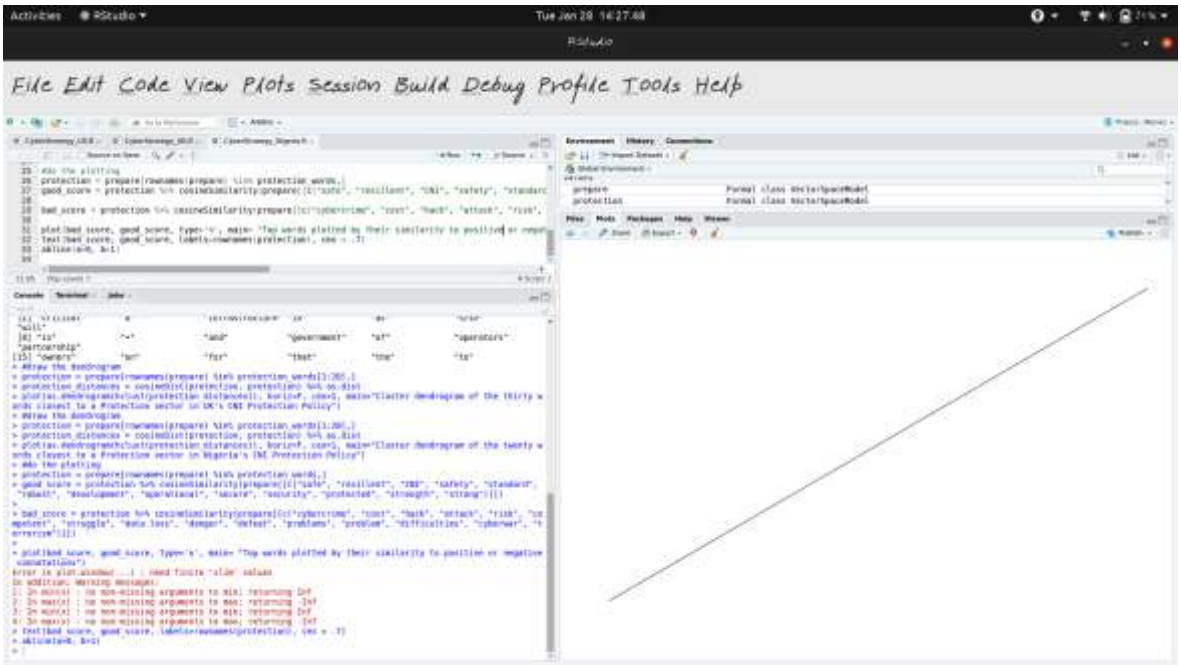

Figure 4.13: Word Map derived from textual analysis of Nigeria's strategy document

Analysis for each of the three countries ran seamlessly enough under the set conditions, except for Nigeria; here, the word similarity concept from which the dendrogram is plotted could only produce twenty words, as against 50 from the other countries. Also, the word map for Nigeria could not be plotted as the keywords could not be found in the essential concept. This was most likely because Nigeria's cyber security document has barely been implemented since its inception, even less so regarding CNI protection. For this reason, the keywords associated with CNI protection as was set in this work could not be found by the program.

The results of the qualitative analysis of the various strategies show that Nigeria is ill-prepared for an attack at all on its power infrastructure or any other CNI, least of all an attack as devastating as cryptojacking. This is evident first in the unavailability of the 50-word connotation for the concept of protecting the country's CNI as used in this study, then in the lack of suitable correlations in the plotted dendrogram and lastly in the absolute lack of data for developing a word map. An explanation for this phenomenon can be found in the fact that Nigeria's Cybersecurity strategy has not yet been properly implemented since its inception.

V. CONCLUSION

This study observed that as more people were jumping on the cryptocurrency bandwagon, competition in crypto-mining forced Miners to innovate new and more cost-efficient ways of mining, birthing crypto-jacking, thus posing significant risks to CNI. Analyses were undertaken qualitatively on strategy documents outlining CNI protection in the USA, UK, and Nigeria. The intention was to observe how Nigeria fared against the other two countries in terms of preparedness and policy robustness regarding protecting the nation's power infrastructure, which is most susceptible to a crypto-jacking attack.

The analyses showed a rather bothersome position for Nigeria, as very few keywords were found in its documents about protecting its power infrastructure or any other CNI in the country. It was also observed that this was partly due to an absence of policy implementation from the parties responsible for such.

While the analyses from this study showed exciting patterns from the policy and strategy documents the other countries were employed to secure their critical infrastructure, continuous improvements and adjustments were needed in keeping with the continuously and rapidly evolving landscape of cyberspace. Consequently, it was surmised that a crypto-jacking (or similar) attack on the three countries under study will be more devastating on the Nigeria power infrastructure, as results have shown. Therefore, it would be in the nation's best interest that relevant policies and strategies be implemented to ensure Nigeria meets up to international standards in cyber operations.

5.1 Further Research

Emphasis on this work was on the power infrastructure in Nigeria. Also, the metrics for

analysis were solely on strategy documents of the selected countries. Further studies using broader analysis metrics could be carried out, encompassing other CNI in the country (Nigeria). This further research could employ prescriptive analysis to ascertain precisely where the faults lie and put forth risk projections, along with possible remedial actions.

REFERENCES

[1]. Said, Ahmed (2019): The Economic Impact of Digital Fiat Currency (DFC): Opportunities and Challenges, 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary.https://www.econstor.eu/bitstream/10419/201744/1/ITS2019-Aswan-paper-44.pdf. Accessed on the 16th June, 2021

[2]. Cardona, M. (2018). "Goodbye Ransomware, Hello Cryptojacking!". https://www.securityroundtable.org/ransomware-data-breach-cryptojacking/Retrieved from on 19 January 2020.

[3]. Chickowski E. (2018). 5 Cryptojacking Consequences CISOs Can't Ignore. Retrieved from https://securityboulevard.com/2018/07/5-cryptojacking-consequences-cisos-cant-ignore/ on January 18 2020.

[4]. Davis, J. (2019). 71% of Ransomware Attacks Targeted Small Businesses in 2018. Retrieved from https://healthitsecurity.com/news/71-of-ransomware-attacks-targeted-small-businesses-in-2018 on 23 January 2021

[5]. Deloitte. (2019). Nigeria's cyber security outlook 2019. Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2019.html# on 4April, 2021.

[6]. Eitzman, R., Goody, K., Wolcott, B. & Kenelly J. (2018). How the Rise of Cryptocurrencies Is Shaping the Cyber Crime Landscape: The Growth of MinersRetrieved from https://www.fireeye.co/blog/threat-research/2018/07/cryptocurrencies-cyber-crime-growth-of-miners.html on 18 January 2019

[7]. Eskandari S., Leoutsarakos A., Mursch T. & Clark J. (2018). A First Look at Browser-Based Cryptojacking. 2018 IEEE European Symposium on Security and Privacy Workshops.https://users.encs.concordia.ca/~clark/papers/2018_sb.pdf. Accessed on 6th June, 2021.

[8]. Fischer, D. (2018). Ransomware is the present, but cryptojacking is the future. Retrieved from https://duo.com/decipher/ransomware-is-the-present-but-cryptojacking-is-the-future on 19th January 2020.

[9]. Forrest, C. (2018). New cryptojacking attack uses WannaCry exploit to mine on Windows servers. Retrieved from https://www.techrepublic.com/article/new-cryptojacking-attack-uses-wannacry-exploit-to-mine-on-windows-servers/ on 19th January 2020.

[10]. Huang Z. (2019). China, home to the world's biggest cryptocurrency mining farms, now wants to ban them completely. https://www.thestar.com.my/news/regional/2019/04/09/china-home-to-the-worlds-biggest-cryptocurrency-mining-farms-now-wants-to-ban-them-completely. Accessed on 18th January, 2021.

[11]. Kerner S.M. (2018). Water Utility in Europe Hit by Cryptocurrency Malware Mining Attack. Retrieved from https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurren cy-malware-mining-attack on January 18,2021.

[12]. Krishnan, H., Saketh, S. & Tej, V. (2015). Cryptocurrency mining – Transition to cloud. International Journal of advanced Computer Science and Applications. 6(9). DOI: 10.14569/IJACSA.2015.060915.

[13]. Mora, C., Rollins, R.L., Taladay, K. et al. Bitcoin emissions alone could push global warming above 2°C. Nature Climate Change 8, 931–933 (2018) doi:10.1038/s41558-018-0321-8

[14]. Mordi, M. (2019). Is Nigeria really the headquarters of cybercrime in the world? Retrieved from https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/ on 19 January 2021.

[15]. Musch M., Wressnegger C., Johns M. & Rieck K. (2018). Web-based Cryptojacking in the Wild. Computer Science Report: Technische Universität Braunschweig, Institute for Application Security.

[16]. Oberhous D. (2018). The City That Banned Bitcoin Mining. Retrieved from https://www.vice.com/en_us/article/8xk4e4/bitcoin-ban-plattsburgh-coinmint-mining on January 18th 2020.

[17]. Okafor, P. (2019). Electricity: National grid suffers 6 system collapses in 4months. Retrieved from https://www.vanguardngr.com/2019/04/electricity-national-grid-suffers-6-system-collapses-in-4months/ on 18th January 2020.

[18]. Page S. (2018). Mining Bitcoin is as energy intensive as mining gold.https://cosmosmagazine.com/ technology/mining-bitcoin-is-as-energy-intensive-as-mining-gold.Retrieved on January 18th 2020.

[19]. Radiflow, 2018. Detection of a Crypto-Mining Malware Attack at a Water Utility" https://radiflow.com/wp-content/uploads/CS-Radiflow-CyberMining-071420.pdf. Accessed on the 12 July, 2021

[20]. Ranger S. (2019). Cyberattacks: China and Russia can disrupt US power networks warns intelligence report. Retrieved from https://www.zdnet.com/article/cyber-attacks-china-and-russia-can-disrupt-us-power-networks-warns-intelligence-report/ on 19 January 2020.

[21]. Sanni, S.O. (2019). Nigeria: Crypto Currency In Nigeria: Regulatory Framework & Related Issues. Retrieved from http://www.mondaq.com/Nigeria/x/855410/fin+tech/Crypto+Currency +In+Nigeria+Regulatory+Framework+Related+Issues on 18th January 2020.

[22]. Simmons, D. (2019). Cyber-attacks 'damage' national infrastructure (2019). Retrieved from https://www.bbc.com/news/technology-47812479 Retrieved on 19 January 2020

[23]. USAID (2019). Nigeria Power Africa Fact Sheet.https://www.usaid.gov/ powerafrica/nigeria. Accessed on 21st April,2021.

[24]. Saad M., Khormali A. & Moheisen A. (2018). "End-to-End Analysis of In-Browser Cryptojacking". https://arxiv.org/pdf/1809.02152.pdf. Accessed on 20th June, 2021

[25]. Sheridan K. (2018). 25% of Businesses Targeted with Cryptojacking in the Cloud. Retrieved from https://www.darkreading.com/cloud/25--of-businesses-targeted-with-cryptojacking-in-the-cloud/d/d-id/1331813 on January 18, 2020.

[26]. Stu S. (2019). 90 percent of Critical Infrastructure hit by cyberattacks.https://blog.knowbe4.com/90 -percent-of-critical-infrastructure-hit-by-cyberattacks?hs_amp=trueAccessed on 19th January 2020

[27]. Hanibal Goitom, 2018. "Our New Reports on Regulation of Cryptocurrency Around the World".The Law Library of Congress. (2018). Washington D.C: United States of America. https://blogs.loc.gov/law/2018/07/our-new-reports-on-regulation-of-cryptocurrency-around-the-world/. Accessed on 12th August, 2021

[28]. Vincent J. (2019). Bitcoin consumes more energy than Switzerland, according to new estimate. Retrieved from https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison on January 18 2020.

[29]. Wahab, B. (2019). Nigerians in darkness as national grid collapses for 11th time in 2019. https://www.pulse.ng/news/local/blackout-as-national-grid-collapses-for-11th-time-in-2019/pggqqsb.Accessed on 18 January 2020.

[30]. Wahab, B. (2020). Nigerians have been thrown into darkness again as the national electricity grid records its first collapse in 2020. https://www.pulse.ng/news/local/ nigerians-in-darkness-again-as-national-grid-collapses-as-usual/gktbd75Accessed on 18 January 2020.

[31]. Zmudzinsky, A. (2019). China passes first ever crypto law going into effect January 2020. Retrieved from https://cointelegraph.com/news/china-passes-first-ever-crypto-law-going-into-effect-january-2020 on 19 January 2020.

[32]. CISA, 2019, "A Guide to Critical Infrastructure Security and Resilience", Cybersecurity and Infrastructure Security Agency, United States Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf. Accessed on 2nd September, 2021

[33]. JCNSS, 2018. "Cyber Security of the UK's Critical National Infrastructure". Joint Committee on the National Security Strategy, House of Lords and the House of Commons https://publications.parliament.uk/ pa/jt201719/jtselect/jtnatsec/1708/1708.pdf. Accessed on 2ndApril, 2021

[34]. ONSA, 2021. "National Cybersecurity Policy and Strategy" Office of the National Security Adviser. http://ctc.gov.ng/wp-content/uploads/2021/02/national-cybersecurity-policy-and-strategy-2021_e-copy_24223825.pdf. Accessed on 2ndSeptember, 2021.

[35]. Ponemon Institute, 2018 "Measuring & Managing the Cyber risks to business operations". Ponemon Institute LLC Publication, copyright 2018 tenable, Inc. https://lookbook.tenable. com /ponemonreport/ponemon-report-2018. Accessed on 4th September, 2021.

[36]. Krause, M.J., Tolaymat, T. Quantification of energy and carbon costs for mining cryptocurrencies. Nat Sustain **1,** 711–718 (2018). https://doi.org/10.1038/s41893-018-0152-7 . Accessed on 4th September, 2021.

[37]. Marshmclennan,2018. "Mining for Virtual Gold: Understanding the Threat of Cryptojacking. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2018/sep/Mining%20for%20Virtual%20Gold_%20Understanding%20the%20Threat%20of%20Cryptojacking.pdf. Accessed on 4th September, 2021