Big Data and National Security Threats in Nigeria: Challenges, Opportunities, and Strategies

Sunday Omanchi Onazi *, Rashidah Funke Olanrewaju , Gilbert Aimufua

Posted Date: 24 February 2025

doi: 10.20944/preprints202502.1883.v1

Keywords: big data; national security; threats; predictive analytics; cybersecurity; intelligence

 doi:10.20944/preprints202502.1883.v1

Article

Big Data and National Security Threats in Nigeria: Challenges, Opportunities, and Strategies

Sunday Omanchi Onazi *, Rashidah Funke Olanrewaju and Gilbert Aimufua

Department of Computer Science, Faculty of Natural and Applied Sciences, Nasarawa State University, Keffi, Nasarawa State, Nigeria

* Correspondence: sonnieonazi@gmail.com

Abstract: Nigeria faces persistent national security threats, including terrorism, insurgency, cybercrime, and communal violence, which have significant socio-economic and governance implications. This study investigates the role of big data analytics in mitigating these security threats by analyzing structured and unstructured data from multiple sources. Using a mixed-methods approach, the study integrates literature review, case studies, and government policy analysis to assess the effectiveness of big data analytics in intelligence gathering, surveillance, cybersecurity, and early threat detection. The findings reveal that while big data enhances predictive capabilities and situational awareness, challenges such as data privacy concerns, infrastructure deficits, and ethical dilemmas must be addressed. The study recommends strengthening legal frameworks, improving technical capacity, and fostering public-private partnerships to maximize the potential of big data in national security strategies. The implications suggest that a data-driven approach can significantly improve Nigeria's ability to respond proactively to emerging security threats while balancing privacy and civil liberties.

Keywords: big data; national security; threats; predictive analytics; cybersecurity; intelligence

Introduction:

Background of Nigeria's National Security Challenges: Nigeria, Africa's most populous country and largest economy, faces a spectrum of security challenges, ranging from terrorism and insurgency to cybercrime and communal conflicts to sophisticated digital threats. (Federal Republic of Nigeria, 2019). Traditional security methods struggle to cope with evolving threats, necessitating the adoption of advanced data-driven approaches. The rise of big data analytics offers a transformative approach to improving intelligence gathering, threat detection, and strategic decision-making in national security. However, while the potential of big data in security operations is vast, issues related to data quality, legal constraints, and privacy concerns remain critical obstacles (United States Congress, 1978).

Additionally, the nation's security infrastructure and economic stability are increasingly at risk from cyber threats including hacking, online fraud, and data breaches. These issues have persisted, placing a burden on public coffers, undermining social harmony, and impeding Nigeria's attempts to achieve prosperity and sustainable development. Big data analytics integration offers a viable path forward in this intricate security environment for improving cybersecurity defences, bolstering intelligence capacities, and reducing new threats. But to effectively use big data for national security, one must have a thorough awareness of the particular difficulties and contextual details that Nigeria's socio-political environment presents.

Big Data and its relevance to National Security: Big data analytics enables security agencies to process vast amounts of structured and unstructured data in real time, extracting valuable insights for proactive decision-making (Anderson & Bi, 2017). By leveraging machine learning algorithms, network analysis, and predictive modelling, security organizations can identify potential threats

 doi:10.20944/preprints202502.1883.v1

before they escalate. However, the application of these technologies must be balanced with robust ethical and legal frameworks to protect individual privacy rights (European Union, 2016). Security agencies may extract useful insight from large datasets to find patterns, spot abnormalities, and foresee possible threats by utilising modern analytics techniques like machine learning and data mining. Using big data analytics to fight terrorism, insurgency, cyber threats, and other illegal activities gives a strategic advantage in Nigeria, where security issues are varied and ever-changing. But in order to fully utilise big data in national security, strong infrastructure, interdisciplinary cooperation, and adherence to moral and legal guidelines are needed to protect civil liberties and data privacy. Big data technology integration becomes essential to Nigeria's security strategy as it works to protect its people and maintain national sovereignty in the face of changing threats. In Nigeria, leveraging big data analytics in combating insurgency, cyber threats, and organized crime is a strategic necessity (International Covenant on Civil and Political Rights, 1966).

A conceptual diagram illustrating the Big Data Analytics Process for National Security, showcasing:

i. **Data Sources**: Social media, financial transactions, surveillance systems, cybersecurity logs.
ii. **Processing Stages**: Data ingestion, data cleaning, analysis, and visualization.
iii. **Applications**: Intelligence gathering, cyber threat detection, predictive policing.

This visual representation will enhance understanding by demonstrating how data flows from collection to actionable security insights.

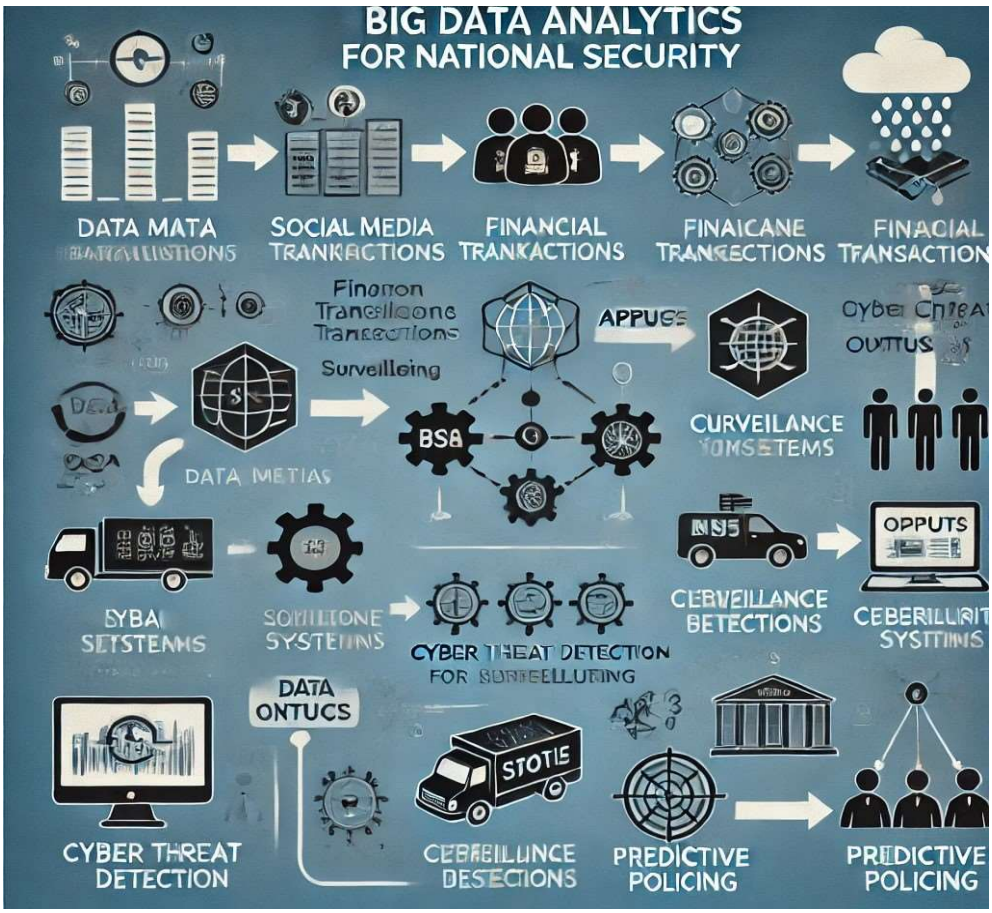

Diagram illustrating Big Data Analytics Process for National Security.

Above, is a conceptual diagram illustrating Big Data Analytics Process for National Security. Visually, it represents how data flows from sources like social media, financial transactions, surveillance systems, and cybersecurity logs through processing stages to applications such as intelligence gathering, cyber threat detection, and predictive policing.

 doi:10.20944/preprints202502.1883.v1

Purpose and scope of the paper: In the context of Nigeria, this paper explores the relationship between big data and national security, emphasising the opportunities, risks, and best practices for using big data analytics to effectively counter security threats. This study aims to give readers a thorough grasp of the ways in which big data technologies might improve Nigeria's national security framework, lessen the impact of new threats, and promote socioeconomic stability. This article looks at Nigeria's present national security concerns, such as cybercrime, terrorism, insurgency, and communal violence. It aims to show how urgently new methods of risk management, threat identification, and intelligence collecting are needed. The report will also examine how big data analytics may be used to reinforce cybersecurity measures, improve intelligence analysis, and improve situational awareness. This paper seeks to provide policymakers, security agencies, and other stakeholders involved in defending Nigeria's national security interests with insights and recommendations based on an analysis of the literature that has already been published as well as government initiatives, case studies, and best practices from other nations. In the end, this paper's scope includes investigating moral and legal issues as well as suggesting tactics for optimising big data's usefulness in tackling national security risks while respecting ethical norms and individual privacy rights.

Applications of Big Data Technologies in National Security

An overview of big data technologies, such as those used in data processing, analytics, storage, *and gathering.* Big data analytics enhances security operations through various applications:

(a) **Intelligence Analysis** – Security agencies use analytics tools to correlate data from multiple sources, uncovering hidden connections and predicting potential threats (United States, n.d.).
(b) **Cybersecurity and Threat Mitigation** – Big data enables real-time analysis of network traffic, detecting anomalies that may indicate cyberattacks (United States Congress, Senate, n.d.).
(c) **Surveillance and Predictive Policing** – By monitoring public communications and financial transactions, security forces can pre-emptively address criminal activities (United Nations General Assembly, 1948).

Big data technologies are essential for improving national security initiatives because they make it possible to gather, store, process, and analyse enormous amounts of heterogeneous data from many sources. In the field of data collecting, cutting-edge technology like sensors, GIS platforms, social media monitoring tools, and surveillance systems make it easier to gather real-time data streams that include text, photos, videos, and sensor data. Security agencies can now obtain intelligence through a variety of sources, giving them a complete picture of possible threats and security issues, thanks to these technologies. Furthermore, scalable and resilient architectures for safely storing enormous datasets are provided by big data storage solutions, such as distributed file systems and cloud-based storage platforms. Security organisations can guarantee data availability, dependability, and durability even in the event of hardware malfunctions or cyberattacks by utilising distributed storage solutions.

In the area of data processing, big data technologies employ parallel processing frameworks, such as Apache Hadoop and Spark, to efficiently process and analyze large datasets distributed across clusters of computers. These frameworks enable high-speed data processing and complex analytics tasks, including pattern recognition, anomaly detection, and predictive modelling. Moreover, advanced analytics techniques, such as machine learning algorithms and natural language processing, empower security agencies to extract actionable insights from big data, uncovering hidden patterns, identifying potential threats, and predicting future security incidents. Studies by Anderson & Bi (2017) highlight the role of machine learning algorithms in identifying suspicious activities, while European Union (2016) discusses legal frameworks for data protection. By harnessing the power of big data analytics, security agencies can enhance their intelligence capabilities, enabling proactive decision-making and timely responses to emerging security challenges.

 doi:10.20944/preprints202502.1883.v1

Applications of Big Data in National Security (e.g., Intelligence Analysis, Surveillance, Cyber Defense)

Apart from providing strong capabilities for data gathering, archiving, processing, and analysis, big data technologies are widely used in many aspects of national security. The extraction of actionable intelligence from many data sources is made easier by big data analytics tools and methodologies, one of the main applications being intelligence analysis. Security agencies can identify patterns, trends, and linkages suggestive of possible security risks by correlating and analysing vast amounts of organised and unstructured data, including financial transactions, social media posts, communications intercepts, and satellite imagery. This improves the capacity to recognise and proactively handle new threats, such as terrorist attacks and organised crime networks.

Additionally, big data is essential to surveillance operations because it allows security agencies to track and monitor targets, organisations, and activities through the monitoring and analysis of enormous amounts of data. Big data analytics-enabled advanced surveillance systems can scan and analyse real-time data streams from drones, CCTV cameras, and other sensor networks, allowing for the detection of potentially dangerous activity, unauthorised movements, and security breaches. Security agencies can improve situational awareness, enable quick reaction to security problems, and discourage criminal activity by using big data analytics for surveillance.

Furthermore, big data technologies play a crucial role in supporting cyber defence mechanisms, where protecting government networks, vital infrastructure, and sensitive information assets requires early identification and mitigation of cyber threats. Big data analytics makes it possible to identify harmful behaviours like malware infections, unauthorised access attempts, and insider threats by analysing network traffic, system logs, and security event data. Furthermore, threat intelligence sharing can be facilitated by big data analytics, allowing security agencies to work with foreign peers and industry partners to share information on new and emerging cyber threats and vulnerabilities. Nigeria has the potential to enhance its cybersecurity posture, reduce cyber threats, and protect its digital assets from ever-changing threats by utilising big data analytics for cyber defence.

National Security Threats in Nigeria

Analysis of Various Security Threats (e.g., Terrorism, Insurgency, Cybercrime, Communal Violence)

Nigeria faces a wide range of threats to national security, all of which pose serious dangers to the country's stability, prosperity, and cohesiveness. The four main dangers are cybercrime, insurgency, terrorism, and intergroup conflict.

The threat of ***terrorism,*** especially from organisations like Boko Haram and the Islamic State of West Africa Province (ISWAP), is still present in Nigeria, especially in the north-eastern areas. Numerous attacks against people, security personnel, and vital infrastructure have been carried out by these extremist groups, resulting in fatalities, population displacement, and socioeconomic problems. These groups use asymmetric warfare, suicide bombings, and kidnappings as tactics, which provide serious obstacles for Nigeria's security forces.

Another major security issue in Nigeria is ***insurgency***, which is frequently associated with socioeconomic grievances and confrontations between ethnic and religious groups. Terrorist organisations in the Niger Delta, including the Niger Delta Avengers, have sabotaged pipelines and oil installations, halting oil production and endangering Nigeria's vital economic infrastructure. Furthermore, rivalry for territory, resources, and ethnic identities has fuelled violent confrontations between herders and farmers in central Nigeria. Insurgent actions worsen social unrest, erode established systems of governance, and obstruct attempts at sustainable development.

Nigeria's national security is facing an increasing danger from cybercrime, which is being fuelled by the widespread use of digital technology and the internet. Cybercriminals engage in a variety of illegal actions, such as financial fraud, identity theft, phishing schemes, and cyber espionage, by taking advantage of weaknesses in digital infrastructure. Cyber threats offer significant risks due to

 doi:10.20944/preprints202502.1883.v1

insufficient cybersecurity protections and enforcement processes, which leave sensitive information and vital systems open to exploitation.

Political dynamics, socioeconomic imbalances, and intergroup rivalry are the main causes of communal violence, which presents serious problems to Nigeria's security environment. Tensions arising from ethnic and religious differences frequently turn violent, resulting in fatalities, population displacement, and property devastation. In addition to endangering social cohesiveness and national unity, these intercommunal conflicts also put a pressure on security forces' capabilities and sabotage efforts at peacebuilding and reconciliation.

It is clear from examining these security risks that they are complex and linked, necessitating all-encompassing approaches that deal with their underlying causes, encourage communication, and support inclusive growth. A comprehensive strategy that incorporates community involvement, law enforcement, information collecting, and international cooperation is required to implement effective countermeasures. Moreover, utilising big data analytics presents encouraging prospects for improving situational awareness, identifying warning indicators, and formulating focused countermeasures to successfully reduce security threats. Nigeria can protect its national security interests and promote resilience in the face of new challenges by comprehending the complexity of these security threats and embracing creative solutions.

Impact of These Threats on National Security and Socio-Economic Development

National Security Threats in Nigeria and Their Impact:

(a) Terrorism:

Impact on National Security: Terrorism weakens public confidence in security agencies, challenges governance systems, and challenges the authority of the state. This is especially true when it comes to acts committed by groups like Boko Haram and ISWAP. Attacks on citizens, security forces, and vital infrastructure on a regular basis upset social order, breed fear, insecurity, and obstruct efforts to resolve conflicts and establish peace.

Effect on Socio-Economic Development: The ongoing danger of terrorism discourages foreign investment, impedes trade, and makes unemployment and poverty in the impacted areas worse. Initiatives for sustainable development are hampered by population displacement, infrastructural degradation, and interruptions to agricultural operations.

(b) Insurgency:

Effect on National Security: State authority, territorial integrity, and resource management are seriously threatened by insurgent activity, especially in the central Nigerian region and the Niger Delta. Attacks on oil installations cause economic losses, revenue shortages, and social discontent by sabotaging Nigeria's main source of income—oil production. Furthermore, ethnic tensions and land disputes drive communal conflicts that put national unity in jeopardy, burden security forces, and exacerbate governance issues.

Effect on Socio-Economic construction: Insurgencies, especially in resource-rich areas like the Niger Delta, impede economic activity, impede the construction of infrastructure, and erode investor trust. Cycles of violence and instability are sustained by the environmental damage brought on by sabotage assaults on oil installations, which also worsen social deprivation, unemployment, and poverty.

(c) Cybercrime:

Effect on National Security: Cybercrime jeopardises sensitive data, damages digital infrastructure, and puts national security at risk. Attacks that target financial institutions, government networks, and critical infrastructure systems jeopardise data confidentiality, interfere with the provision of key services, and reduce public confidence in digital systems. Information warfare techniques and cyber espionage also pose a threat to diplomatic ties, state sovereignty, and strategic interests.

Effect on Socio-Economic Development: Cybercrime hinders digital transformation efforts, discourages foreign investment in Nigeria's rapidly growing tech industry, and stifles innovation.

 doi:10.20944/preprints202502.1883.v1

Financial fraud, identity theft, and online scams place a heavy financial burden on people, companies, and the government. They also hinder attempts to promote digital inclusion, discourage entrepreneurship, and limit economic progress.

(d) Communal Violence:

Impact on National Security: Communal violence, driven by ethnic and religious tensions, poses challenges to social cohesion, cultural diversity, and national unity. Inter-group conflicts strain security forces, exacerbate governance challenges, and undermine efforts towards peacebuilding and reconciliation. Furthermore, communal violence contributes to the proliferation of small arms and light weapons, exacerbating security risks and perpetuating cycles of violence.

Impact on Socio-Economic Development: Communal violence disrupts economic activities, displaces populations, and hampers infrastructural development, particularly in regions prone to inter-group conflicts. The destruction of property, loss of lives, and displacement of communities exacerbate poverty, increase social vulnerabilities, and hinder inclusive development initiatives, perpetuating cycles of poverty and instability.

Opportunities and Benefits of Big Data in Enhancing National Security: -

(i) Improved Intelligence Gathering and Analysis:

Security agencies can gather, handle, and examine enormous amounts of heterogeneous data from a variety of sources, such as social media, communications intercepts, and sensor networks, thanks to big data analytics. Security agencies can find actionable intelligence, recognise patterns, and obtain comprehensive insights into potential security threats by integrating data from numerous sources. Furthermore, sophisticated analytics methods—like machine learning algorithms—allow for the automated examination of big datasets, saving time and effort while enhancing the precision and efficiency of intelligence analysis.

(ii) Predictive Analytics for Early Threat Detection:

Security agencies can use data-driven algorithms and predictive models to anticipate and proactively mitigate new security threats thanks to big data analytics. Predictive analytics facilitates the early detection of possible security problems by analysing past data patterns, identifying aberrant behaviours, and projecting future trends. This enables security forces to put preventive measures in place and mitigate threats before they become more serious. By being proactive, security operations become more effective, response times are shortened, and the negative effects of security threats on public safety and national stability are reduced.

(iii) Better Decision-Making and Situational Awareness:

Through the provision of real-time insights about security occurrences, trends, and developments, big data analytics improves situational awareness. Security agencies are able to make well-informed decisions and allocate resources because of the integration of data from several sources, such as social media feeds, open-source intelligence, and surveillance systems, which gives them a thorough picture of the operational environment. Additionally, security staff may more easily recognise trends, patterns, and anomalies and make data-driven decisions in high-pressure, dynamic circumstances thanks to visualisation tools and dashboards that make complex data easier to understand.

(iv) Enhanced Cybersecurity Protocols:

Because big data analytics makes it possible to identify, evaluate, and mitigate cyber risks instantly, it is essential to bolstering cybersecurity defences. Big data analytics finds signs of compromise, questionable activity, and possible vulnerabilities through the examination of system logs, network traffic, and security event data. This helps security teams to react to cyberattacks quickly and efficiently. Additionally, advanced analytics techniques, such as behavioral analytics and threat intelligence, enhance the accuracy and efficacy of cybersecurity defenses, enabling organizations to adapt and respond to evolving cyber threats effectively.

 doi:10.20944/preprints202502.1883.v1

Challenges and Risks Associated with Big Data in National Security:

(a) Data Privacy and Civil Liberties Concerns:

The gathering, processing, and analysis of enormous volumes of private and sensitive data is known as "big data analytics," which raises issues with data privacy and civil liberties. The lawfulness and moral consequences of data collecting methods are called into question by the indiscriminate gathering of data from a variety of sources, such as social media platforms, communication intercepts, and surveillance systems. Furthermore, concerns to individual privacy rights and fundamental freedoms are posed by the possibility of unauthorised access, data breaches, and misuse of personal information; therefore, strong safeguards and legal frameworks are required to prevent abuse and exploitation.

(b) Data Quality and Reliability Issues:

The accuracy and efficacy of security operations are severely hampered by the dependability and quality of the data utilised in big data analytics. Big data sources frequently include unstructured, heterogeneous data that is rife with errors, inconsistencies, and noise. These data can skew analytical results and impair decision-making. Erroneous conclusions and false alarms can result from data analysis attempts being further complicated by missing or outdated data, data biases, and data interoperability challenges. To guarantee the integrity and correctness of data used in security analytics, addressing issues with data quality and dependability necessitates the implementation of thorough data governance frameworks, data validation procedures, and data cleansing methodologies.

(c) Limited Technical Expertise and Infrastructure:

Sophisticated infrastructure, significant financial investments, and specialised technical knowledge are needed to implement big data analytics in the context of national security. But in order to properly support big data projects, many security agencies in Nigeria face obstacles linked to poor technical expertise, antiquated IT infrastructure, and insufficient finances. Security agencies are exposed to cyber risks, intelligence gaps, and operational inefficiencies as a result of the lack of qualified data scientists, cybersecurity experts, and IT specialists, which impedes the development and implementation of sophisticated analytics solutions. In order to close these capacity gaps and increase organisational resilience and capacities, specific investments in workforce development programmes, training courses, and technological infrastructure upgrades are needed.

(d) Potential for Misuse and Abuse of Data:

There are worries over the possibility of data exploitation and misuse for immoral or illegal goals due to the extensive use of big data analytics in national security. Large-scale sensitive data collecting and storage centrally increases the possibility of insider threats, illegal access, and data breaches, which can result in invasions of privacy, improper use of surveillance techniques, and violations of human rights. Furthermore, prejudices, discrimination, and profiling may be made worse by the application of predictive analytics and algorithmic decision-making in security operations, which would serve to maintain social inequities and inequalities. Strict supervision procedures, transparency policies, and accountability frameworks are required to reduce the risks of data exploitation and abuse and guarantee that decisions based on data are made morally, responsibly, and in accordance with the law and ethical norms.

Case Studies and Best Practices

(a) Examination of successful implementations of big data analytics in other countries:

Many nations have effectively used big data analytics in a variety of fields, including national security, to boost cybersecurity defences, increase threat detection, and improve intelligence capabilities. For example, the National Security Agency (NSA) of the United States uses big data analytics to identify potential dangers and enemies by analysing enormous volumes of electronic communications data for intelligence purposes. Likewise, Israel's Unit 8200 employs big data

 doi:10.20944/preprints202502.1883.v1

analytics to gather and examine signals intelligence, facilitating pre-emptive counterterrorism actions and well-informed strategic choices. Big data analytics is also used by the Government Communications Headquarters (GCHQ) of the United Kingdom to safeguard vital infrastructure, improve situational awareness, and identify and neutralise cyber threats. These case studies highlight the effectiveness of big data analytics in enhancing national security capabilities, providing valuable insights and best practices that can be adapted and applied to the Nigerian context.

(b) Lessons learned and insights applicable to the Nigerian context:

These case studies offer a number of takeaways and revelations that are relevant to Nigeria's attempts to use big data analytics for security purposes. First and foremost, developing strong technological capabilities and infrastructure is necessary for big data analytics projects to be implemented successfully. Nigeria needs to make investments to modernise its IT infrastructure, train people in data analytics, and create alliances with the corporate and academic sectors in order to efficiently employ cutting-edge technologies and produce a competent labour force. Second, in order to preserve public confidence in data-driven decision-making processes, it is critical to guarantee accountability, transparency, and adherence to legal and ethical requirements. Nigeria can use the power of big data for national security while preserving civil liberties and human rights by learning from global best practices in data governance, privacy protection, and oversight systems. To fully utilise big data analytics in tackling intricate security issues, it is also essential to promote cooperation and information exchange among pertinent parties, such as governmental organisations, law enforcement, intelligence services, and the commercial sector. Nigeria may improve its national security capacities, lessen new threats, and advance regional peace and stability by absorbing best practices and learning from successful deployments.

Government Initiatives and Policies

(a) Overview of existing government efforts to leverage big data for national security:

Governments all throughout the world are realising more and more how big data analytics may improve national security and effectively combat new threats. Government-led programmes and projects have been launched in a number of nations to use big data analytics in cybersecurity, threat detection, and intelligence collecting, among other areas of national security. The Comprehensive National Cybersecurity Initiative (CNCI) of the United States, for instance, has provisions for using big data analytics to improve cybersecurity skills, identify cyberthreats, and safeguard vital infrastructure. Similar national projects have been started by nations like China and Russia to build sophisticated data analytics capabilities for intelligence gathering and strategic decision making. In order to fully utilise big data in protecting national security interests, these efforts entail the creation of specialised agencies, funding for research and development, and cooperation with the private sector.

(b) Analysis of policy frameworks and regulations related to data privacy and security:

Strong legislative frameworks and laws are essential to handle data privacy and security concerns as governments use big data more and more for national security. In order to control the gathering, handling, and dissemination of private and sensitive information in the interest of national security, numerous nations have passed laws and regulations. The General Data Protection Regulation (GDPR) of the European Union, for example, places stringent restrictions on data protection and privacy, including clauses pertaining to data minimization, purpose limitation, and individual rights protection. In a similar vein, the US has passed legislation like the Foreign Intelligence Surveillance Act (FISA) and the Privacy Act to control government monitoring operations and protect people's right to privacy. Specific legislation addressing data privacy and security concerns in the context of national security are necessary, even though Nigeria's current data protection laws, such as the Nigeria Data Protection Regulation (NDPR), provide a framework for protecting personal data. Careful consideration, stakeholder participation, and openness in the policy-making processes are necessary to strike a balance between the demands of national security

 doi:10.20944/preprints202502.1883.v1

and individual privacy rights. Nigeria has the opportunity to create comprehensive policy frameworks that support fundamental rights and freedoms as well as national security interests by learning from foreign best practices and participating in multi-stakeholder dialogues.

Ethical and Legal Considerations

(a) Discussion on the ethical implications of big data analytics in national security:

The growing use of big data analytics in national security creates significant ethical questions pertaining to civil liberties, human rights, and privacy. Huge volumes of personal data are being collected, analysed, and used in a way that may violate people's right and freedom to privacy. Furthermore, biases, prejudice, and profiling may be introduced into security operations through the use of predictive analytics and algorithmic decision-making, which could result in unfair outcomes and societal disparities. Concerns are also raised about the possibility of abuse or misuse of surveillance authorities, as well as the accountability and transparency of government surveillance programmes. Big data analytics projects in national security must be developed and implemented in accordance with ethical frameworks, such as justice, transparency, accountability, and respect for individual rights, to guarantee that they follow moral precepts and uphold democratic values.

(b) Compliance with legal frameworks and international norms:

- **Legal Compliance** – Security operations using big data must adhere to national and international regulations, such as GDPR and the Nigerian Data Protection Regulation (United Nations General Assembly, 1948).

Big data analytics projects in national security must adhere to legal frameworks and international norms in addition to ethical concerns in order to function legally and uphold international human rights standards. In order to control the gathering, processing, and exchange of personal data in the interest of national security, numerous nations have passed laws and regulations that include requirements for accountability, transparency, and supervision. For instance, government agencies are required by law to respect people's right to privacy and to ensure the lawful and appropriate use of surveillance authorities under the Foreign Intelligence Surveillance Act (FISA) of the United States and the General Data Protection Regulation (GDPR) of the European Union. (United Nations General Assembly, 1948). Furthermore, governments are required to follow certain guidelines and standards in their surveillance operations by international human rights instruments like the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights. These guidelines and standards include protections against arbitrary interference with an individual's right to privacy and other freedoms. When using big data analytics for national security, adherence to these legal frameworks and international norms is crucial to protecting individual rights, maintaining the rule of law, and upholding democratic ideals.

Strategies for Leveraging Big Data for National Security in Nigeria

(a) ***Capacity building and training programs:*** In order to effectively use big data for national security in Nigeria, a workforce with the requisite technological know-how and analytical skills must be developed. To improve the proficiency of security professionals, government officials, and other stakeholders in data analysis, cybersecurity, and data governance, capacity building and training programmes ought to be instituted. These courses should include a broad range of topics, such as privacy protection, legal frameworks, and ethical issues, in addition to more specialised subjects like data analytics tools and techniques. Nigeria can develop a skilled workforce that can use big data analytics to successfully address complex security concerns by funding capacity building programmes.

(b) ***Public-private partnerships for data sharing and collaboration*:** To fully utilise big data for Nigeria's national security, cooperation between the public and commercial sectors is necessary. Public-private partnerships have the potential to enhance security capabilities by promoting data sharing, knowledge exchange, and collaboration on research and development projects. In

 doi:10.20944/preprints202502.1883.v1

order to obtain the cutting-edge technologies know-how, and resources required to create and implement advanced analytics solutions, government agencies can collaborate with tech companies, academic institutions, and civil society organisations. Additionally, cooperative efforts can support best practices in data management and governance, standardisation, and interoperability of data, guaranteeing the smooth interchange of knowledge and insights across various stakeholders. Through the promotion of public-private partnerships, Nigeria may effectively handle new risks and build its national security infrastructure by utilising the combined knowledge and resources of diverse stakeholders.

(c) ***Development of a comprehensive national security data strategy:*** Nigeria need a thorough data strategy with defined goals, priorities, and action plans for using data analytics capabilities in order to use big data for national security. A comprehensive approach to data collecting, processing, analysis, and utilisation that takes into consideration the various demands and requirements of various security agencies and stakeholders should be included in the national security data plan. To guarantee the appropriate and ethical use of data, the strategy should involve the implementation of data governance structures, data sharing protocols, and data protection systems. To improve cooperation and information exchange, the policy should also specify how various government departments and agencies will integrate and coordinate data analytics projects. By developing a comprehensive national security data strategy, Nigeria can effectively harness the power of big data to strengthen its security infrastructure, enhance intelligence capabilities, and mitigate emerging threats in a coordinated and strategic manner.

Conclusion and Recommendations

In conclusion, Nigeria faces both opportunities and difficulties at the nexus of big data and national security. This study has examined the present state of the art, as well as the possible advantages, drawbacks, and implementation tactics of using big data analytics to counter security threats.

Key conclusions and insights summarised: This investigation has produced a number of important conclusions and revelations. Numerous security risks, such as cybercrime, terrorism, insurgency, and intergroup violence, jeopardise Nigeria's stability and socioeconomic advancement. Big data analytics present exciting prospects for boosting cybersecurity defences, augmenting situational awareness, and acquiring better intelligence. By integrating predictive models and real-time surveillance analytics, security agencies can improve intelligence gathering and threat detection (Federal Republic of Nigeria, 2019). However, in order to fully utilise big data in national security, issues such data privacy concerns, gaps in technical capabilities, and ethical considerations need to be resolved.

An appeal to decision-makers, law enforcement, and other interested parties: Proactive action is required by legislators, security agencies, and other stakeholders to fully utilise big data analytics for national security. This involves making investments in training and capacity-building initiatives to create a workforce with cybersecurity and data analytics expertise. Furthermore, encouraging collaboration and public-private partnerships is essential for advancing best practices, innovation, and data sharing. The creation of a thorough national security data strategy that outlines specific goals, priorities, and action plans for efficiently utilising big data should also be given top priority by policymakers.

Prospective avenues for investigating and doing research: Looking ahead, resolving current gaps and obstacles in utilising big data for national security in Nigeria should be the main focus of future research and implementation initiatives. This entails investigating moral and legal issues in more detail, creating sophisticated analytics methods that are suited to particular security risks, and improving data governance structures to guarantee the responsible and open use of data. Furthermore, it is crucial to continuously monitor and review big data projects in order to determine their efficacy, pinpoint areas in need of development, and modify plans in response to changing security dynamics.

 doi:10.20944/preprints202502.1883.v1

In conclusion, Nigeria can leverage the power of big data analytics to fortify its national security infrastructure, counter new threats, and advance peace, stability, and prosperity in the area by embracing innovation, collaboration, and strategic planning.

Recommendations: To harness big data for national security, Nigeria should:

(a) **Strengthen Data Governance** – Implement policies that regulate data usage while ensuring compliance with privacy laws.
(b) **Enhance Technical Capacity** – Invest in advanced analytics tools and cybersecurity infrastructure.
(c) **Foster Collaboration** – Encourage public-private partnerships for data sharing and intelligence exchange.
(d) **Improving Cybersecurity Measures:** Establish safeguards against data breaches and cyberattacks.

By integrating big data analytics into national security strategies, Nigeria can proactively address emerging threats while maintaining ethical standards and legal compliance.

References

1. Anderson, M. B., & Bi, Y. (2017). Big Data Analytics in Cybersecurity: A Review. In 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 276-279). IEEE. Anderson & Bi (2017).
2. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. European Union (2016).
3. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171. International Covenant on Civil and Political Rights (1966).
4. The Federal Republic of Nigeria. (2019). Nigeria Data Protection Regulation. Retrieved from https://nitda.gov.ng/nigeria-data-protection-regulation/ Federal Republic of Nigeria (2019). United States Congress. (1978). Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783. United States Congress (1978)
5. United States. (n.d.). The Privacy Act of 1974. Retrieved from https://www.justice.gov/opcl/privacy-act-1974. United States (n.d.)
6. United States, Congress, Senate. (n.d.). Comprehensive National Cybersecurity Initiative Act. Retrieved from https://www.congress.gov/bill/112th-congress/senate-bill/21. United States Congress, Senate (n.d.)
7. United Nations General Assembly. (1948). Universal Declaration of Human Rights, G.A. Res. 217A (III). United Nations General Assembly (1948)
8. Federal Republic of Nigeria. (2019). *Nigeria Data Protection Regulation*.