INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, MANAGEMENT, PEACE AND CONFLICT RESEARCH (IJSMPCR)
Journal homepage: https://ijsmpcr.com/

Impact of DDoS attacks on critical national information infrastructure and human security in Nigeria

BY
[1]ZWINGINA Kabrah., [2]AMB. ENIKANOLAIYE Sola., [3]ZAMANI Andrew Prof., [4]IGWEBUIKE Paul Ozoemene., [5]IRABOR Beatrice Isi., [6]MARGWA Rifkat., [7]ONIBIYO Ezekiel R
[1]Ministry of Interior, Abuja
[2]Ministry of Foreign Affairs
[3&7]Al-Mustapha Peace and Development Initiative (APUDI)
[4,5&6]Nigeria Security and Civil Defence Corps, NHQ, Abuja

International Journal of Social Science, Management, Peace and Conflict Research, 2024, 01(04), 069–084
Publication history: Received on 29 July 2024; Revised on August 18, 2024; Accepted on 28 August 2024

The unprecedented performance reliance of modern society on critical national information and infrastructure (CNII); financial system, electoral system, stock exchanges, clearing system, crypto currency exchanges, data networks, and satellite communication systems, have opened up States to opportunities and threats from forms of cyber-attacks, whose consequences could negatively influenced economic and societal implications. This study decomposed human security into economic and societal implications. It was against this background that this study engaged economic theory to examine impact of distributed denial of services (DDoS) attacks on CNII in Nigeria and human security. This study employed qualitative research design with reliance on publicly available archival documents and examining literature that relates to cyber-attacks, CNII, DDoS threats, and human security. Findings from empirical literature revealed that there exist economic impact of DDoS attacks on CNII in Nigeria. These ranges across financial losses, operational disruptions, and skewed economic development, while societal consequences of DDoS attacks spanned and seen on disruptions of public services, erosion of public trust, and social implications of cyber incidents. This study recommended that the ministry of interior and office of the National Security Advisers should formulate and implement robust cybersecurity policies through constellations of cyber security industry experts, private sector, academia, civil society, NSCDC as lead agency for protection of CNAI, and Satellites driven agencies towards prevention, detection, response, and recovery strategies on challenges posed by DDoS attacks on financial and societal implications linked to CNII in Nigeria. The study further recommended that all tiers of government should deepen cybersecurity awareness, targeting industries, government officials, IT professionals, education sectors, and the general public to promote best practices to foster a culture of cybersecurity resilience. Such awareness should be fortified with investment in cutting-edge cybersecurity technologies and threat intelligence platforms to bolster the resilience of Nigeria's CNII. **Keywords:** Critical National Information Infrastructure, DDoS Attacks, Economic Theory, Human Security

Introduction

The digital age has ushered in an unprecedented level of reliance on critical national information infrastructure (CNII) for the functioning of modern societies (Chaudhuri & Kahyaoğlu, 2023; Adetoye et al., 2013). While this technological advancement has brought numerous benefits, it has also opened up new avenues for malicious actors to exploit vulnerabilities and launched cyberattacks (Mazzolin & Samueli, 2020). The impact of such attacks on critical infrastructure can be devastating, threatening economic prosperity, investors' confidence, social well-being, and national security of countries around the world (Riggs et al., 2023). Nigeria is not insulated from this world order, having also been rated third in global internet crimes and attacks (National Communication Commission, 2017).

*Corresponding author: **Zwingina et al.**
Mininstry of Interior, Abuja, Nigeria

Cyber attacks on critical information infrastructure can take various forms, from disrupting essential services like internet service provision, electoral system, internal security, electricity, transportation, and communication, to compromising sensitive data and financial systems (Mungadi et al., 2021; Riggs et al., 2023). The collective impact of these attacks drain innovation, negatively impact the economy, and commerce without necessarily reaching the threshold that would trigger a meaningful government or commercial response (Mazzolin & Samueli, 2020). The global character of information system vulnerabilities poses a severe challenge to both national governments and the private entities responsible for critical infrastructure (Lukasik et al., 2003). This lack of understanding and preparedness By governments and industries on the extent and integration of the "web" on which their infrastructure relies, leaves critical systems susceptible to a wide range of threats, including unintended incidents, criminal activities, terrorist attacks, and even malicious acts by adversarial foreign nations (Warfield, 2012).

The potential for these cyberattacks particularly of DDoS cause significant damage to a country's economy and societal well-being is well-documented (Riggs et al., 2023). DDoS attacks on CNII are becoming more prevalent globally, targeting essential systems such as government networks, financial institutions, healthcare facilities, and energy grids. DDoS attacks can disrupt critical services and operations, leading to downtime, financial losses, and reputational damage for organizations and governments relying on CNII. DDoS attacks on CNII can have significant economic repercussions, causing loss of revenue, increased operational costs, and potential long-term damage to the affected country's economy. DDoS attacks on CNII can have far-reaching societal effects, disrupting public services, undermining trust in government institutions, and impacting citizens' access to essential services such as healthcare, education, and emergency response systems. These attacks on CNII pose national security risks by compromising sensitive data, disrupting critical infrastructure, and potentially enabling adversaries to achieve political or strategic objectives through cyber warfare (Long, 2024).

In the same year, 14% of the over 90 million Nigerians internet users suffered a form of cyberattack. According to a report, cyberattacks cost the Nigerian economy about $500 million per annum. According to the FBI's Internet Crimes Report in 2016, Nigeria ranked 19th on top countries by cybercrimes victims. According to Delloite's 2018 Nigeria Cyber security Outlook, it is projected the country will witness increased DDoS ransom ware, attackers will turn to Crypto currency, increased attack on cloud facility, and Internet of things (IoT) compromise. In a 2016 report, Serianu reported that Nigerian e-Commerce platforms were hit with more online scams, there was Automated Teller Machine (ATM) Skimming and Identity theft, and customized malware targeting critical mobile and Internet banking infrastructure.

Critical National Information Infrastructure (CNII) has become an indispensable part of modern society globally, and effectively protecting it has significant implications for nations worldwide. However, developing countries, including Nigeria, face substantial challenges in safeguarding their Critical Information Infrastructure (CII) and remain vulnerable to cyber threats. The rapid advancement of technology, especially the growing reliance on Information and Communication Technology (ICT), has further heightened the risks of cyberattacks in these infrastructures (James, 2023). The integration of traditional Critical Infrastructure with cyberspace has blurred the distinction between the two, giving rise to Critical Information Infrastructure (CII) (Mbanaso et al., 2020).

CII encompasses elements of cyber risk and has become a prime target for cyberattacks, with Distributed Denial of Service (DDoS) attacks being particularly prevalent. Safeguarding CII is of paramount importance for developing nations like Nigeria, as it profoundly impacts various aspects of society and the economy. The increasing reliance on cyberspace capabilities underscores the critical role played by CII in the functioning of modern societies (James, 2023).The characterization of CNIs is increasing due to rapid urbanization and population growth, and is becoming a key requirement for the development of any modern society and the economy (Srinivasu and Islamia, 2013). Although there are similarities in such infrastructures globally, every nation determines the value to attach to each infrastructure depending on its developmental goal, priorities and the level of dependency on such infrastructure. Several countries identified Electricity, Telecommunications, Water, Transportation, Health, Education as Critical Infrastructure (CI). Twelve countries categorised food, financial services and civil administration as CS (Mbanaso et al., 2019).

DDoS attacks are a common type of cyberattack that specifically target the availability of systems rather than breaching them with malware or viruses. Hackers initiate DDoS attacks by overwhelming networks or servers with fake traffic, rendering the system unable to respond to genuine user requests. Such disruptions incapacitate CII from providing services to customers. Cybercriminals may also attempt to extort money by launching a minor DDoS attack as proof of their capability to breach a target system and then threaten to initiate a ransomware attack. They may demand payment in cryptocurrency, which is difficult to trace. Threats to critical infrastructure, financial institutions, government entities, and service providers have been prevalent in the cyber threat landscape in recent years (Akintaro, 2023). According to the Annual Industry Survey (2022), 29% of the over 2,000 submissions from different organizations reported falling victim to a DDoS attack and network breach in the past year alone. DDoS attacks were considered a major threat to organizations and their revenue streams, ranking closely behind malware and fraud as the most common security incidents (Annual Industry Survey, 2022).

The Nigeria Security and Civil Defence Corps (NSCDC) is the lead agency for the protection of Critical National Assets and Infrastructure (CNAI) which is a wider subset of CNII and the agency is domicile in the Ministry of Interior in Nigeria withy primary concerns of protecting the internal affairs of Nigeria against subversive criminal elements. This concern also falls under the purview of the Office of the National Security Adviser. The responsibilities of these government functionalities cannot be ignored in marshaling constellations of agencies for the protection of CNII in Nigeria against cyber threat.

However, juxtaposing global investigations with the Nigerian context highlights a significant void. The lack of localized research undermines a holistic understanding of the nuanced intricacies surrounding DDoS attacks on CNII within Nigeria (Adebayo & Adeyemi, 2023). Herein lies the significance of the current study, which aspires to shed light on the unique challenges, vulnerabilities, and consequences intrinsic to the Nigerian landscape. This research strives to transcend these limitations by methodically dissecting vital sectors, such as energy, transportation, telecommunications, and finance, offering an intricate analysis of the implications of DDoS attacks on CNII in Nigeria. Looking more closely, DDoS attacks' impact on the transportation sector necessitates particular attention. Smithson et al. (2020) argue that transportation systems' interconnectivity amplifies vulnerabilities to cyber threats.

Research Questions

This study provides answer the following research questions to adequately investigate the impact of cyberattacks on critical information infrastructure in Nigeria.

i. What are the economic implications of DDoS attacks on CNII in Nigeria?
ii. What are the societal implications of DDoS attack on CNII in Nigeria?

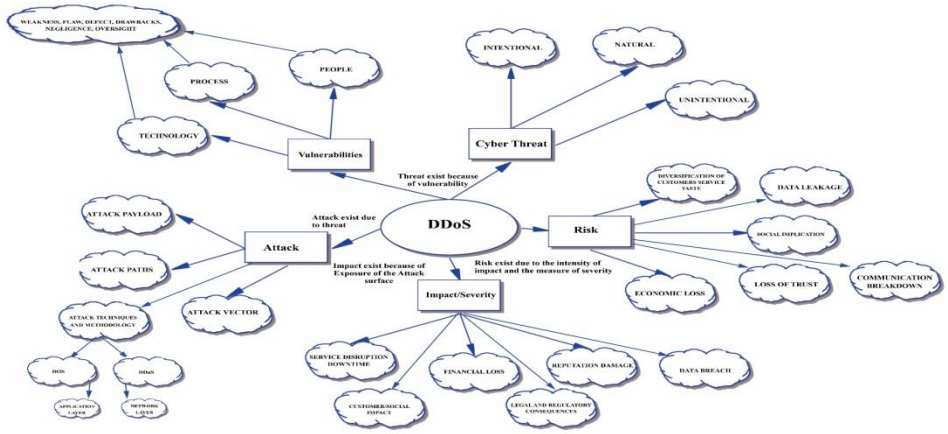
1. Literature Review

Conceptual

Distributed Denial of Service

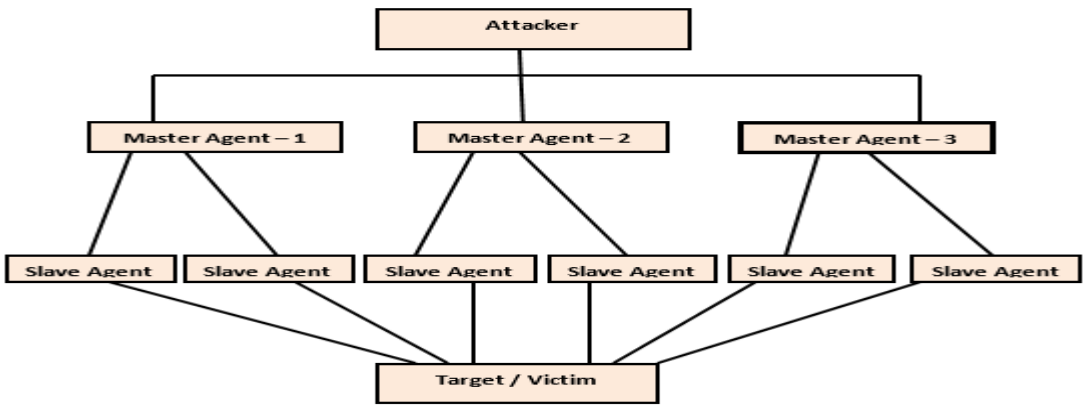
Distributed Denial of Service (DDoS) attack is a type of attack in which an attacker creates a large effect on the target by multiplying the influence of attack derived from a large number of computer agents (Vivek & Omer, 2021). The attacker controls a large number of computers over the internet before attacking. The attacker utilizes the weakness of these computers by using some hacking techniques or by inserting malicious code so as to put these Computers under his control. These computers are usually called zombies. The group of zombies is termed as botnet. The magnitude of the attack depends upon the size of the botnet (Zhang et al., 2011). The larger the botnet, the more disastrous and severe will be the attack. In a botnet, handlers are chosen by the attacker that perform control functions and pass all the guidelines of the attacker to the zombies and also the information that they receive from zombies to the attacker about the victim under each handler there is a group of zombies and these handlers communicate with the zombies and the

attacker (Zhang et al., 2011). Zombies and the handlers are the machines from the public network but the users of these machines do not know the fact that these computers are used as botnet.



DDoS Attacks Spread

DDoS attacks are continuously evolving as hackers strive to outdo each other in hours of downtime, and they pose significant risks to CII in sectors such as transport, power, finance, and telecommunications (Embroker Team, 2023). Nigeria, South Africa, and Kenya are among the top 100 countries globally facing online threats. Nigeria ranks 50th, South Africa ranks 82nd, and Kenya ranks 35th on the global list (Akintaro, 2023). The number of DDoS attacks increased more than 4.5 times in 2021 compared to previous years (Kaspersky, 2022). Norton's statistics also indicate that DDoS attacks are on the rise, with a 14% increase in recent years (Stouffer, 2022).



A Typical DDoS Attack Structure (Shankar et al., 2013)

Vulnerabilities

Vulnerabilities of critical infrastructures have increased with the widespread use of information technologies. As Critical National Information Infrastructures are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for any organization as well as nation. The risks to continued operations from failing to upgrade ageing infrastructures or not meeting mandated regulatory

regimes are considered higher given the demonstrable impact of such circumstances. Due to the rapid increase in sophisticated cyber threats targeting critical infrastructures with significant destructive effects, cybersecurity of critical infrastructures has become an agenda item for academics, practitioners, and policy makers. Attacks to such critical systems include penetrations to their network and the installation of malicious tools or programs that can reveal sensitive data or alter the behaviour of specific physical equipment. A holistic view, which covers technical, policy, human, and behavioural aspects, is essential to handle the cybersecurity of critical infrastructures effectively.

Vulnerabilities stand as the foundational element within the conceptual framework of DDoS attacks on Critical National Information Infrastructure (CNII). These vulnerabilities encompass a wide spectrum of weak points and susceptibilities that exist within the intricate fabric of modern digital systems. They can be considered as chinks in the armour of otherwise sophisticated and interconnected technology ecosystems.
In the landscape of CNII, vulnerabilities emerge as inherent attributes or as a result of defects, weaknesses, or negligence in the design, implementation, and management of information systems (Islam et al., 2022). They can stem from outdated software, un-patched applications, misconfigurations, and even human errors. Visualizing vulnerabilities within the framework as the starting point accentuates their pivotal role in shaping the subsequent variables. As digital systems become more complex and interwoven, new vulnerabilities may arise, potentially magnifying the threat landscape (Ogunleye et al., 2022). The dynamic nature of vulnerabilities necessitates constant vigilance, regular system assessments, and continuous updates to mitigate their potential exploitation.

Cyber Threats

a. Internal Threat

It is defined as "One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm." Insider betrayals cause losses due to IT sabotage, fraud, and theft of confidential or proprietary information. This may be intentional or due to ignorance.

b. **External Threat:** Arise from outside of the organization by individuals, hackers, organizations, terrorists, foreign Government agents, non-state actors and pose risk like Crippling CII, Espionage, Cyber/Electronic warfare, Cyber Terrorism etc.

Cyber threats materialize as malicious actors exploit identified vulnerabilities to breach systems, infiltrate networks, and compromise sensitive data (Islam et al., 2022). This transition from vulnerabilities to cyber threats marks a pivotal shift in intent and action, transforming latent weaknesses into active risks. Cyber threats are dynamic and diverse, stemming from an array of sources and motives. These threats can range

from cybercriminals seeking financial gain through attacks on critical sectors like finance and energy, to state-sponsored entities aiming to undermine national security by disrupting essential services (Ogunleye et al., 2022). Hacktivists may exploit vulnerabilities to advance their socio-political agendas, while insider threats can exploit their privileged access to compromise systems from within.

c. Attack

As the conceptual framework unfolds, the variable of attack assumes a pivotal role in the progression from cyber threats to the tangible impact of Distributed Denial of Service (DDoS) attacks on Critical National Information Infrastructure (CNII). Attacks represent the culmination of intent, strategy, and execution by malicious actors seeking to exploit vulnerabilities and capitalize on identified cyber threats.

An attack in the context of DDoS refers to the deliberate and concerted effort by cybercriminals and threat actors to overwhelm targeted systems, networks, or applications with a flood of malicious traffic. This influx of traffic, often originating from a botnet a network of compromised devices results in a significant increase in network and system resource consumption. The sheer volume of incoming requests exhausts the target's processing capabilities, rendering it unavailable to legitimate users and disrupting essential services.

d. **Impact/Severity**

Impact and severity collectively represent the tangible consequences and disturbances wrought by successful DDoS attacks, transitioning the theoretical landscape into real-world disruptions. DDoS attacks wield a multi-dimensional impact that reverberates through various layers of CNII. The term "impact" encapsulates the measurable ramifications of an attack on critical sectors such as energy, finance, telecommunications, and transportation. These effects span a spectrum, ranging from localized service unavailability to wide-reaching disruptions that traverse and imperil numerous interconnected sectors.

On the other hand, "severity" gauges the magnitude of the consequences arising from DDoS attacks (Jones & Martinez, 2021). It assesses the extent of the disruption, the financial losses incurred, and the societal turbulence left in the wake of the attacks. A higher severity rating signifies far-reaching and profound negative outcomes, encompassing not only immediate operational disturbances but also economic losses, compromised safety, and public inconveniences (Sullivan & Kim, 2020).

e. Risk

The variable of risk occupies a critical juncture within the conceptual framework illustrating the impact of Distributed Denial of Service (DDoS) attacks on Critical National Information Infrastructure (CNII) (Brown et al., 2020). Risk embodies the culmination of vulnerabilities, cyber threats, potential attacks, and the resulting impact/severity, encapsulating the potential for harm and disruption that DDoS attacks pose to CNII.

Risk, in the context of DDoS attacks, signifies the likelihood of vulnerabilities being exploited, cyber threats being actualized, and attacks materializing, leading to tangible impacts and severities (Brown et al.,

2020). It's the amalgamation of uncertainties that accompanies the interconnected elements within the framework, reflecting the potential for adverse outcomes. The risk factor is inherently dynamic and fluid, as it adapts to changes in technology, threat landscape, and organizational defenses.

Critical National Information Infrastructure

Critical National Information Infrastructure (CNII) is described as those ICT infrastructures that are dependent on core assets that are important for the running of the organization. Such that, if such assets are compromised, it has disastrous effect on national security, government, the economy, and the country's overall status (Aladenusi, 2015). Food and agriculture, dams, financial services, oil and gas, commercial facilities, communication, defense, emergency services, power and energy, government and facilities, information technology, healthcare, transportation systems, and water and sanitation are among the 15 industry sectors defined as critical information infrastructure in Nigeria, according to Aladenusi (2015). The importance of critical infrastructure in nation-building is demonstrated by the fact that critical information infrastructures are interdependent on a large number of services and infrastructure, and the failure of any of these CII infrastructures causes a catastrophic domino effect that negatively impacts other services

Financial Critical National Information Infrastructure

DDoS (Distributed Denial of Service) attacks can target various types of financial critical national information infrastructures. DDoS attacks can disrupt online banking services, preventing customers from accessing their accounts, making transactions, or using digital banking services. Attacks on stock exchanges can disrupt trading activities, leading to market volatility and financial losses for investors and institutions relying on real-time trading data. The Nigeria Stock Exchanges is not insulated from a DDoS attacks. The **Payment Gateways are also susceptible through** disruption of e-commerce transactions, preventing businesses from processing payments and causing financial losses.

Attacks on clearinghouses and settlement systems can disrupt the process of reconciling transactions and settling payments between financial institutions. DDoS attacks on insurance systems can disrupt claims processing, policy management, and customer services, impacting the operations of insurance companies and their clients. DDoS attacks targeting financial regulators can disrupt regulatory oversight activities, hindering their ability to monitor and enforce compliance within the financial sector. Attacks on financial news websites and services can disrupt the dissemination of market news, analysis, and financial information, affecting investor sentiment and decision-making. Interestingly, DDoS attacks on cryptocurrency exchanges can disrupt trading activities and the ability to buy, sell, or transfer digital currencies, impacting both investors and users of cryptocurrencies.

Due to their dependent on digital infrastructures, (Muhammad et al., 2023) developing a framework for information security to protect financial institutions from DDoS attacks. The research suggested that financial institutions must implement an information security framework consisting of risk assessment, policies and procedures, robust network infrastructure, employee training, incident response procedures, continuous monitoring and testing, and business continuity plans in order to prevent DDoS attacks. By implementing these, financial institutions can safeguard their systems, consumers and reputation. DDoS attacks are launched almost every day. Even the most prominent Websites like Twitter, Facebook, Google couldn't escape themselves from being hit by it, which caused millions of their users affected (Ketki et al., 2011). Even the develop countries were not safe, including White house, Federal Trade Commission and the US Department of the Treasury. Washington Post and the New York Stock exchange, NASDAQ. Where a Botnet comprising of 30,000 – 60,000 infected computers were used, the attack traffic consumed 20-40 gigabytes of bandwidth per second.

Telecommunication Critical National Information Infrastructure

The vulnerability of telecommunications network of High-speed internet connections, fiber optic cables, and wireless networks can be targeted by DDoS attacks to disrupt communication services. These networks include voice and data networks that facilitate communication between individuals and organizations. A DDoS attack targeting the core routers of a national telecommunication network, disrupting voice and data services across the country. In 2019, a DDoS attack on a major US internet service provider's backbone network caused widespread internet outages across the country (Satter, 2023). Another vital platform susceptible to disruptions are the Internet Service Providers (ISPs), a vital components of the telecommunication infrastructure, providing internet connectivity to users. An attack targeting the DNS servers of a major ISP, causing widespread internet outages in a region.

Satellite communication systems play a crucial role in providing connectivity in remote or underserved areas. A targeted DDoS attack on the ground station of a satellite communication provider, affecting communications for critical services such as emergency response or military operations. **Mobile Network Operators (MNOs)** provide cellular services to mobile users, connecting them to voice and data services. A DDoS attack on the signaling infrastructure of a mobile network operator, leading to network congestion and service disruptions for millions of subscribers. **Law Enforcement Critical Communication Infrastructure,** includes emergency communication systems, such as those used by law enforcement, fire departments, and emergency medical services. A targeted DDoS attack on the emergency communication network of a city, disrupting first responder operations during a crisis situation.

Empirical Review of Previous Studies

As contained in Zayo Group's 2023 annual report on distributed denial of service (DDoS), where it was stressed that DDoS attack is a deliberate cyberattack against an organization's online presence Zayo (2023).

The report analyzes more than 70,000 threat detections and mitigations experienced by Zayo customers across 14 industries and regionally across North America and Western Europe between January 1 and June 30, 2023. It was found out that telecommunication companies experienced more DDoS attacks than any other industry where it said to grow to 1,175% in the 1st and 2nd quarter of 2023 over the past year. This finding is corroborated by that of Vivek and Omer (2021), who also in their report discovered massive DDoS attacks in the telecommunication sector.

Furthermore, the financial industry faced numerous cybersecurity attacks. At 5.85 million dollars, the mean cost of cybercrime in the financial services business is also among the highest of any industry (Najaf et al., 2020, Bossler, 2021). It has compelled financial institutions like banks and insurance firms to continue providing online assistance to their customers. Again, the majority of employees worked from home in an insecure network. Once employees are at work, they are bound by certain security measures, which were not there before and which became the new normal practice. Employees were more vulnerable to cyber risks when using an insecure network (Babulak et al., 2020). Customers increasingly rely on online banking, which exposes them to hackers. Hackers commonly target the financial sector with distributed denial of service (DDoS), phishing, and malware cyberattacks. ATM transactions (Omolara et al., 2019) were visited by hackers that stole bank credit cards to withdraw money. During the Covid-19 crisis, there was an increase in credit card fraud (Zhu et al., 2021; Payne and Morgan, 2020). Therefore, there is an urgent need to protect data from intruders by developing a hybrid cipher (Omolara et al., 2014) and up-to-date safe encryption algorithms to secure data in online transactions.

In the case of insurance firm cyber-attack, the Avaddon gang attacked the European insurance business AXA in May 2020. The incident occurred shortly after the corporation announced significant insurance policy modifications. In essence, AXA said it would no longer reimburse many of its clients for ransomware charges. The hacker group acquired access to a colossal 3 TB of data in this one-of-a-kind (and rather ironic) threat on a cyber-insurance corporation that made the news. Another significant insurance firm was hit by ransomware earlier in March 2020. In March 21, 2020, a hacker group targeted CNA's network, encrypting 15,000 devices, including many computers used by remote employees. The hacking group Evil Corp is suspected of being behind the attack, which uses a new strain of malware known as Phoenix CryptoLocker.

Williams et al. (2015) predict the effects of DDoS Attacks on a Network of Critical Infrastructures, the research utilized several machine learning techniques including support vector machine, K-nearest neighbour, decision trees, among others. The results showed that the classifiers are able to identify behavioural changes, with a mean average of 62.96%. The specificity results, however (attack behaviour

changes) were less-successful; with only 2, (SVC and PolyC) able to identify 100% of abnormal behaviour occurrences.

Mungadi et al. (2021) investigated the vulnerability of Nigeria's critical national asset and infrastructures during the nationwide Endsars cyber warfare protest. The study employed triangulation research design with purposive and snowballing sampling techniques and regression for data analysis. Findings from the study showed that the nation's information and financial infrastructures were extensively overwhelmed during the protest to no avail with both NARSDA nor NITDA helpless in rescuing the penetration of the hackvisit. Study submitted that more need to be done in the protection of CNAI as cyberwarfare is beyond rhetoric. Study did not consider cybersecurity policy nor legal framework but limited to critical national assets

Maitanmi et al. (2013) investigated the impact of cybercrimes on Nigeria economy by probing the level of awareness of individuals on cybercrimes and its impact on Nigerian economy. Study engaged survey research design with administered questionnaire. Analysis showed that pornography, software piracy, and cracking are among others prevalent cybercrimes in Nigeria. Study was on the economy with no focus on financial telecommunication sector which this study captures in order to arrive at a robust conclusion. A notable example, the research by Islam et al. (2022), delved into DDoS Attacks in an IoT-Based Monitoring System of the Banking Sector Using Machine Learning Models. Their study, primarily focused on the financial sector, demonstrated the dominance of support vector machines over alternative algorithms. Despite its sector-specific focus, the findings underscore the intricate interplay of DDoS attacks across various domains.

Oaikhena (2022) interrogated the embryonic stage of cyber liability insurance in Nigeria in a qualitative study. Study submitted that there is the need to take a more proactive approach to cyber-security now that cyber insurance brokers and lawyers start to serve as risk advisors and partner to business whose large chunk of operations depends on technology, hence exposure to cyber risk heightened. In a similar study Tijani and Oloyede (2020), investigated cyber Insurance in Nigeria and her risk hedging capabilities in an increasingly threatened landscape. Study corroborated the nascent stage of cyber liability in Nigeria such that finding revealed that top ten insurance firm had no provision in their financial statement for cyber liability policy. Studies in this regard was limited to financial service sector while this study extends to the telecommunication sector.

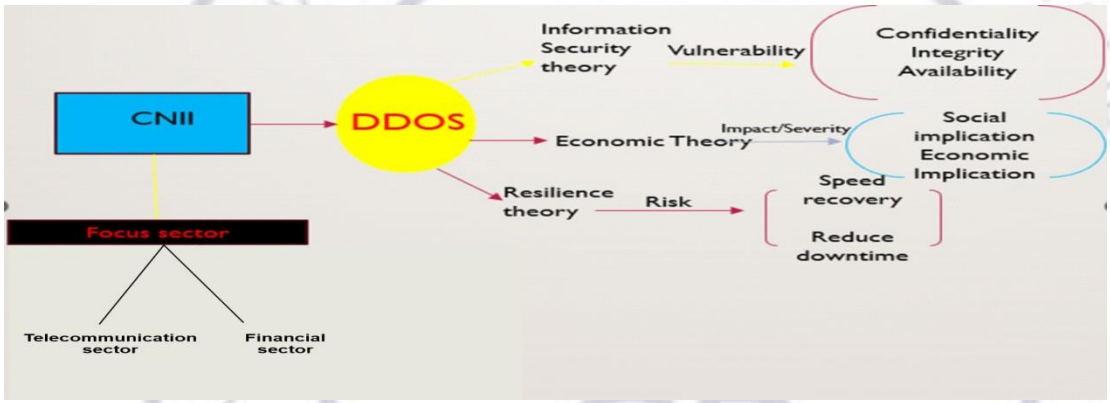
Gavou et al. (2024) engaged survey research design to interrogate cyber threats from innovative technologies in North Central (Middle Belt) Nigeria. The study engaged goggle documents to administer on 200 purposefully sampled respondents in the Middle Belt Nigeria using innovative technologies for their

daily jobs including crime agencies. Major findings revealed that serious steps are needed to better secure the cyberspace against cybercrimes, threat, and regular update of software, use strong password, back up data and information, produce strong cybersecurity policy. The study submitted that cybercrime has extraordinary societal implications for individuals, organizations, societies, and governments.

Theoretical Review

Economic Theory

Within the discourse of comprehending the repercussions of DDoS on Critical National Information Infrastructure (CNII) in Nigeria, Economic Theory emerges as an essential theoretical framework, casting a spotlight on the intricate financial dimensions of Distributed Denial of Service (DDoS) attacks. This theoretical foundation provides a lens through which to delve into the economic ramifications of such attacks, encapsulating both costs and benefits.



Economic Theory offers a structured avenue to dissect the financial intricacies associated with safeguarding CNII against potential DDoS-induced disruptions. It enables a systematic analysis of the expenses incurred in implementing protective measures, juxtaposed with the potential economic losses that could result from successful attacks. Moreover, this theory delves into the motivations propelling cybercriminals to engage in DDoS attacks, unraveling the economic incentives underlying their actions (Varian, 2019). The significance of Economic Theory is manifested in its ability to quantify the economic impact across key sectors of CNII, including power, finance, telecommunications, and transportation (Akintaro, 2023). By quantifying economic costs, this framework equips stakeholders with a tangible understanding of the potential financial toll of DDoS attacks. This understanding, in turn, underscores the importance of prudent investments in robust cyber security measures to mitigate financial vulnerabilities (Granados et al., 2018). Consequently, Economic Theory not only provides insights into the financial implications of DDoS attacks but also guides strategic decision-making by revealing the value proposition of proactive cyber security investments.

Methodology

This study adopts exploratory research design to conduct detailed qualitative analysis of DDoS attacks on CNII in Nigeria through literature review, case studies, data from cyber incident reports and security breach records, engagement with cybersecurity experts, National Information Technology Development Agency (NITDA), the Computer Professionals (Registration Council of Nigeria) CPN, the Central Bank in Nigeria (CBN) as the apex regulatory financial institution, the Nigeria Communication Commission (NCC) in Nigeria to gather insights on cyber threats and their implications on economic and societal effects of DDoS attacks to understand the frequency and severity of DDoS attacks in the Nigerian context. The study relies solely on secondary data. The literature was obtained through searches in publicly available material, literature from non-serial publications, journals, official reports, and conferences particularly if they have been cited by other references in term of cyber threats and attacks, DDoS vulnerabilities, economic and societal implications.

Discussion of Findings

The review of literature of DDoS attacks on CNII revealed that there exist economic impacts of DDoS attacks on CNII in Nigeria ranges across financial losses, operational disruptions, and skewed economic development. The rationale for this could be the inability of the state to give bites to her Child Rights Act after seventeen years of its domestication. The apparent inability to prosecute those flouting the child rights could account for parents selling off or trading their children into child labour economy practices. The finding is in tandem with the findings in the previous works Islam et al. (2022); Oaikhena (2022); Mungadi et al. (2021); Tijani and Oloyede (2020) who found poor investment and attention preparedness in Nigerias resilience against cyber threats particularly DDoS attacks.

The result gotten from empirical literature submits that most there is societal consequences of DDoS attacks on critical national information infrastructure as seen on disruptions of public services and these further deepen the erosion of public trust, and social implications of cyber incidents. The rationale for this finding could be informed by The inability of Nigeria's independent National Electoral Commission to deploy full automation of election transmission amidst scare of cyber threats signifies dearth of collaboration efforts by both public and private sector. This finding is consistent with the findings in the previous work of Gavou et al. (2024) who align with submissions that cyberattacks has societal implications on individual, organisations and government stability.

Conclusion and Recommendations

The study concludes that DDoS attacks on CNII in Nigeria has negative economic impact and also most hidden to cover shallow or dearth mitigation plan and resilience. The study equally concludes that the scare of DDoS attacks do not only exist in Nigeria but that the societal implication was escalated during the 2023

General Election which revealed shallow preparedness by Nigeria Independent Electoral Commission as data transmission was done manually outside the IREV

Based on the conclusions of this study, the following recommendations are made;

i. This study therefore recommends that the ministry of interior and Office of the National Security Advisers should formulate and implement robust cybersecurity policies tailored towards prevention, detection, response, and recovery strategies on challenges posed by DDoS attacks on financial and societal linked CNII in Nigeria. This should be done through constellations of cyber security industry experts, private sector, academia, civil society, NSCDC as lead agency for protection of CNAI, and Satellites driven agencies with dedicated Cyber Incident Response Teams (CIRTs) equipped with expertise and resources to effectively respond to DDoS attacks on CNII in Nigeria.

ii. This study also recommends that the Federal and all tiers of government should deepen cybersecurity awareness campaigns targeting government officials, IT professionals, education sectors, employees, and the general public to promote best practices about cyber threats, and foster a culture of cybersecurity resilience. Such awareness campaign should be fortified with investment in advanced cybersecurity Technologies, deploy cutting-edge cybersecurity technologies such as intrusion detection systems, DDoS mitigation tools, and threat intelligence platforms to bolster the resilience of Nigeria's critical information infrastructure against cyber attacks.

References

Adetoye, A.O., Goldsmith, M., Creese, S. (2013). Analysis of Dependencies in Critical Infrastructures. In: Bologna, S., Hämmerli, B., Gritzalis, D., Wolthusen, S. (eds) *Critical Information Infrastructure Security. CRITIS 2011. Lecture Notes in Computer Science*, 6983. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41476-3_2

Akintaro, O. O. (2023). Cybersecurity Threats and Countermeasures in Africa. In D. Niyato, L. Wang, & Q. Yan (Eds.), *Cybersecurity and Privacy for Smart Cities* (pp. 75-96). Springer.

Akintaro, S. (2023, June 2). Nigeria, South Africa, Kenya face the highest online threats in Africa. Retrieved from https://nairametrics.com/2023/06/06/ nigeria-south-africa-kenya-face-the-highest-online-threats-in-africa-report/. Accessed July 2, 2023.

Aladenusi T. (2015). Nigeria: Nigerian Cyber Security Outlook 2015. Retrieved from https://www.mondaq.com/nigeria/data-protection/451084/nigerian-cyber-security-outlook-2015

Annual Industry Survey. (2022). Telecoms.com Annual Industry Survey 2022 Report. *Telecoms.com intelligence*. Retrieved from https://telecoms.com/intelligencetelecoms-com-annual-industry-survey-2022/. Accessed July 2, 2023.

Babulak E., Hyatt J., Seok, K. K., & Ju J. S. (2020). COVID-19 & cyber security challenges US, Canada & Korea. *Int. J. Trans. Machine Learn. Data Mining, 2020(2),* 43–59.

Brown, S., Lam, R., Parsad, S., Ramasubramanian, S., Slauson, J. (2020). "Honeypots in the Cloud", University of Wisconsin-Madison, Vol.11.

Chaudhuri, A., & Kahyaoğlu, S B. (2023, March 8). Cybersecurity assurance in smart cities: a risk management perspective. *Taylor & Francis, 67*(4), 1-22. https://doi.org/10.1080/07366981.2023.2165293

Embroker Team. (2023, April 17). How to Prevent DDoS Attacks. *Embroker*. Retrieved from https://www.embroker.com/blog/how-to-prevent-ddos-attacks/. Accessed May 16, 2023.

Gavou, T. P., Iliya, J., Ekomaru, C. I., Gusen, J. N. (2024). Cyber security enhancement in Nigeria. A case study of six states in the north central (middle belt) of Nigeria. *American Journal of Humanities and Social Sciences Research, 08*(05), 95-115.

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., Khan, J. A., Rehman, A.U., Shafiq, M. (2022). Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. *Sustainability*, *14*, 8374. https://doi.org/10.3390/su14148374

James, L. (2023, March 20). Energy sector: More cyberattacks in 2022 than ever before. *Power&Beyond.* Retrieved from https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a01oc7a7e-7d3/. Accessed June 23, 2023.

Kaspersky. (2022). DDoS attacks hit a record high in Q4 2021.*Kaspersky*. Retrieved from https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021. Accessed July 2, 2023.

Ketki A., Krishan K., & Monika S. (2011). Impact analysis of recent DDoS attacks. *International journal of Computer Science and Engineering (IJCSE)*. 3(2), 0975-3397

Long, D. A. (2024). *Countering Russian Cybergang Ransomware Attacks Against Critical Infrastructure in the United States* (Doctoral dissertation, National American University).

Lukasik, S J., Goodman, S E., & Longhurst, D W. (2003, August 1). Chapter 5: Strategic Options. *Taylor & Francis, 43*(359), 49-58. https://doi.org/10.1080/714027899

Maitanmi O., Ogunlere S, Ayinde S, & Adekunle Y. (2013): Impact of Cybercrimes on Nigerian Economy. *The International Journal Of Engineering And Science (IJES)* 2(4), 45-51

Mazzolin, R., & Samueli, A M. (2020, August 24). A survey of contemporary cyber security vulnerabilities and potential approaches to automated defence. https://doi.org/10.1109/syscon47679.2020.9275828

Mbanaso, U. M., Kulugh, V. E., & Makinde, J. A. (2020). A framework for determination of critical national information infrastructure in Nigeria. *Journal of Information Science, Systems and Technology, 4*(3), 1-18.

Mungadi, D. D., Kana, A. A., Yusuf, A. U., Owa, F. T., Abubakar, I. A., & Onibiyo, E. R. (2021). Endsars cyber warfare protest and critical national asset and infrastructures in Nigeria. *Infokara Research, 10*(3), 194-208.

Najaf, K., Schinckus C., & Yoong L. C. (2020). VaR and market value of fintech companies: An analysis and evidence from global data. Managerial Finance. 2020

National Communication Commission. (2017). Nigeria ranks third in global internet crimes. (2017, August 23). *The Cable*. Retrieved from https://www.thecable.ng/ncc-nigeria-ranks-third-global-internet-crimes/ Accessed July 21, 2024.

Oaikhena, V. (2022, January 25). Cyberinsurance: The State of Nimbleness in Nigeria. *Mondaq*. Retrieved from https://www.mondaq.com/nigeria/insurance-laws-and-products/1153878/cyberinsurance-the-state-ofnimbleness-in-nigeria

Omolara, A. E., Jantan, A., & Abiodun, O. I. (2019). A comprehensive review of honey encryption scheme. *Indonesian J. Electr. Eng. Comp. Sci. 13*(2):649–656.

Omolara O. E., Oludare A. I., & Abdulahi S. E. (2014). Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication. *Comp. Eng. Intelligent Syst., 5*(5), 34–46.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M A., Amir, A., Vuda, K V., & Sarwat, A I. (2023, April 17). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Multidisciplinary *Digital Publishing Institute, 23*(8), 4060-4060. https://doi.org/10.3390/s23084060

Satter, R. (2023, October 11). Internet companies report biggest-ever denial of service operation. *Reuters*. Retrieved from https://www.reuters.com/technology/internet-companies-report-biggest-ever-denial-service-operation-2023-10-11/Accessed July 23, 2024.

Srinivasu, B., & Islamia, J. M. (2013). Infrastructure development and economic growth: *Prospects and perspective, 2(1*), 81–91.

Stouffer, C. (2022, April 29). DDoS attacks: A simplified guide + DDoS attack protection tips. *Norton*. Retrieved from https://us.norton.com/blog/emerging-threats/ddos-attacks. Accessed July 2, 2023.

Tijani, R., & Oloyede, R. (2020, October 1). Cyber Insurance in Nigeria: Risk Hedging in an Increasing Threat

Varian, H. (2019). 16. Artificial Intelligence, Economics, and Industrial Organization. In A. Agrawal, J. Gans & A. Goldfarb (Ed.), *The Economics of Artificial Intelligence: An Agenda* (pp. 399-422). Chicago: University of Chicago Press. https://doi.org/10.7208/9780226613475-018

Vivek, G., & Omer, Y. (2021). DDoS Attack Trends for 2021 Q1. *The Cloudflare blog*. retrieved from https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1/

Warfield, D. (2012, January 1). Critical infrastructures: IT security and threats from private sector ownership. *Taylor & Francis, 21*(3), 127-136. https://doi.org/10.1080/19393555.2011.652289

William H., Nathan S., Quentin M., (2015). Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures. Thirteenth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'15), Liverpool, United Kingdom. ff10.1109/CIT/IUCC/DASC/PICOM.2015.256ff. ffhal-01314192f

Zayo (2023). Protecting your business from Cyber Attacks: The State of DDoS attacks. *Insight from Q1 & Q2*.

Zhang, J., Luo, X., Perdisci, R., et al., (2011a). Boosting the scalability of botnet detection using adaptive traffic sampling. *Proc. 6th ACM Symp. on Information, Computer and Communications Security*, p.124-134.