ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

A Framework for NASRDA-Led LEO Satellite Internet for Secure Government and Critical National Infrastructure Communications in Nigeria

Anthony M. Akagwu[1]; Stephen E Ali[2]; Israel Dickson[3]; Jehu W. Zakpo[4]; Aisha Yakubu[5]; C. O. Chime[6]; Marcus Olaide Awobotu[7]; Toro Sani Safwan[8]

National Space and Research Development Agency (NASRDA)

Publication Date: 2026/08/08

Abstract: E-governance has improved public service delivery through the integration of internet capabilities to Critical National Infrastructures (CNI). Nations that are at a disadvantage due to a low internet penetration struggle to deliver on government's pertinent responsibilities of national security and sovereignty preservation. Recent commercialization of out of space activities has seen players such as Space X and Amazon deploy Low Earth Orbit (LEO) satellites in a bid to provide an alternative accessibility to regions that is traditionally unreachable to present terrestrial infrastructure. LEO infrastructure provides improved bandwidth, regional penetration and reduced latency.

This paper designed a framework for the implementation and deployment of LEO internet satellite to be led by National Space and Research Development Agency (NASRDA) to accommodate the Federal Government's needs in the area of secured communication and to ensure operational continuity of connected Critical National Infrastructure (CNI). The paper identified relevant stakeholders to participate in the deployment of LEO internet satellite infrastructure (NIGCOMSAT, NCC, Galaxy Backbone and ONSA) while NASRDA plays a technical and strategic implementation role.

Furthermore, the paper itemized the technical implementation to be adopted, a three phased implementation strategy roadmap to guide the implementation government and security frameworks that shapes the development and deployment of the framework.

Finally, the paper summarized some of the challenges of existing infrastructure and how the deployment of LEO internet satellite can effectively supplement the gains of the terrestrial infrastructure in place.

Keywords: *Low Earth Orbit satellite, Cyber security and Critical National Infrastructure (CNI).*

How to Cite: Anthony M. Akagwu; Stephen E Ali; Israel Dickson; Jehu W. Zakpo; Aisha Yakubu; C. O. Chime; Marcus Olaide Awobotu; Toro Sani Safwan (2026) A Framework for NASRDA-Led LEO Satellite Internet for Secure Government and Critical National Infrastructure Communications in Nigeria. *International Journal of Innovative Science and Research Technology*, 11(7), 3408-3414. https://doi.org/10.38124/ijisrt/26jul1651

I. INTRODUCTION

Low Earth Orbit (LEO) satellite constellations have grown recently into another global use case in the areas of telecommunications with an operational systems orbit at 500 km and 2,000 km; above Earth which has a significant impact on an improved latency and bandwidth performance of internet connectivity. Unlike geostationary satellites that typically operates at approximately 35,786 km above Earth (Berthoud, et al., 2022). This architecture enables a significant shift in broadband penetration to regions that have been underserved by traditional terrestrial internet connectivity. Africa is well below global ranking of internet accessibility per its population, which is drawn largely from fixed and wireless connections.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

Region	Fixed & Wireless Broadband Subscribers (million)	Market Penetration Rate (per 100 population)
Africa	24	2.4
China	103	7.7
Rest of Asia	292	12.0
Eastern Europe	55	16.2
Latin America	62	10.8
Middle East	42	13.4
US & Canada	174	51.4
Western Europe	262	64.3
Total	**1014**	**15.0**

Fig 1. Internet Accessibility for Various Regions and Continents.

Factors such as national income, government's interests and investments are highlighted as some of the key challenges facing nations with especially developing nations with high rate of citizen's not able to have internet access (Curran & Poland, 2011).

The emergence of Starlink internet services, operated by SpaceX, has demonstrated the viability of LEO-based internet service delivery at a wider global scale. Starlink provides internet speeds ranging between 50 to 400+ Mbps and latency as low as 20 to 40 milliseconds for residential uses in optimal conditions (Starlink, 2026). Starlink provides a receiver which is to be mounted at an elevated point and aimed at the sky ensuring there's no obstruction to the line of sight. The said device is connected to an access point to ensure a seamless configuration process and usage. Similarly, OneWeb and Amazon's Project Kuiper are expanding competitive alternatives, each targeting enterprise, government, and consumer markets.

Global demand for LEO satellite internet is being driven by persistent gaps in terrestrial infrastructure such as the latest technologies of 5G/6G, particular peculiarity in Africa, rural Asia, and parts of Latin America (Zamacola, Leyva-Mayorga, Martinez, Osario, & Popovski, 2026) . Broadband penetration in Nigeria has remained a critical challenge for the nation despite being Africa's largest economy. This continued uneven broadband penetration, unreliable network performance, and significant rural connectivity deficits have been associated with many factors most notably are Critical National Infrastructure-CNI (as designated by the federal government), lackluster public and private sector investments and economic reality of its citizens (Lawal , Gidari-Wudil, & Adedeji, 2025), (Laursen, 2025). National communication infrastructures, e-governance adoption and other digital public services are effectively interrupted occasionally due to these limitations in terrestrial broadband penetration in the country.

Nigeria's National Space Research and Development Agency (NASRDA) in this context is positioned strategically to provide a redefined national satellite communication capabilities policy, guideline and infrastructure. However, current reliance on foreign-owned LEO providers raises concerns regarding sovereignty, data control, and secure communications for government and critical infrastructure systems for nations with poor satellite infrastructure, experienced personnel and funding such as Nigeria.

This paper proposes the framework to guide the development and deployment of LEO satellite internet into Nigeria's national communication and broadband architecture led by the nation's space agency (NASRDA).

II. OPPORTUNITIES OF LEO SATELLITE INTERNET ECOSYSTEM AND LIMITATIONS OF EXISTING TECHNOLOGY

The current wave of LEO internet satellites constellation emerged between 2014 and 2016 which bares minimal resemblance to those deployed in the 1990's from overall system's digital payloads, multi-beams antennas, advanced modulation, manufacturing, weight, improved frequency reuse and cheaper build and lunch models (Portillo, Cameron, & Crawley, 2019). Starlink of Tesla, Oneweb by Eutelsat Group and Amazon Project Kuiper represent the three most prominent service providers in this ecosystem, with vast consumer broadband capabilities, future technology compatibility (5G/6G) and enterprise connectivity (Osoro & Oughton, 2021).

Inter-Satellite Links (ISLs) enabled LEO systems rely on careful constellation design, beam planning and centralized resource management for a reduced dependency for multiple gateways. ISL implements two level structures of control with (i) network management center generating a system wide

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

strategy and (ii) LEO satellites broadband operations that are executed in real time (Su, et al., 2019).

LEO broadband integration to already existing terrestrial technologies such as 5G/6G remains ideal but introduces challenges such as scalability, interoperability, business-model and technical knowledge for integration (Lin, et al., 2021), (Verma, 2025). LEO broadband services tend to provide better bandwidth to some terrestrial service providers even in urban areas with low-frequency mobile satellite services at its core, LEO systems often target IoT and low to medium-rate handheld services, while target like the Ku/Ka-band systems broadband are reserved for more higher need terminals (Lin, et al., 2021).

III. CHALLENGES OF NIGERIA'S EXISTING GOVERNMENT COMMUNICATION INFRASTRUCTURE

The existing communication infrastructure in Nigeria is dominated by terrestrial communication systems, including microwave radio links, fiber-optics networks and cellular networks. While digital connectivity and service delivery has been significantly improved by these systems, they remain vulnerable to technical, physical and cyber threats that seek to undermine the confidentiality, integrity and availability of the information they communicate and technology they possess. As operation of government increasingly become more digital and the need to protect states secrets and sovereignty, these communication technologies have been globally deemed and classified as Critical National Infrastructure (CNI) (Amin, 2000), (Banisakher, Omar, & Clare , 2019).

Nigeria's major terrestrial communication network backbone is predominantly reliant on fiber-optics network architecture. This presents a major challenge as these fiber-optics network cables are frequently disrupted by theft, flooding, vandalism, road construction and insurgent attacks which has resulted in outages that has affected government communication and essential public services (Ebipadou & Ebiegberi, 2024) & (Adeyemo, 2011). Disruptions of this scale and frequency highlights the vulnerability of communication architecture that relies on primarily ground-based infrastructure thereby underscoring the need for a more reliable alternative capable of sustaining continuity of services during disasters and emergencies.

The nation's poor power infrastructure equally presents a major challenge since communication facilities (cellular base stations, network switching facilities and data centres) depends on uninterrupted supply of power to maintain the functionality of such services further deepens the crises experienced in the telecommunication sector (Adeyemo, 2011). Prolonged power outages places significant burden on the operational costs, impaired emergency communication and reduces communication services availability as a whole.

Since terrestrial communication network completely relies on the availability of power infrastructure, a failure in the power greed often cascades into the way and means communication networks function hence other sectors such as health, financial services, commerce, transportation and public administration seldom suffers. (Imam, 2024).

Cybersecurity threats constitute another growing concern which has seen government communication networks being a potential target. Attacks such as ransomware attacks, malware infections, phishing campaigns, distributed denial-of-service (DDoS) attacks, and unauthorized network intrusions continue to probe government networks as they are believed to be targets of promising value and assets (Ebipadou & Ebiegberi, 2024). As digital transformation gains more traction across government institutions, attack surfaces expand and governments are at the risk of having their sensitive information compromised. According to the *Global Cybersecurity Index* published by the International Telecommunication Union (ITU), strengthening cyber resilience requires not only technical safeguards but also improving cyber security policy and building a resilient communication architecture capable of operating securely under adverse conditions (International Telecommunication Union (ITU), 2026).

Although Nigeria already owns and operate its indigenous satellites through the Nigerian Communications Satellite (NIGCOMSAT) and commercial providers, their utilization within government communication networks remains relatively limited and is mostly integrated as a supplementary communication medium rather than a primary communication medium. Consequently, government institutions continue to depend largely on terrestrial communication infrastructure.

These challenges highlight the necessity for a complementary communication architecture that leverages the advantages of Low Earth Orbit (LEO) satellite internet. Due to their low latency, global coverage, high throughput, and inherent resilience against localized terrestrial disruptions, LEO satellite constellations offer a viable platform for establishing secure government communications. A NASRDA-led framework would in no doubt integrate LEO satellite internet into Nigeria's national communication architecture. This will provide a more practical and reliable solution to communication systems resilience, improved operational continuity, and enhance the protection of critical national infrastructure while ensuring the country's broader objectives of digital sovereignty and national security are maintained and preserved.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

IV. PROPOSED NASRDA-LED FRAMEWORK FOR LEO SATELLITE INTERNET DEPLOYMENT

As most MDAs both at Federal and State levels continue to adopt e-governance and integrating both technical and administrative functions with the functions and capabilities of the internet and deploying resources of computers and software, there is an immediate need to adopt a government dedicated communication infrastructure that will prioritize security and national sovereignty of Nigeria. Hence, existing terrestrial communication networks, while indispensable, remain vulnerable to physical disruption, cyberattacks, and natural disasters. Consequently, this paper proposes a NASRDA-led framework for deploying Low Earth Orbit (LEO) satellite internet to provide secure communication services for government institutions and Critical National Infrastructure (CNI) in Nigeria.

The proposed framework adopts a multi-layered architecture comprising governance, space, ground, and user segments. It leverages NASRDA's expertise in space science and satellite technology while fostering collaboration with relevant government institutions, including the Nigerian Communications Satellite Limited (NIGCOMSAT), Nigerian Communications Commission (NCC), Galaxy Backbone, the Defence Space Administration (DSA), the Office of the National Security Adviser (ONSA), and other security agencies. Such institutional coordination ensures that policy formulation, technical implementation, spectrum management, cybersecurity, and operational service delivery are concisely captured and deployed.

➢ *Governance Framework*

At the strategic level, NASRDA is proposed as to take the lead as technical coordinator responsible for developing the national architecture, establishing technical standards in line global best practices, research and development, and overseeing system integration. Unlike commercial satellite internet deployments that primarily target public broadband access, the proposed framework examines the development and deployment of a secure communication infrastructure for the government of Nigeria and to support the needs of other dependent CNI.

The Federal Government would provide strategic oversight through relevant ministries and security institutions, while operational responsibilities would be distributed among participating agencies. NIGCOMSAT would provide operational satellite services and ground infrastructure where appropriate, the NCC would oversee spectrum coordination and regulatory compliance, Galaxy Backbone would facilitate integration with existing terrestrial government digital infrastructure, while security agencies would define operational communication requirements and limits.

This collaborative governance model minimizes institutional duplication and expulsion of valuable needs of other branches of government while leveraging on the advantages of each participating organization.

➢ *Technical Architecture*

The proposed technical architecture consists of four components:

- The Space Segment will provide a constellation of LEO satellites with a nationwide coverage to achieve low-latency broadband connectivity. Depending on national investment priorities, a hybrid approach is the best fit, partnerships with existing commercial LEO operators will afford the team enough time to progressively develop and deploy indigenous satellite capabilities.
- Ground Segment: This will be a network of strategically distributed gateway stations, mission control facilities, and Network Operations Centres (NOCs) which will be responsible for satellite monitoring, traffic routing, system maintenance, and network management and administration.
- Secure Communication Backbone: This component will oversee the secure connection of by providing an encrypted satellite communication layer interconnecting government data centres, command-and-control facilities, and emergency communication centres. This backbone provides redundancy to terrestrial fibre-optics networks and radio communication to ensure continuity during terrestrial infrastructure failure.
- User Segment: A secure satellite terminal to be deployed across Ministries, Departments and Agencies (MDAs), defence establishments, emergency management centres, border security posts, airports, seaports, energy facilities, and other critical national infrastructure requiring uninterrupted communication.

The layered architecture proposed by the framework will ensures redundancy by allowing seamless data transition between terrestrial and satellite communication channels whenever one network experiences disruption.

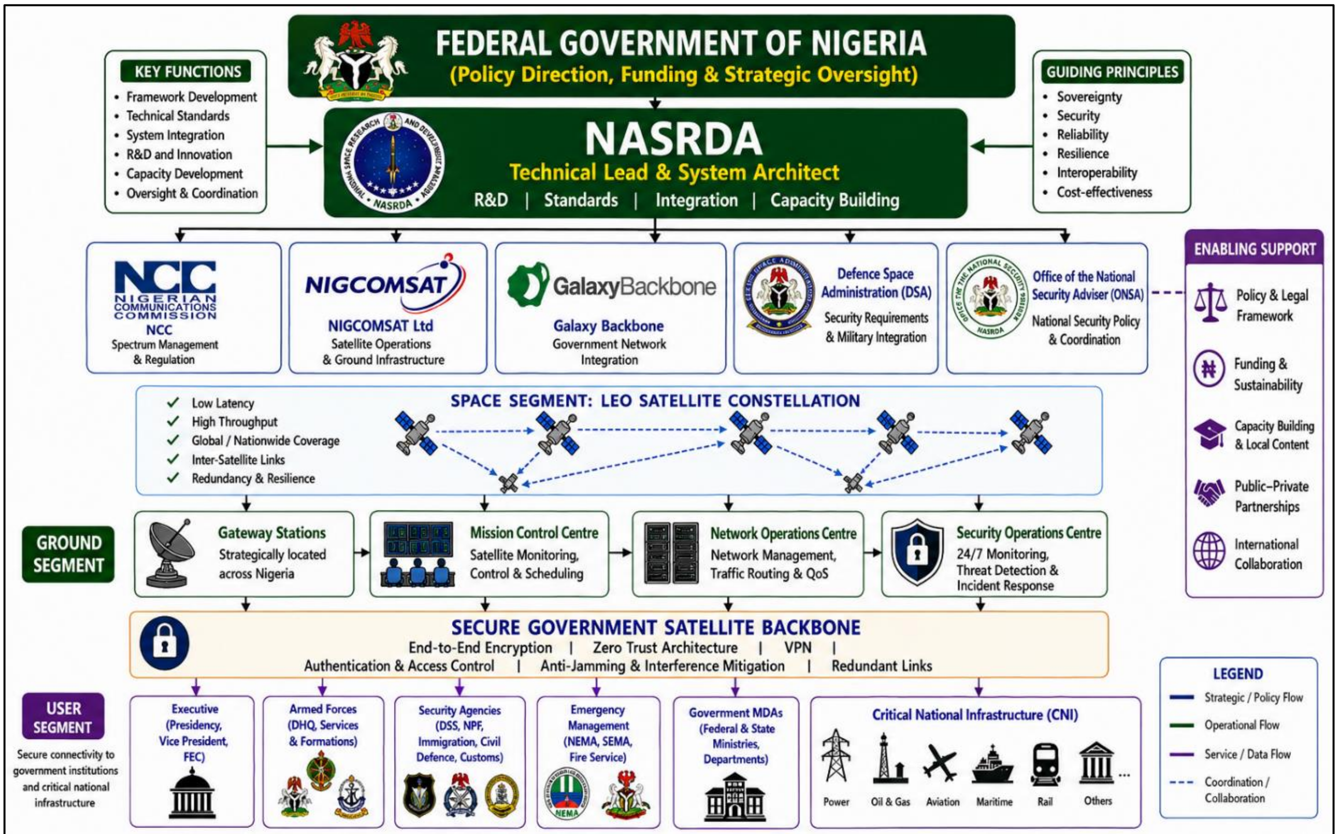

Figure 2: *Proposed NASRDA-Led Framework for Secure Government and CNI Communications using LEO Satellite Internet*

➢ *Security Framework*

The framework is keen on ensuring security is of utmost priority since data and resources relying on the deployed LEO internet infrastructure communicate sensitive government activities, which are by all national security measures considered secretive and highly classified. Therefore, the proposed framework adopts a defense-in-depth security architecture comprising;

- Anti-jamming and interference detection capabilities
- Security Operations Centre responsible for continuous network health monitoring
- End-to-end encryption for all connected nodes on the network
- Multi-factor authentication for every attempted access to the network
- Zero Trust security principles that continuously verify users and connected devices;
- Secure key management infrastructure
- Adoption of asymmetric key encryption for highly classified nodes and communications on the network
- Security Operations Centres (SOC) for continuous network monitoring

These measures are in tandem with international best practices and adopting industry standards in order to seamlessly integrate with existing technologies. Data confidentiality, integrity, availability and nonrepudiation are keenly fit into this proposed framework.

➢ *Implementation Strategy*

In order to ensure the implementation of the framework's objective, a phased approach will minimize both financial and operational risks.

- Phase I will focus on feasibility study, measuring stakeholders' responsibilities and needs, policy development a pilot program of selected institutions to measure the viability before a wide sector deployment.
- Phase II will examine the satellite connection to be established between critical national infrastructure, mass transportation lines, electricity transmission facilities, immigration and customs agencies etc. during which interoperability between LEO satellite internet and terrestrial infrastructure communication networks should be determined.
- Phase III this phase will ensure the support a national integration across MDAs and strategic institutions.

This proposed framework should guide Nigeria's with a achievable roadmap for developing a secured and resilient communication architecture that complements existing terrestrial communication networks rather than an abrupt overhaul of existing terrestrial infrastructure. With NASRDA's

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

technical leadership, implementing a LEO satellite internet to Nigeria government communication ant critical national infrastructure support can significantly strengthen national security, improve disaster resilience and advance Nigeria's long-term objectives of digital sovereignty and strategic autonomy in the space sector.

V. BENEFITS, CHALLENGES AND POLICY RECOMMENDATIONS

The successful deployment of the proposed LEO satellite internet has the potential of delivering a reliable, improve tamper-proof and highly secured communication solution capable of enhancing security, continuity of operations and services of systems relying on this solution. Unlike the current terrestrial internet services solutions available, LEO satellite networks are unlikely to be susceptible to power failure, vandalism, localized disasters and unintentional destruction of fibre-optic cables. Communication is assured even during even during harsh conditions (emergencies and infrastructure disruption)

The proposed framework will in no doubt strengthen Nigeria's position regarding command-and-control of its national sovereignty, improved security agencies coordination and an overall enhanced communication with Critical National Infrastructure (CNI). A full implementation of this framework will be a prove that Nigeria is not only a consumer of these technologies but a player to be contended with especially in the aspect of expanding the scope of its digital inclusivity drive.

Despite the aforementioned benefits to be achieved with the implementation of this framework, there are challenges that must be addressed even at the conceptualization phase. LEO satellite communication network requires substantial capital investment by the government since the deployment is focused on the security and sovereignty needs of Nigeria. Ground infrastructure, mission control facilities, user terminals and secure gateway are areas that require the financial investment of the government. A successful implementation of this framework will require a closely knitted collaboration between agencies such as NASRDA, NIGCOMSAT Ltd., the Defence Space Administration (DSA), the Nigerian Communication Commission (NCC), Office of the National Security Adviser (ONSA) and the Galaxy Backbone. This collaboration must clearly identify and assign responsibilities to all participating agencies.

Furthermore, cyber security risks and vulnerabilities should be investigated and continuously monitored to mitigate against threats such as frequency jamming, Distributed Denial of Service (DDoS), Advanced Persistent Threat (APT) and signal interference. A continuous investment in penetration testing and development of mitigation strategies is also required to ensure systems within the network function as intended.

Consequently, the proposed NASRDA-led framework represents a practical and scalable roadmap to guide towards strengthening Nigeria's communication resilience by providing redundancy to existing terrestrial networks with a secure LEO satellite internet connectivity, thus, the framework implementation will provide government operations continuity, enhanced critical national infrastructure protection, and advance Nigeria's strategic objectives towards national security, digital sovereignty, and space technology development.

VI. CONCLUSION

The digital divide in Nigeria just like any developing nation has impacted on how the government communicate and deliver impactful policies and reforms to better the lives of its citizens and protect its sovereignty. The meager gains recorded in recent times has seen Nigeria evolved into a technology hub to include e-governance and integration of some public services to the potentials of internet. These gains continue to face threats from physical to cyber on the existing terrestrial infrastructure in place. While terrestrial fibre-optic and wireless networks remain indispensable, they are susceptible to physical disruption, power failures, vandalism, cyberattacks, and natural disasters, all of which can compromise the continuity of government operations and the protection of Critical National Infrastructure (CNI).

This paper examined the opportunities and limitations of deploying LEO satellite internet infrastructure to support the internet connectivity needs of Nigerian government. The paper further explored the challenges the existing terrestrial solutions (fibre-optics and wireless radio stations) face and how the proposed LEO internet infrastructure will be deployed to supplement the existing infrastructure in place.

The also identified various participating stakeholders that needs to be involved in the development and implementation of the framework. Participating agencies were captured and assigned roles considering their legislative mandates they presently operate on. The framework recognizes NASRDA's strategic role in space research, technology development, and systems integration while acknowledging that successful implementation depends on close inter-agency collaboration and alignment with existing statutory mandates. By complementing, rather than replacing, existing terrestrial communication infrastructure, the proposed framework provides redundancy, improves operational continuity during emergencies, and strengthens the protection of national security communications and critical infrastructure.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1651

REFERENCES

[1]. Adeyemo, A. B. (2011). E-government implementation in Nigeria: An assessment of Nigeria's global e-gov ranking . Journal of internet and information system , 11-19.

[2]. Amin, M. (2000). National Infrastructures as Complex Interactive Networks . Electric Power Research Institute (EPRI) , 263-286.

[3]. Banisakher, M., Omar, M., & Clare , W. (2019). Critical Infrastructure - Perspectives on the Role of Government in Cybersecurity . Journal of Computer Sciences and Applications, 37-42.

[4]. Berthoud, L., Hills, R., Bacon, A., Havouzaris-Waller, M., Hayward Kieran, Gayrard, J.-D., . . . Combdlles, L. (2022). Are Very Low Earth Orbit (VLEO) satellites a solution for tomorrow's telecommunication needs? CEAS Space Journal, 609-623.

[5]. Curran, K., & Poland, K. (2011). Broadband Penetration in Countries Around the World. International Journal of E-Business Development (IJED), 34-37.

[6]. Ebipadou, A. F., & Ebiegberi, A. D. (2024). Digital Communication And Public Service Delivery: An Examination Of The Challenges And Opportunities In Contemporary Nigeria. International Journal of Academic and Applied Research (IJAAR), 177-183 .

[7]. Farrea, K. A., Baig, Z., Doss, R., & Liu, D. (2025). Zero trust-based authentication for Inter-Satellite Links in NextGen Low Earth Orbit networks. Ad Hoc Networks.

[8]. Imam, A. (2024). Poor Internet Connectivity and its Implications on Nigeria's e-Governance Trajectory. SSRN.

[9]. International Telecommunication Union (ITU). (2026, June 3). National Strategies. Retrieved from International Telecommunication Union (ITU): https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

[10]. Laursen, L. (2025). In Nigeria, Why Isn't Broadband Everywhere?: It Has 8 Undersea Cables, but Fiber-Optic Networks Miss Half the Country. IEEE Spectrum.

[11]. Lawal , L. S., Gidari-Wudil, T. S., & Adedeji, F. A. (2025). Implementation of Telecommunication Corridor on Infrastructure Roll out (Rail, Road, Power Lines and Inland Waterways) to Fast Track Broadband Penetration and Nation-Wide Surveillance. International Journal of Information and Communication Sciences, 23-33.

[12]. Lin, X., Cioni, S., Charbit, G., Chuberre, N., Hellesten, S., & Boutillon, J.-F. (2021). On the Path to 6G: Embracing the Next Wave of Low Earth Orbit Satellite Access. IEEE Communications Magazine.

[13]. Osoro, O. B., & Oughton, E. J. (2021). A Techno-Economic Framework for Satellite Networks Applied to Low Earth Orbit Constellations: Assessing Starlink, OneWeb and Kuiper. IEEE Access.

[14]. Portillo, I. D., Cameron, B. G., & Crawley, E. F. (2019). A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. Acta Astronautica, 123-135.

[15]. Salim, S., Moustafa, N., & Reisslein, M. (2025). Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. IEEE Communications Surveys and Tutorials, 372 - 425.

[16]. Starlink. (2026, 06 15). Starlink Pricing. Retrieved from Starlink: https://starlink.com/

[17]. Su, Y., Liu, Y., Zhou, Y., Yuan, J., Cao, H., & Shi, J. (2019). Broadband LEO Satellite Communications: Architectures and Key Technologies. IEEE Wireless Communications.

[18]. Verma, A. K. (2025). Cybersecurity in Satellite Communication Networks: Key Threats and Neutralization Measures. IEEE Open Journal of the Communications Society.

[19]. Zamacola, S. M., Leyva-Mayorga, I., Martinez, R., Osario, R., & Popovski, P. (2026). Demand- and Topology-Aware Resource Allocation in Non-Terrestrial Networks (NTNs) With Multi-Satellite Beam Hopping. IEEE Transactions on Communication.