Critical National Assets and Infrastructure and National Security Architecture in Nigeria: an Evaluation[1]

Gani Joses Yoroms[2], Obinna Ukaeje[3]

Abstract:

Critical national assets and infrastructure are essential for effective functioning of the state and well-being of the citizens, of which their disruption would have a devastating impact on the state. It is on this premise that the Nigerian government made CNAI a key component of its national security to be protected under the national security architecture. However, despite efforts of the government through the office of the national security advisor, whose responsibility is to coordinate the country's national security architecture, CNAI Protection in Nigeria remains weak, thereby increasing the vulnerability of these infrastructure and national assets to vandalism and attack. Using qualitative research approach and dwelling largely on empirical literature and documented evidence, the paper examined the endangered state of CNAI in Nigeria and the efforts of the federal government toward safeguarding and protecting these vital assets. The paper found out that there is a serious gap between the policies and strategies of ONSA and the implementation itself, which it attributed to challenges like poor coordination, interagency rivalry, and sabotage among others. The paper therefore recommends among others the full implementation of CNAIP Protection Strategy as articulated in the NSS 2019, improve resource allocation for agencies responsible for CNAI Protection, and enhanced cooperation among agencies responsible for the protection of these critical assets.

Keywords:
Critical national assets and infrastructure; national security; national security architecture; vandalism; terrorist attack; sabotage; national security component.

[1] DOI: 10.12700/jceeas.2025.5.4.425

[2] Professor of Political Science, Department of Defence and Security Studies, Centre for Strategic Research and Studies, National Defence College, Abuja, Nigeria; ORCID: 0000-0002-4456-3783; yoromsgani@yahoo.com.
[3] Research Fellow, Department of Defence and Security Studies, Centre for Strategic Research and Studies, National Defence College, Abuja, Nigeria; ORCID: 0000-0002-7231-168X; obinnaukaeje@yahoo.com.

Introduction

Over the past two decades, the Nigerian State has been bedevilled with severe security challenges of threatening lethality and violent fatalities, including terrorism, insurgency, militancy, herders-farmers conflict, armed banditry and kidnapping for ransom, separatist agitations, and vandalism, among others. Apart from the fatalities and threats to life and property they have unleashed on the country, their impacts on Critical National Assets and Infrastructure (CNAI) have been unimaginably huge. They have become targets for attacks by criminal elements, particularly, armed criminal groups including bandits, terrorists, insurgents, separatists, etc., across the country because of their significance to the functioning of the state.

The Nigerian Security and Civil Defence Corps (NSCDC) report released in 2023 revealed that attacks and destruction of schools, buildings and oil installations by criminal elements between 1999 and 2022 were valued at US$200 billion (TVC News, 2023). This, however, did not include the value of destroyed infrastructure through attacks recorded in sectors like power, telecommunication, transport, rail and construction including national assets like electoral offices and police and military barracks and formations in majority of the states of the federation where terrorism, armed banditry, insurgency and separatist movements have remained major security challenges.

Beyond the attack from criminal elements, rioters and protesters have often went for attack and destruction of critical infrastructures and national assets as ways of venting their anger and getting at the government. The "ENDSARS" protest in 2020 for instance, resulted in a massive destruction of infrastructure and assets across the 13 states valued at N200 billion (naira) which is about US$486.4 million (Atlas Magazine, 2021). It recorded an estimated destruction of 234 government facilities and infrastructure, 81 government warehouses and 269 facilities belonging to the private sector (The Guardian, 2020).

Similarly, in 2024, precisely between 1st and 10th of August, the country witnessed another protest, "THE END BAD GOVERNANCE" protest that resulted in another massive destruction of critical infrastructure and national assets across the states of the federation, with an estimate average loss of N350 billion per day (Economist Alaje in Channels TV, 2024). In addition to the cost of the physical infrastructure and assets destroyed and looted, the economic loss to businesses nationwide was huge with severe consequences on not only the economy of the state but also the effective functioning of government and welfare of the people. Both the citizens and the state rely on services from these infrastructures for their socioeconomic well-being – a situation that is capable of compromising the task of nation building in Nigeria.

It is pertinent therefore to evaluate the state of critical national assets and infrastructure protection and national security architecture in Nigeria. This scholarly preoccupation is necessary in order to generate knowledge that may be useful in dealing with the challenges of national security within the contest of CNAI protection in Nigeria. The discussion revolves around the significance of mobilizing the support for effective

CNAI protection in Nigeria. To achieve this, the paper therefore is organized into seven parts. The first is the introductory remark, which provides a background to the study and the methodology of the study. The second is the conceptual exploration of critical infrastructure and national security architecture, as well as the theoretical framework of the study. The third reflects an overview of the endangered state of CNAI in Nigeria. The fourth and fifth reflect the efforts of the government at protecting critical infrastructure and national assets and the challenges hampering government efforts at safeguarding and protecting CNAI, respectively. The sixth explains the relationship between CNAI and national security architecture in Nigeria while the seventh concludes the paper and articulates the way forward.

Methodology

The methodology adopted a qualitative research approach dwelling largely on secondary sources of data. The secondary sources of data collection focused on documented evidence and situational reports from libraries and through social media handles. These sources were analysed using the content analysis technique and findings were presented qualitatively. In addition, a thorough evaluation of pertinent literature on the subject matter was utilized.

Conceptual Exploration

Critical National Assets and Infrastructure

The term "Critical National Assets and Infrastructure (CNAI) was coined by the Nigerian Government to identify the essential physical and cyber systems, networks, and assets that are vital for a nation's functioning and well-being, of which any disruption or loss of their functionality would have a devastating effect on the nation (NSS, 2019). According to the Nigeria Ministry of Interior (2021), they are assets, services and systems that support the economic, political and social life of a nation, such as schools, hospitals, electricity and telecom facilities, oil and gas facilities, transportation amenities like roads, rails, and many others. To ensure their effective functioning, these assets must be protected under the law. The key objective of protecting CNAI as captured in the Nigeria's National Security Strategy (2019) is to secure and protect the nation's vital facilities from threats – both conventional and non-conventional – to ensure the continuous and effective functioning of these assets, thereby supporting national development, economic prosperity, and overall public safety and welfare.

The concept of CNAI is synonymous with the global concept of Critical Infrastructure (CI), a relatively new concept that could be traced to the United States of American Congress Executive Order 13010 of 15 July 1996, which defines critical infrastructure as "systems so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of the United States". The Order identifies eight sectors as critical infrastructure that should be protected under the U.S. National Security Act including telecommunications sector, electrical power sector, oil and gas sector,

banking and finance sector, transportation sector, water supply sector, emergency services sector, and government (US Executive Order, 1996).

However, the concept of critical infrastructure has undergone a redefinition process after the September 11 attack on the United States of America. As a result, the United States Congress through the Patriot Act of 2001 redefines critical infrastructure to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national, economic and social security, and the stability of the economy" (US Patriot Act, 2001). Although both definitions offered by the United States are similar, there is a slight difference; the inclusion of virtual systems and assets which is absent in the first definition. This inclusion is not unrelated to the crucial role of information communication technology (ICT) systems played in the 9/11 attack. Most importantly, while the Executive Order 13010 focused on the essential role of CI, the Patriot Act focuses on the defence of the US CI against terror attacks.

Furthermore, recent global events like the COVID-19 Pandemic which locked down the economy of the world in 2020 and reduced social and economic activities to virtual and the rising cyber security threats have brought a new meaning to critical infrastructure. They influenced the expansion of the sectors designated to critical infrastructure protection to include facilities like public health, information communication technology, manufacturing, nuclear reactors, food and agriculture, and defence industrial base (CISA, 2020). Presently, 16 sectors are globally recognized and designated for protection as critical infrastructure. However, more sectors are likely to be included depending on how crucial they become in the running of the state and their impact on the well-being of citizens.

National Security Architecture

For a comprehensive understanding of national security architecture, it is important to understand what national security means, so as to be able to distinguish between national security and national security architecture. National security is the overarching goal of a state to protect its sovereignty, citizens, and interests from various threats, while national security architecture refers to the institutions, policies, strategies, and structures a nation uses to achieve that goal. In essence, national security is what needs to be protected and why, whereas the architecture is the how, meaning the specific frameworks and components in place to provide that protection. According to David and Salifu (2020), "a nation's security architecture comprises the totality of its constitutional and legal framework, and institutions that form and provide safety and security services for its citizens and the defence of its territorial integrity". The efficacy of a country's security architecture as captured by Saleh (2020) largely depends on the politically led governance system; influenced by a constitutionally mandated defence, security, and intelligence community system, and institutions that are organized, skilfully trained, well equipped, professionally led, and psychologically motivated.

In Nigeria, the management of national security is exclusively conferred on the President, who is the chief executive and commander in chief of the armed forces. The president manages the country's national security through the Office of the National Security Advisor to the president (ONSA), who in turn designs and coordinates the country's national security architecture. The national security architecture in Nigeria encompasses two levels of operation – the external and internal security. Primarily, internal security responsibilities are vested in the Nigerian Police Force (NPF), the State Security Service (SSS) also known as Department of State Security (DSS), the Nigerian Immigration Service (NIS), the Nigerian Customs Service (NCS), the Nigerian Correctional Service (NCoS), the Nigerian Security and Civil Defence Corps (NSCDC), the Nigerian Fire Service (NFS), and the Federal Road Safety Corps (FRSC) (Mbachu in David & Salifu, 2020).

Equally, the protection of the state from external threats is fundamentally the responsibility of the Nigerian Armed Forces. These include military establishments under the Ministry of Defence comprising the Defence Headquarters (DHQ), the Nigerian Army (NA), the Nigerian Navy (NN), the Nigerian Air Force (NAF), the Defence Intelligence Agency (DIA) (Mbachu in David & Salifu, 2020).

The key instruments of law that highlight critical national assets and infrastructure security in Nigeria are the National Security Strategy (NSS)2019 and the Designation and Protection of Critical National Information Infrastructure Order 2024. While the NSS 2019 emphasizes the need for appropriate security strategy for the protection of all CNAIs to ensure their effective functioning for the well-being of the nation, the Designation and Protection of Critical National Information Infrastructure Order 2024 aims to designate, secure, and ensure the continued operation of the information communication systems (ICT) that are integral to the nation's functioning. Nevertheless, both instruments fall within the purview of the national security architecture, thus making CNAI an element of national security to be protected and safeguarded under the national security architecture.

Theoretical Framework

The analysis of this study is anchored on the securitisation theory. Securitization theory is a process of shifting interest from normative to significant security concerns when the life wire of the state faces an existential threat. Holmes (2015) noted that policymakers get confused when they conflate secondary factors defined as social or public health matters with national security. Beyond the secondary factors, national security concerns remain the vital interest or referent object, which, when threatened, the existence of the state is undermined. Therefore, the identification of what is of vital interest to a nation is indeed what explains the Securitisation theory.

In a considerable situation where a referent object faces precarious and existential threats, it is moved from low priority to a high priority level of concern for enhanced strategic attention and protection (Rita, 2006). In this case, decision makers prioritize national security interests in terms of existential threats. Securitisation, therefore, is a

powerful lens through which national decision-makers transform a seemingly ordinary issue into urgent security threats that require extraordinary measures (Otukoya, 2024). Therefore, for a referent object to be placed on securitisation pillar, it must command a priority in the live wire of national survival of a country. It must also require protection and must not be subject to the binding rules and regulations. Whenever a securitizing move is made in a democratic system, existential threats are envisaged.

As Buzan and his Colleagues (1998:24) noted, securitization has to be appropriately addressed to avoid the disruption of the state survival. Or else, the state no longer exits and no one would be alive or be free to deal with a situation that no one would wish it happened (Buzan, et al, 1998). Thus, when a referent object is securitised, it becomes apolitical, operating in the realm of the security threshold. Thus, securitisation of a referent object is an "expanded realm where investing in security enables the state to suspend all democratic requirements and legal norms. It also enables the state actors, their professional security agencies and relevant stakeholders to play important roles in defending the security landscape of the country without having to wait for a legal directive. For instance, as the Nigerian economy grows, the security of critical infrastructure becomes increasingly central to her national security, due to their reliability for the effective functioning of the state (Alex-Adedipe and Okorotie, 2024).

The security and resilience of the national assets and infrastructures are vital to a nation's well-being, affecting not only national security but also the daily lives of the citizens and the overall development of the economy (Hamzat, 2024). Thus, CNAI and security are mutually reinforcing. As much as national security depends on CNAI to function, the latter cannot also exist without the protection provided by the agencies of national security. Any disruption of either of the two will lead to the paralysis of the nation, undermining the economy and by implications placing national security in jeopardy. In addition, revenues derive from CNAI do not only fund national security as the later depends on it (CNAI) to function.

The State of Critical National Assets and Infrastructure in Nigeria

Critical National Assets and Infrastructure in Nigeria, unlike most part of the world have been subjected to attacks by criminal elements be it either non-state armed groups like insurgents, or terrorists, bandits, separatist groups, vandals or rioters. The actions of these various groups have often resulted to the destruction or disruption of the effective functioning of these vital assets thereby affecting the well-being of the state and its citizens. Almost every sector of the economy is affected, from agriculture and energy to finance and technology including the social amenities such as schools, water supply, electricity supply, and healthcare facilities etc. According to the report released by the NSCDC, several sectors in Nigeria are highly vulnerable to attack, including the oil and gas industry, the telecommunication sector, banking sector, education sector and agriculture due to various threats like cyberattacks, banditry, and militant activity (Channels TV, 2021). This explains the endangered state of critical national assets and

infrastructure in Nigeria. Worst still is the threat it poses to the effective functioning and well-being of the state and its citizens.

Given the importance of these assets and facilities to the effective functioning of the country, the federal government has made concerted efforts towards the security and protection CNAI, from the establishment of the NSCDC in 2003 to the inclusion of CNAI as a component of national security in the national security strategy and policy document in 2019, and several other arrangements that aim at enhancing security and protection of CNAI in Nigeria.

Nevertheless, attack and destruction of these vital assets has continued unabated across the country and across several sectors. For instance, in 2020, just less than inclusion of CNAI Protection in Nigeria's national architecture, the ENDSAR protest erupted across the country. During the crisis, an estimated 269 private/corporate, 234 government facilities and 81 government warehouses were vandalized, looted, and burnt across 13 states of the country (The Guardian, 24 March 2020). The estimated economic cost of the loss was at the tune of N200 billion (Naira) valued at US$486.4 million at then by the Nigerian Insurers Association (Atlas Magazine, October 2021). In addition, a report released by the NSCDC in 2023 revealed that attack on CNAIs like schools, buildings, and oil installations from 1999 and 2022 is valued at US$200 billion (TVC News, March 2023). This is suggestive of the negative impact of CNAI attacks to Nigeria's economy.

Beyond the ENDSARS crisis, several sectors have witnessed severe attack on their critical assets and infrastructures. In 2021, the Vanguard Editorial of 27 June 2021 reported a heist by vandals for the struggling Nigeria Railway Corporation as no fewer than five instances of vandalism of the rail trucks: rail tracks and clips were removed by vandals from rail lines across the country. Additionally, the Punch Newspapers of 14 October 2021 reported an interception of a heavy-duty truck conveying no fewer than 970 railway slippers to an unknown destination. This indicates that more efforts need to be done by the intelligence community to prevent the destruction of CNAI from taking place by involving not only human intelligence but also technological intelligence to detect signals on attacks by vandals or natural disaster.

Another sector that has been under constant attack and vandalism is the petroleum sector, with persistent pipeline attack either by oil thieves or militants trying to weaken the economy of the country by disruption oil and gas production output, which is the mainstay of the Nigeria economy. Decades of crude oil theft and pipeline vandalism have constrained the petroleum sector's capacity to meet the OPEC quota of 1.8 million barrel per day (bpd), thus undermining revenue project targets and national growth and development. The Nigerian Extractive Industry Transparency Initiative 2021 report on oil and gas observed that N22.05 billion (Naira) was spent on pipeline repairs and maintenance in six months of 2021 (Tunji, 2023). The Nigerian National Petroleum Company Limited (NNPCL) was also reported to have spent N34.47 billion (Naira) to repair and manage pipelines in 18 months in 2023 (Yoroms and Ukaeje, 2024). Additionally, the NSA, Mallam Nuhu Ribadu while assessing incidents of attacks of oil

and gas pipelines in 2023 few months after resumption as NSA, noted that Nigeria loses US$4 million daily (about 400,000 barrel of crude oil) to crude oil thieves despite efforts to end the menace in the country (Sahara Reporters, 2023).

Another sector that has continued to witness incidents of attack is the power sector. The power sector has been the subject of attack and vandalism by non-state armed groups like bandits, terrorists and vandals, deepening Nigeria's infrastructural deficit and disrupting smooth running of the system and the well-being citizens. The Transmission Company of Nigeria (TCN) for instance reported over 13 cases of vandalism on their transmission facilities across the country, which as a result disrupted electricity supply in many parts of the country (Ogunleye, 2025). The cost of the repair of these facilities was estimated at about N8.8 billion, resulting in frequent power outages in major cities like Abuja, Lagos and Kano during the period (Ogunleye, 2025).

Recent specific incidents that underscored the severity of attacks on electricity transmission infrastructure in Nigeria include, the destruction of transmission towers by vandals along the Katsina-Gazoua axis on 9 January 2025, putting the entire transmission system at risk of collapse, and destruction of 132KV underground transmission cables near Millennium Park, Abuja, disrupting power supply to key areas (Ogunleye, 2025). The consequences of such vandalism are dire because of the contribution of electricity power to economic growth and development. The World Bank explained it better when it noted that vandalism in the power sector is a major threat to Nigeria economy due to its negative effect on the country's GDP. It further noted that it costs Nigeria an estimated loss of about US$429 billion annually (World Bank, 2025). This is suggestive of the critical nature of the power sector to the well-being of the country and the need to ensure its security against any form attack that may affect its functionality.

Another sector that has been a subject of attacks and vandalism is the information and communication technology sector. The rising incidents of information and communication infrastructure theft such as fibre optic cuts, equipment thefts, and vandalization of telecom infrastructure across Nigeria have created uncertainty and doubt around efforts at ensuring the protection of critical national information infrastructure (CNII). The Business Day (2025) report noted that Nigeria's telecommunications sector is facing an alarming surge in sabotage, with an average of 1,744 attacks recorded weekly across the country. This includes approximately 1,100 fibre cuts, 545 incidents of access denial, and 99 cases of theft, posing a significant threat to service quality, network expansion, and national security (Business Day, 2025).

Furthermore, the cybersecurity sector has been bedevilled by threats as exemplified by the rising spate of cyber threats on its facilities. For instance, in 2020, cybercriminals attacked the Central Bank of Nigeria's (CBN) website, resulting in denial of service (The Guardian, 2020). These threats have increased considerably in response to the FGN policies on cashless and digital economy. Nigeria experienced an average of 1.5 million cyber-attacks daily in the run off to the 2023 Presidential Elections with over 6 million attacks on the day of the Presidential Elections (Izuaka, 2023). This is in spite of

concerted interventions such as the enactment of the Cybercrime Prohibition Act (CPA) 2015 and the National Cyber Security Policy and Strategy (NCSPS) 2021 to promote a safe cyber space and enhance CNAI protection in the country.

The above analysis on the state of critical national assets and infrastructure across sectors in Nigeria highlighted the vulnerabilities they face and the concomitance danger such vulnerabilities pose to Nigeria's national security. It is on this basis that we shall look at the efforts of the government towards CNAI Protection in Nigeria.

Government Efforts to CNAI Protection in Nigeria

Although the protection critical national assets and infrastructure was considered important in Nigeria right from independence due to their direct impact on daily life, national security and economic growth. However, its consideration as a top priority on government protection could be formally traced to the creation of the Nigeria Security and Civil Defence Corps (NSCDC) in 2023 through the NSCDC Act 2003. Therefore, the federal government first effort at ensuring effective protection of CNAI was the establishment of the NSCDC.

The NSCDC Act 2003 established the Corps as a full-fledged paramilitary agency to protect lives, property, and critical national assets and infrastructure. However, due to conflict role it crossed path with other security agencies responsible for internal security, thus the Act was reviewed in 2007 to grant full authority to the NSDC as the lead institution for CNAI Protection in Nigeria. The new mandate reflects federal government commitment towards safeguarding and protecting its vital national resources like the energy sector, communication networks, and public transportation (Ukaeje, 2022). Despite this, the issue of conflict of role between the NSCDC and other security agencies like the Nigerian Police Force (NPF) continued to occur, resulting in some instances to clashes during operation. This however created opportunity for vandals to exploit and vandalise national assets and facilities for their financial gains. Experts attributed this challenge as a reflection a lack of clarity on the lead agency responsible for CNAI protection.

To mitigate the challenge of lack of clarity of role and to enhance CNAI protection, the federal government in 2017 through the National Security Advisor's office commenced efforts at considering CNAI as a national security component. Consequently, the slow efforts materialized in the 2019 reviewed and expanded National Security Strategy, a policy document for Nigeria's national security. The NSS 2019 encompassed CNAI as a component of Nigeria's National Security. It also recognized the statutory role of the NSCDC as the agency responsible for CNAI Protection, while ONSA retained the coordinating role. ONSA has the key responsibility of mobilizing other security agencies towards safeguarding and protecting CNAI across the country. This means that the NSCDC as the lead agency is to collaborate with other security agencies on the protection of CNAI.

It is pertinent to note that adoption of CNAI Protection as a component of Nigeria's national security is drawn from the United Nations Security Council Resolution 2341 on

critical infrastructure protection passed in 2017. The UNSC Resolution 2341 urged member states to ensure the protection of critical infrastructure as national security components (UNSC CTC 2341).

Another bold step by the federal government towards enhancing the protection of CNAI especially from attacks by non-state armed groups was the establishment of the National Counter Terrorism Centre (NCTC). The Centre plays a vital role in protecting critical infrastructure by doing the following: coordinating national efforts to combat terrorism and prevent violent extremism, ensuring a unified approach to securing critical infrastructure; facilitates information sharing among government agencies, security services, and international partners to identify and mitigate potential threats; develops and implements strategies to counter terrorism, including analysing threats and vulnerabilities to CNAI such as cyberthreats through regulation, threat analysis, and cyber resilience exercises; and developing frameworks to identify and protect CNAI, particularly in the financial services, telecommunications, and defence sectors (Towoju, 2024).

Another effort at enhancing CNAI protection by the federal government is the validation of a draft: Critical National Assets and Infrastructure – National Protection Policy and Strategy – CNAI-NPPS in 2023 organized by the ONSA and the NSCDC. The Exercise aimed at establishing or consolidating a multi-stakeholder protection partnership for CNAI for the first time in Nigeria at the national level between the coordinating, lead and support agencies as well as other relevant stakeholders from within and outside the shores of Nigeria (Aregbesola, 2023). It is expected that the Draft when approved will provide new policy document for CNAI Protection in Nigeria. However, the document is yet to be approved by the federal government to ensure full implementation of policy.

Another effort at strengthening the safety and security of CNAI by the federal government was the gazetting of Designation and Protection of Critical National Information Infrastructure (DPCNII) Order, No.21 by President Bola Ahmed Tinubu on 24th day of June 2024. This Executive Order makes it an offense to damage critical national information infrastructure, such as telecommunication towers and fibre optic cables, with the goal of ensuring the security and resilience of Nigeria's ICT systems and infrastructure. It specifically covers essential sectors including power, water, telecommunications, banking, healthcare, defence, transport, and emergency services. According to Alex-Adedipe and Okorotie (2024), the Executive Order is seen as a significant step by the FGN to protect its information security framework and maintain national stability.

To further strengthen CNAI Protection, towards the end of 2024, precisely in November, the federal government through the ONSA inaugurated a Federal Coordinating Council on CNAI Protection (FCCCNAIP), consisting of heads of security agencies and other relevant stakeholders, and the National Security Advisor as the chairman (Punch, 2024). The aim is to further strengthen collaboration among the relevant security agencies and stakeholders towards effective protection of CNAI across

the country. This effort situates stakeholders' cooperation and collaboration as a factor in enhancing the protection CNAI for enhanced national security in Nigeria.

Despite the efforts, CNAI remains vulnerable to attacks and vandalism across sector, the case of ongoing vandalism of street lights, sewage covers, electricity transmission towers and fibre optic cables in the federal capital territory, Abuja, where the office of the president and headquarters of all security agencies including the ONSA are located is unimaginable and worrisome. This however is attributed to some key challenges. These are discussed below.

Challenges Militating against Efforts Towards CNAI Protection in Nigeria

Several challenges militate against the efforts of the federal government towards protecting Nigeria' critical national assets and infrastructure. These challenges are identified as follows:

Institutional Capacity Constraints

Security agencies and institutions responsible for CNAI protection lack the required capacity, including the necessary personnel, equipment, funding and training, to effectively protect CNAI across the country. For instance, the NSCDC, the lead agency has serious challenge in the area of personnel, equipment and logistics required for CNAI protection across the 36 states of Nigeria and Abuja, and the 774 local government areas in Nigeria. It was observed that weapons available to the agency are G3 and AK-47, while the criminals are equipped with more sophisticated weapons, making it difficult for the Corps to overcome the criminal during operation in some cases (Ali, et al., 2023). In addition, security operatives protecting oil and gas infrastructures in the Niger Delta region lacks the adequate logistics, particularly vehicles required to match the terrain for effective CNAI protection.

Poor Coordination

The NSDC Act 2007, the NSS 2019, and the DPCNII Executive Order 2024 define and designate responsibilities and roles including accountability to each agency involves CNAI protection. However, this has not been effectively articulated to achieve the objectives of the frameworks towards CNAI Protection due to poor coordination by ONSA. In addition, the act establishing agencies like the DSS and NPF still maintain their superiority over agencies like NSCDC in internal security management including CNAI Protection. This creates problems of interagency rivalry, competition and conflicting institutional priorities among the agencies, leading to delay in intelligence sharing, disjointed operations, reduced effectiveness against threats, eroded public trust and ultimately undermining the collective goal of protecting critical national assets and infrastructure.

Lack of Inter-Agency Cooperation

Lack of inter-agency cooperation among agencies responsible for CNAI protection in Nigeria is one of the major challenges affecting CNAI Protection. It has created a deep-rooted institutional rivalry for dominance and resources, and an unhealthy competition among the security agencies, which has led to fragmented efforts, poor information sharing and operational inefficiency, undermining the security agencies' ability to safeguard critical infrastructure from threats like vandalism and attacks. There is an instance where strategic backup or vital information that would have enhanced the progress and success of a joint task operation on CNAI Protection were held back, leading to the failure of the operation (Ukaeje & Yoroms, 2024). This shows how lack of interagency cooperation can undermine operational effectiveness and success. Thus, there is special need for interagency cooperation for CNAI Protection in Nigeria.

Sabotage

Sabotage connotes a deliberate action aimed at weakening a polity, government, effort, or organization through subversion, obstruction, demoralization, destabilization, division, disruption, or destruction. It severely impacts CNAI security and protection by weakening security measures, fostering institutional corruption, leading to the diversion of funds meant for infrastructure, and creating a pervasive environment of insecurity and fear that hinders effective security governance. This vulnerability allows for the widespread vandalism of assets, oil theft, cyberattacks on government systems, and compromises the overall capacity of the state to deliver security and development. The majority of vandalism and attacks on critical national assets and infrastructures across major sectors like railways, oil and gas, electric power, and telecoms are supported sabotage. A good example is the May 2021 arrest of a syndicate responsible for stealing rail infrastructure in Nigeria by the Nasarawa State Police Commissioner, Mr Bola Longe. Among the arrested syndicate were the Special Adviser to the Nasarawa State Governor on Infrastructure, Mr. Yusuf Musa, police and NSCDC personnel, a local government Supervisory Councillor, a Chinese national and a staff of the NRC (Vanguard Editorial, 27 June 2021). This indicates the severe impact of sabotage towards CNAI protection in Nigeria.

Rising Security Threats

The rise in security threats, including terrorism, insurgency, armed banditry, and separatist agitation affect CNAI protection because they target CNAI, causing damage and disrupting essential services. The majority of significant CNAI attacks across the country are carried out by terrorists, insurgents, and militants, including vandals. For instance, the collapse of socio-economic and education activities in the northeast is as a result of Boko Haram attacks on public institutions and facilities for essential services such as telecommunication masts, schools, banks, and hospitals among others. This is applicable to the incessant attacks by militants on oil and gas facilities in the Niger Delta

that nearly crippled the economy before the federal granted amnesty for the militants in 2009. This is same in majority of the states where there are severe security challenges.

Inadequate Infrastructure

Inadequate infrastructure is indeed a significant challenge to protecting CNAI in Nigeria. It can increase the vulnerability of CNAI to various threats such as terrorist attacks, cyber-attacks, and natural disasters. In Nigeria, major infrastructures such as physical (maintained roads, bridges, and power transmissions), digital (cybersecurity measures), communication (communications systems), are poorly maintained and unreliable, which can impede the response efforts and coordination among security agencies towards CNAI protection. For instance, roads, bridges, and power transmission lines are often in despair, making them vulnerable to attacks and disruption. The same is the inadequate cybersecurity measures that leaves critical systems and infrastructure exposed to cyber threats.

Lack of Public Awareness

Lack of public awareness about the importance of CNAI protection and the potential consequences of attacks hinder efforts to prevent and respond to threats, by creating a climate where individuals may not understand the importance of these assets, their vulnerability, or the need to report potential threats. This lack of awareness can lead to citizen apathy, undermining the effectiveness of security measures and making CNAI more susceptible to attacks. For instance, when the public is unaware of the importance of CNAI and the threats they face, they are less likely to report suspicious activities or potential attacks. This can prevent delay or timely intervention by security agencies, allowing attackers to proceed with their plans.

Institutional Corruption

Corruption among security agencies and government institutions undermines efforts to protect CNAI, allowing threats to go unchecked. For example, when funds meant for procurement of equipment, capacity building for personnel, and intelligence are diverted to other ventures that have no bearing on operational strength and effectiveness CNAI Protection, the capacity of the agencies to deliver on their responsibilities are eroded, leaving the infrastructure more vulnerable to attack and vandalism. This systemic issue erodes public trust, demoralizes personnel, diminishes national security, and hampers the government's ability to effectively safeguard critical assets.

Between CNAI Protection and National Security Architecture in Nigeria

It is important to draw attention to the fact that the established National Security Architecture is presented in figure 1 below is the primary architecture that governs security space in Nigeria. It is security/military heavy with minimal supervisory impact

from ONSA. However, Designation and Protection of Critical National Information Infrastructure (DPCNII) Order, 2024 has more supervisory control by ONSA.

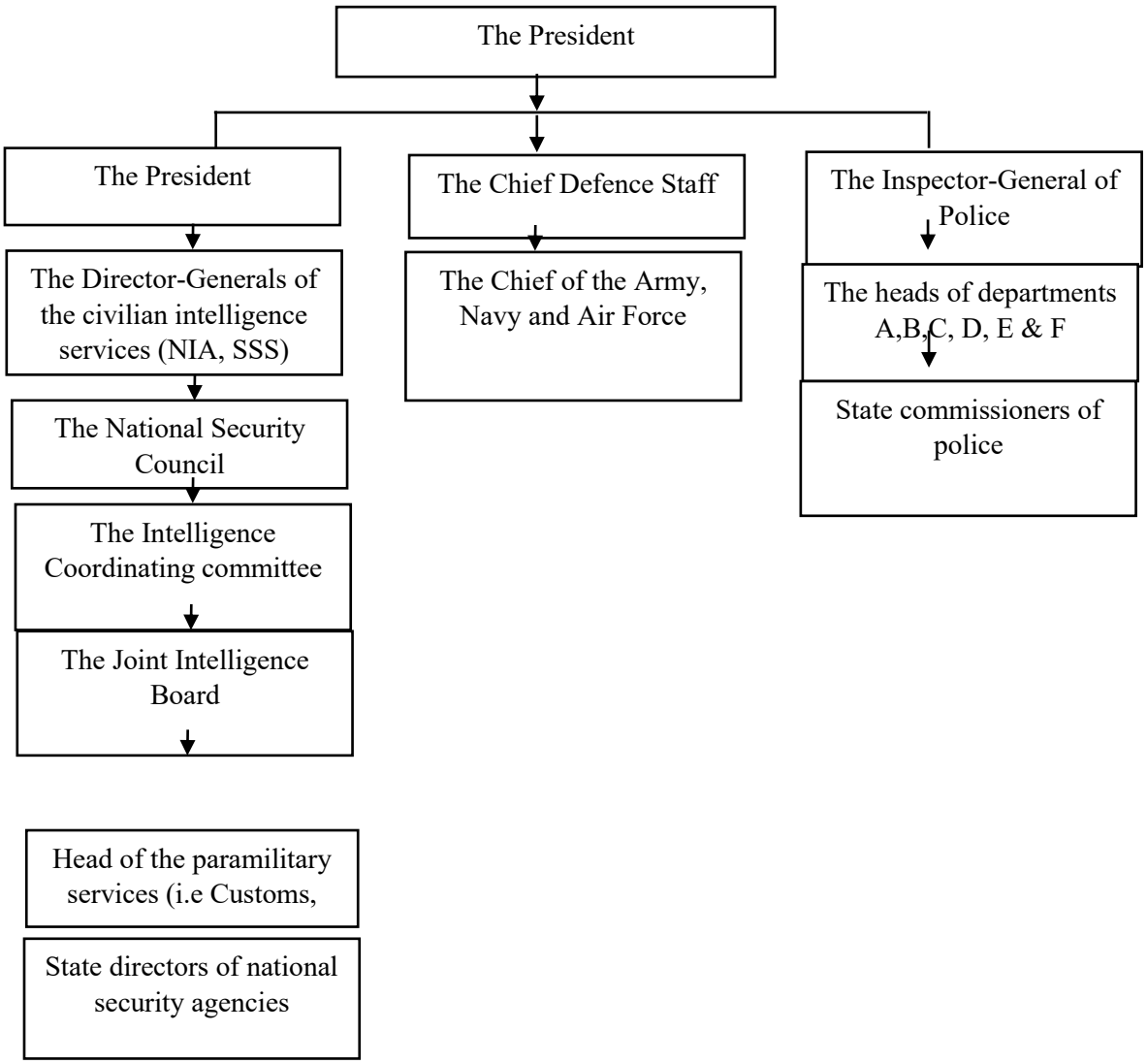

Figure 1: Established Primary National Security Architecture of Nigeria Source: Authors' arrangement.

From figure 1 above we can deduce a sub-National Critical Infrastructure Security Architecture that is more comprehensive and inclusive of critical sectors, critical subsectors, critical services and regulatory agencies as shown in figure 2 below.

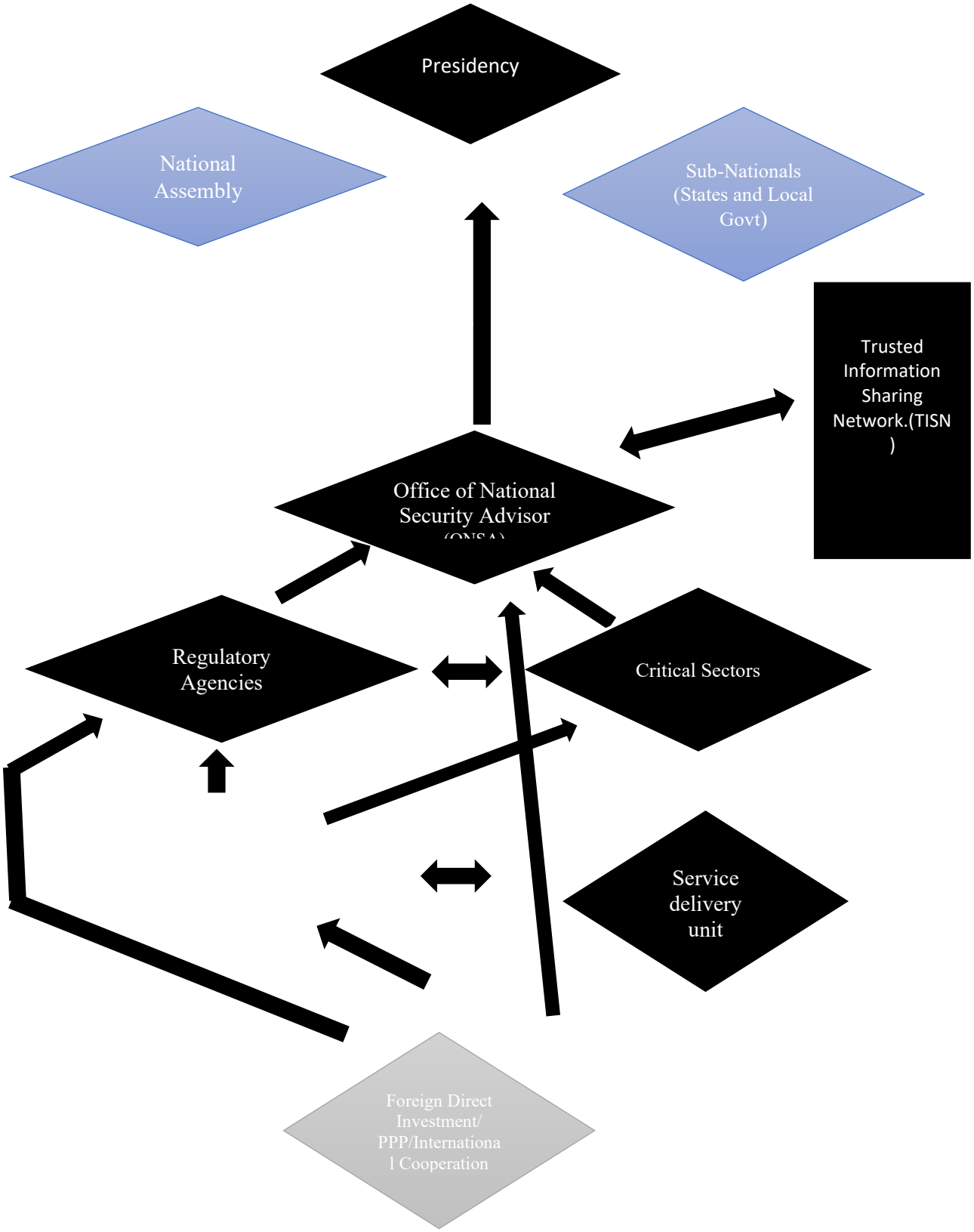

Figure 2: National Critical Infrastructure Protection Architecture

It is important to draw attention to the fact that though the 2019 National Security Strategy stated that NSCDC should be the lead agency in CNAI Protection the DPCNII defers elaborately to ONSA. With ONSA, becoming overwhelmed with the burden of security bearing, it is important that the security architecture of CNII would require comprehensive structure of decision-making. This will help to accommodate the wired interest that provide for critical and regulatory agencies.

In retrospect, the ONSA has effectively put in place some structural platforms that would help to recalibrate the national critical infrastructure architecture. First, the NSS 2019 document established CNAI Protection as a key element of Nigeria's national security to be led by the NSCDC and coordinated by the ONSA. It specifically mandated ONSA to be responsible for identifying, classifying and prioritizing CNAI, and to determine appropriate levels of protection required for each CNAI or groups of CNAI so as to enhance the resilience of CNAI to hazard or attacks. This included the provision for the development of a CNAI Protection Response Plan that would designate roles and responsibilities for all stakeholders to actualize the goal of CNAI Security and Protection.

To further strengthen CNAI Protection, the 2019 NSS also included the design and development of institutional capacity, systemic resilience, physical protection and contingency plans for CNAI by all MDAs. This therefore empowers ONSA to ensure the effective coordination of Nigeria's security architecture for CNAI Protection. Sadly, some of these strategies are yet to materialize. For instance, the CNAI Response Plan has not been put into practice, resulting in the frequent attack on CNAI across the country.

Secondly, ONSA developed a National Crisis Management Doctrine (NCMD) in 2022, to further strengthen CNAI Protection. The Doctrine provided a detailed methodology for national crisis response, outlining interactions among Ministries Departments and Agencies (MDA) at strategic, operational and tactical levels. However, its effectiveness in protecting CNAI is unclear and likely limited, due to factors like weak existing protection techniques, high vulnerability of assets, and potential implementation challenges despite the doctrine's aim for coordinated, effective crisis response. While the NCMD was launched to coordinate responses to various threats, including those affecting CNAI, its practical application and success in protecting these assets have not been clearly documented.

Given security situation in Nigeria, where the six geopolitical zones and even the federal capital territory is threatened by severe security challenges with threatening lethality and fatality, and the timing of CNAI as a key element of Nigeria's national security, ONSA has demonstrated effort and commitment to coordinating CNAI protection across sectors through initiatives like NCMD, DPCNII Order 2024, FCCCNAIP, while efforts to build a consistent approach to CNI protection and cyber resilience are underway. However, ONSA is overwhelmed with the omnibus security challenges across the country, resulting in the little or less attention it pays to issues like CNAI Protection.

ONSA focused more on security/military operations such as the internal security operations going on across the six geopolitical zones rather than protection CNAI. This therefore has affected its supervisory and coordinating role, resulting in the inability of the security agencies responsible for CNAI Security and Protection to foster an effective collaboration needed for a well-coordinated approach to securing the country's vital assets and infrastructure. As a result, the vulnerability of CNAI remains high.

Conclusion and Way Forward

It is obvious that there is an umbilical connection between critical national assets and infrastructure and national security architecture in Nigeria. While critical national assets and infrastructure are vital components of national security, protecting them is a core function of the national security architecture. It is on this premise that the federal government through the ONSA has made efforts to ensure protection and safeguarding of CNAI in Nigeria.

To achieve this, ONSA expanded the national security document to include CNAI to its 2019 National Security Strategy, developed a national doctrine for CNAI Protection response strategy – NCMD in 2022, ensured the validation of a national protection policy and strategy for CNAI – CNAI-NPPS in 2023, and ensured the gazetting of DPCNII Executive Order in 2025 and the critical national infrastructure protection plan – CNIIPP aimed at effective and efficient safeguarding of critical national assets.

Despite the efforts, CNAI faces significant threats, due to several factors including, poor coordination, lack of interagency cooperation, institutional capacity constraints, rising security threats, inadequate infrastructure, corruption, and lack of public awareness. Addressing these challenges requires effective implementation of the NSS 2019 CNAI Protection strategy that combines the institutional capacities of the NSCDC and other security challenges and the effective leadership of the ONSA. This includes improving resource allocation, strengthening accountability mechanism to prevent unnecessary interagency rivalry, and enhancing collaboration and cooperation between NSCDC, the military and other security agencies. Additionally, creating public awareness on the importance of CNAI protection will further reinforce security efforts, creating a more resilient and stable environment for CNAI protection.

Notes on Contributors

Gani Joses Yoroms is a professor of Political Science and former Provost of the Centre for Strategic Research and Studies (CSRS) at the National Defence College, Abuja, Nigeria. His areas of interest are Conflict, Security, and Defence Studies, with a bias towards Conflict Resolution, Terrorism and Violent Extremism, and Energy Security. He has attended professional training programmes on Defence Management at the University of Witwatersrand, South Africa, the UK Defence Academy/Cranfield University, and the CoESPUS Course, Italy. He has extensive research experience and has coordinated several national and international security research and programmes, such as the GIZ and ECOWAS Project on Farmer-Herder conflicts in West Africa. He served as Chair, Security Sub-Committee of the Thematic Committee on Defence, Peace and

Security of the Technical Working Group of the Medium-Term National Planning Experts on the Nigerian Agenda 2050. He is a fellow of ASSRC-MacArthur at the Watson Institute, Brown University.

Obinna Ukaeje is a Political Scientist and Research Fellow in the Department of Defence and Security Studies, Centre for Strategic Research and Studies, National Defence College, Nigeria. His areas of interest include national security, Election Violence, and Regional Counterterrorism and Counterinsurgency (CTCOIN). He has extensive research experience in defence and security studies, particularly in national security and CTCOIN. He has contributed immensely to several discourses on issues of national security and regional CTCOIN. He is a member of the Nigerian Institute of International Affairs (NIIA), a Member of the Nigerian Political Science Association (NPSA), a member of International Security Management (ISMC), and a member of the Savannah Centre for Diplomacy, Democracy and Development (SCDDD) National Quarterly Review on National Security and Promotion of Peace in Nigeria. He is currently the Deputy Coordinator of Research at the Irregular Warfare Centre (IWC), National Defence College, Nigeria.

Conflict of interest

The author hereby declare that no competing financial interest exists for this manuscript.

References

Akinlade, A. (2020). Telecommunications Disruption and National Security in Nigeria. *Journal of Nigerian Law*(45).

Alex-Dedipe, A., & Okorotie, H. (2024). Safeguarding Nigeria's Critical National Information Infrastructure: A Review of a New Order. *Pavestones Newsletter*, *29*(1).

Aregbesola, R. (May 9, 2023). *Full Speech on the Validation of the First Ever Critical National Assets and Infrastructure National Protection Policy and Strategy*. Transcorp Hilton.

Arise News. (August 1, 2024). *Protest Turn Violent in Kano as Demonstrators loot NCC Building*. Retrieved September 27, 2025 from https://www.arise.tv/protest-turn-violent-in-kao-as-demonstrators-loot-ncc-building/

Australian National Security. (2024). *Critical Infrastructure*. Retrieved September 27, 2025 from https://www.nationalsecurity.gov.au/protect-your-business/critical-infrastructure/

Bearne, S., Olga, O., O'Brien, K. A., & Rathmell, A. (2005). *National Security Decision-Making Structures and Security Sector Reform" Technical ReportTR-289-SSDAT. Prepared for the United Kingdom Security Sector Development Advisory Team.* RAND Europe.

Bergen, P. L. (2025). September 11 Attacks (Article History). In *Encyclopaedia Britannica (Updated)*.

Business Day. (2025). *Nigeria Records 1,700 Weekly Attacks on Telecom Infrastructure*. Retrieved September 25, 2025 from

https://businessday.ng/technology/article/nigeria-records-1700-weekly-attacks-on-telecom-infrastructure/

Channels Television. (2021). *85% of Schools in Nigeria are Vulnerable to Attack* [Video]. Youtube. https://www.youtube.com

Chisom, D. (May 10, 2023a). National Security Adviser, NSCDC Validate Critical National Assets Protection Policy. *News Planet International*. www.newsplanetinternational.com

Chisom, D. (May 10, 2023b). National Security Adviser, NSCDC Validate Critical National Assets Protection Policy. *News Planet International*. www.newsplanetinternational.com

Eroukhmanoff, C. (Január 14, 2018). Securitization Theory: An Introduction. *E-International Relations*. https://www.e-ir.info/2018/01/14/securitizsation-theory-an-introduction/

Federal Ministry of Interior. (2021). *FG Committed to Safeguard Critical National Assets and Infrastructure.* Retrieved June 22, 2025 from https://interior.gov.ng/press-release/fg-committed-to-safeguard-critical-national-assets-and-infrastructure-aregbsola/

Federal Republic of Nigeria. (2007). *Nigeria Security and Civil Defence Corps (NSCDC) Amendment Act No.6*.

Federal Republic of Nigeria. (2019). *National Security Strategy of the Federal Republic of Nigeria. Abuja*. Office of the National Security Adviser to the President.

Hamzat, K. (2024). *What Makes the Critical National Infrastructure So Critical*. Retrieved June 22, 2025 from https://www.harlemsolicitors.com/2024/12/07/what-makes-the-critical-national-infrastructure-so-critical/

Holmes, K. R. (2015). *What is National Security?* The Heritage Foundation. Retrieved June 22, 2025 from www.heritage.org/sites/default/files/2019-10/2015-_index0FUSSmilitarystrength_what%20is%national%20security.pdf/

Identifying Critical Infrastructure During COVID-19. (2020). *Cybersecurity and Infrastructure Security Agency (CISA)*. https://www.cis.gov/identifying-critical-infrastructure-during-covid-19/

Izuaka, M. (2023). *Nigeria Recorded 12.9 Million Cyber Attacks During Presidential, NASS Elections - Minister*. AllAfrica. Retrieved June 22, 2025 from https://allafrica.com/stories/202303150510.html

National Assembly. (2021). *National Security Summit Report, June* (Vol. 56). House of Representatives.

Ogunleye, K. (May 19, 2025). Safeguarding Nigeria's Critical Infrastructure against Vandalism. *Business News*. https://wabusinessnewsng.com/safeguarding-nigerias-critical-infrastructure-against-vandalism-2/

Okamgba, J. (2024). *Telcos Record N27bn Loss from Damaged Fibre Cables*. Punch. Retrieved April 21, 2024 from https://punchng.com/telcos-record-n27bn-los-from-damaged-fibre-cables/

Otukoya, T. A. (2024). The Securitization Theory. *International Journal of Science and Research Archive*, *11*(1), 1747-1753. https://doi.org/1030574/ijsra2014:11.10225

Premium Times. (2024). *EndBadGovernance Protest: Hoodlums Attack Uncommissioned NCC Office in Kano*. Agency Report. Retrieved August 1, 2024 from https://www.premiumtimesng.com/top-news/719686-endbadgovernance-protest-hoodlums-attack-uncommissioned-ncc-office-in-kano/

Punch. (2024). *FG Inaugurates Council for Critical Infrastructure Protection*. Retrieved June 22, 2025 from https://punchng.com/fg-inaugurates-council-for-critical-infrastructure-protection/

Rita, T. (2006). *Securitization Theory and Securitization Studies*. University of Warwick. https://doi.org/http://dx.doi.org/10.1057/palgravejird.1800072/

Shodunke, A. O. (2021). Boko Haram and Counterinsurgency Operations in Nigeria: Explicating the Military Ordeal. *African Journal on Terrorism*, *11*(2), 65-98.

SPA Ajibade & Co. (2024). *The Federal Government Has Officially Signed the Designation and Protection of Critical National Information Infrastructure Order 2024*.

The Guardian. (Oktober 19, 2020). *Alleged Cyber Attack on CBN Causes Stir in Banks*. Retrieved June 22, 2025 from https://guardian.ng/news/alleged-cyber-attack-on-cbn-causes-stir-in-banks-others/

The Guardian News. (November 24, 2020). EndSARS Protest: Counting the losses and the Gains. *Guardian Nigeria*. https://guardian.ng/features/endsars-protest-counting-the-losses-and-the-gains/

The United States of America Patriot Act. (2001). *Public Law 107-56. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*.

Towoju, R. B. (2024). *One Year of Unflinching Counter Terrorism Efforts in Nigeria*. The National Counter Terrorism Centre, Office of the National Security Adviser. Retrieved March 15, 2024 from www.nctc.gov.ng/

TVC News. (2023). *Nigeria Lost $200 Billion to Attacks on Critical Infrastructure*. Retrieved June 22, 2025 from https://www.tvcnews.tv/2023/05/nigeria-lost-200-billion-to-attacks-on-critical-infrastructure/

Ukaeje, O. (2020). Sectarian Violence and National Security in Nigeria: Boko Haram in Perspective. *Wukari International Studies Journal*, *3*(1), 41-55.

Ukaeje, O. (2022). Institutional Corruption as the Bane of Critical Infrastructure Protection in Nigeria. *Security and Defence Quarterly*, *39*(3), 63-75. https://doi.org/10.35467/sdq/147652

United Nations (UN). (2012). *Security Sector Reform: Integrated Technical Guidance Notes*. United Nations SSR Task Force.

United Nations Security Council 2341. (2017). *On Protection of Critical Infrastructure Against Terrorist Acts*. UN Security Council Counter-Terrorism Committee Executive Directorate Retrieved June 22, 2025 from

https://www.un.org/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ict_may_2021.pdf

United States of America Executive Order 13010. (1996). The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Federal Register, 61(138). In O. Ukaeje (Ed.), *Institutional Corruption as the Bane of Critical Infrastructure Protection in Nigeria (2002)* (pp. 63-75). Security and Defence Quarterly, 39(3). https://doi.org/10.35467/sdq/147652

Upsurge in Rail Track Vandalism. (June 27, 2021). *Vanguard News,*. https://www.vanguardngr.com/2021/06/upsurge-in-rail-track-vandalism/

Yoroms, G. J., & Ukaeje, O. (2024). Protecting Critical National Assets and Infrastructure in Nigeria: The Role of Intelligence Management. In I. M. Alumona (Ed.), *Intelligence and National Security Handbook*. Institute for Security Studies, Bwari-Abuja Nigeria.