



Algorithmic Sovereignty: Pervasive Digital Infiltration and the Transformation of National Security Boundaries

¹Ibietonye Benjamin, ²Sophia Daniel Sonime

¹*Department of Sociology, Rivers State University, Nkpolu/Oroworukwo
Port Harcourt, Rivers State, Nigeria, Email: benjamin.ibietonye@ust.edu.ng*

²*Okey Onuchuku Institute of Peace and Conflict Studies
Ignatius Ajuru University of Education, Email: sophia.daniels@iaue.edu.ng*

Abstract

The aim of this research is to explore the question of algorithmic sovereignty, its potential impact on the way national security boundaries are changing in the digital age, and to argue that the extensive digital infiltration via social media, data surveillance devices, and algorithmic decision-making systems creates new opportunities for external actors both (state and non-state) to influence the political process, economic stability, and perception of people within the state. The study is based on Techno-politics Theory, which is an explanation of technological systems and digital infrastructures to be used as instruments in political power and geopolitical influence. Methodologically, the study uses documentary analysis, critical discourse analysis, and comparative case studies, which enable an in-depth examination of the impact of algorithmic control and digital platforms on governance, information ecosystems, and national security strategies, from emerging and advanced digital societies. The results indicate that the algorithmic systems are now used as a strategic tool of influence to challenge the autonomy of the state, influence the public discourse, and help to shape governance of security. The extensive use of digital technologies, artificial intelligence, and algorithm-driven platforms has transformed the nature of the world's power landscape and the understandings of national security, traditionally based on territorial defense, military power, and political sovereignty. As such, the study calls for greater digital governance, regulatory and strategic cyber capabilities to safeguard national interests in a world increasingly powered by algorithms.

Keywords: Digital governance, Cyber geopolitics, Information manipulation, Data sovereignty, Technological power.

Introduction

Traditional notions about national security are characterized by control of territory, military power, state survival, and freedom of the sovereign state to govern itself without outside interference to its laws. Thomas Hobbes among the classical philosophers has defined sovereignty as the supreme power with a defined area of territory, where the state creates order and protects citizens from internal disturbances and external threats. This sense of the state as the main protagonist for the protection of national interests and maintaining security later formed the core of international relations and security studies. Later, in the study of international relations and security, the state was viewed as the primary entity responsible for national security and the protection of national interests (Buzan, 1991). Instead, the increasing

spread of digital technologies, artificial intelligence, and platform-based tools has challenged such traditional ideas of sovereignty and security. In the digital era, national security is not only about the territory or military assets, but also about digital infrastructures, data flows, and algorithmic systems that are part of interweaving global networks. The shift poses a major challenge to the modern national security system, especially in developing countries where the regulatory system, technology infrastructure and digital independence is weak. These days, the digital sphere is infiltrated, and the attacks taking place, such as cyber, data manipulation, misinformation campaigns and algorithmic influence reveal flaws in traditional security strategies that were never anticipated.



Digital ecosystems are not confined to national borders and are increasingly posing a threat to the power of states to control information, protect strategic assets and protect citizens. It has been claimed that digital technologies are changing the nature of power by allowing for new modes of governance and surveillance, frequently outside of the control of the direct government itself (Zuboff, 2019). Relevant issues arise about the state sovereignty, policy autonomy and safeguarding of national interests. In this context, this research explores the constraints of current national security frameworks to deal with the challenges of algorithmic power and omnipresent digital penetration and its implications for a reimagined notion of sovereignty in the digital age. In particular, the study attempts to address the questions below: How does algorithmic governance of transnational digital platforms impact the traditional state and its security boundaries? How is digital infiltration so widespread and what new security risks does it bring, especially for developing nations? How can institutional and policy frameworks contribute to enhance algorithmic sovereignty and minimize national security threats in the context of digital dependency? In the current context of governments looking to maintain national sovereignty and strategic autonomy while enabling technological innovation, it is more important than ever to answer these questions (Farrell & Newman, 2019).

Theoretical Framework

This study is situated within the theoretical framework of technopolitics theory by Mitchell (2002), which explains the technological systems and infrastructures as instruments of political power, governance and strategic influence in modern societies. The theory proposes that technologies are not instruments without politics; they are rather political products that reflect political values, institutional interests, and power dynamics that influence the use and maintenance of power. It focuses on the way digital infrastructure (including platforms, data systems and algorithmic decision-making tools) becomes an integral part of governance, defines communication, governs information flows, and

shapes societal outcomes. In today's digital environment, algorithmic structures have the power to highlight, weaken, or prioritize information, influence public discourse, and affect political engagement and knowledge creation. This capability gives power to those who design and control systems that place the power in a different location than traditional state institutions. In the realm of national security, the theory highlights the pivotal role data flows and algorithmic systems play in the preservation of state sovereignty. It exposes the ways in which digital places can be spaces of political contestation in which influence is spread outside of any territorial limits. This is where the algorithmic sovereignty of the state becomes an important aspect of power. The framework thus addresses the fact that AI, data analysis and cyberspace are increasingly reshaping the landscape of security, placing poorly equipped States in a new position of greater vulnerability and potential loss of sovereignty in the digital era.

Literature Review

As digital technologies and algorithmic infrastructures continue to proliferate and develop rapidly, a burgeoning literature has emerged around the connection between technology, national sovereignty, and national security; traditional theories of sovereignty imagined the state as the principal actor of sovereignty, which encompasses land, institutions and political arrangements. Scholars of science and technology have long claimed that technical systems are embedded in political systems and governance processes. Winner (1980) suggested that technologies have political characteristics and that they shape social relationships and distribute power in particular ways; this observation was the basis of current studies of digital infrastructures as governance tools. Likewise, the emphasis of Latour (2005) on technological artefacts as socio-technical networks, which can affect institutional power and decision-making processes, implies that algorithmic systems are not neutral tools but are also socio-technical arrangements that can influence governance and authority.



As a result, algorithmic governance (Kitchin, 2017) has become an important perspective on the political dimensions of digital technologies, as they increasingly control social and economic life by automating decision making, forecasting human actions and organizing information traversal over digital platforms. The amount of data that these systems handle is so immense that it is increasingly influencing public communication, economic transactions, political engagement and security narratives that are part of the governance system, thus altering how power functions in digital societies. The concept of platform power is closely tied to algorithmic governance, and refers to the idea that the algorithms governing global technology firms have come to dominate digital infrastructures, affecting how communication, economic transactions, and knowledge is created. In the “platform society” described by Van et al., (2018), digital platforms are the central organizing structures of social, political, and economic life, algorithms are the mechanisms by which information comes to be visible, and they shape the political narrative and the formation of public opinion.

Zuboff, (2019) added another dimension to this concept by stating the new form of capitalism, which is called surveillance capitalism, is the process of having a big amount of data of human behaviours collected and analysed to predict and manipulate human behaviours, introducing new power imbalance between corporations, governments and citizens. This process makes personal data an economic, political resource and security concern, which poses privacy, democratic accountability and national sovereignty issues. Legal scholars discussed the implications of algorithmic systems for governments and regulation, arguing that algorithms are often “black boxes” that make it hard for the government and citizens to closely examine how digital platforms influence economic and political outcomes (Pasquale, 2015). This opacity poses important challenges to states trying to regulate digital infrastructures that span jurisdictions. In IR scholarship, researchers have been progressively examining the geopolitical consequences of digital technologies, Farrell, & Newman, (2019) argue

that the increasing geopolitical competition over AI and data governance is emblematic of a wider contest for digital sovereignty among the great powers.

The European Union's General Data Protection Regulation (GDPR) and new AI governance frameworks have put the connection between algorithmic governance and security into scholarly focus, highlighting how predictive policing and AI-driven surveillance affect state-citizen relations and sparking key questions about democratic accountability and technological governance Pasquale, (2015). Algorithmic infrastructures exist in transnational technological networks, which have to be understood as a contestation of the traditional territorial sovereignty, as highlighted by contemporary research on artificial intelligence governance (Srivastava, 2025). This tension has been termed by Srivastava as a sovereignty interdependence paradox, where states try to exert sovereignty over digital technologies, and at the same time depend on international technological ecosystems. Moreover, as political economists Allen (2022) argue, technological power has emerged as a key component of international geopolitical competition, and the contest over AI systems, semiconductor supply chains and global data infrastructures is evidence of technological power's newfound importance to national security and strategic independence.

As the architecture of governance is changing with algorithmic systems, they pose important theoretical questions about the nature of digitally mediated sovereignty, accountability, and authority. The study finds that the governance of AI is becoming multi-stakeholder, involving governments, technology companies and international bodies, as Zuboff, (2019) identify a number of different layers of governance mechanisms. This governance frameworks are designed to reduce the dangers of algorithmic decision-making, including those of anonymity, lack of transparency and security concerns in defining contemporary political power and national security dynamics. Gillespie, (2014) sees digital sovereignty as a moral “battle” over “authority” over the digital infrastructure, rather



than a technical “control” over it. As stated, the law's traditional governance structures were never intended for the challenges posed by automated decision-making systems, and new approaches are needed to address the algorithmic risks.

AI-powered digital government highlights that the use of algorithmic systems in public services, for policy assessment, and in decision-making is increasing. Studies on the implementation of AI in government entities indicate that digital governance is not just about technology, but also involves institutional trust, the engagement of stakeholders, and regulatory guidance. In addition, they highlighted the global governance challenges and dilemmas of AI, while emphasizing the need for algorithmic governance in the context of broad democratic governance accountability and institutional legitimacy. In this intricate international landscape, where various countries vied for regulatory authority over AI and others need access to foreign technological networks and international cooperation, new governance models that synthesize national autonomy with collaborative regulation are needed to address this paradox, Gwagwa & Mollema, (2025) contend.

Methodology

This research uses a qualitative research method to explore the extent to which digital infiltration is becoming an integral part of the national security landscape and how national security is being reimagined in the digital age. Studies investigating complex socio-political phenomena, institutional shifts, and new forms of governance that are hard to quantify are well suited to qualitative methods, as algorithmic sovereignty involves the interplay between the technological realm, political power and security governance. The research uses a documentary research approach that consists of a systematic analysis of policy documents, academic publications, institutional reports, and digital governance frameworks that are relevant to algorithmic systems and national security in different contexts (Bowen, 2009). Through the analysis of national cybersecurity policies, strategies on the governance of AI, international technology policy reports, and scholarly publications on algorithmic governance and digital

sovereignty, we gained insights into how governments and institutions think about and react to the increasing influence of algorithmic infrastructures on the boundaries of the state.

Further, Yin (2018) states that case study research can be used to explore the phenomenon in real-life settings in-depth, especially when the boundaries between the phenomenon and the context are not clearly understood. To analyse the interaction between algorithmic governance structures and national security strategies, the study uses illustrative cases from technologically advanced and emerging digital societies, in order to identify patterns in regulatory responses, governance mechanisms and technological vulnerabilities in various political settings, and to employ critical discourse analysis to interpret policy narratives and political discourse on algorithmic governance and digital sovereignty. According to critical discourse analysis (Fairclough, 2013), it has been helpful to study how language, policy frameworks and institutional narratives contribute to the perception of security threats and technological governance, which makes it useful in examining the qualitative data that can be organized and interpreted in thematic technique for analytical rigor. Thus, this methodological approach supports the systematic analysis of the relationship between digital technologies, algorithmic power and national security transformation, namely through the documentary analysis, comparative case studies and critical discourse analysis of the extent of digital infiltration and its implications in redefining the strategic contours of sovereignty and security in the twenty first century.

Findings and Analysis

The document analysis of the qualitative research (documents review, comparative case examination, critical discourse analysis) shows that there are some main patterns that can be deduced from the analysis of the created algorithmic infrastructures and their influence and impact on national security boundaries. The results show that the traditional security barriers have been massively restructured by digital penetration, creating new modes of technological power that are not based on a traditional territorial system of



the state. In the course of the analysis four major themes emerged from the study, the transformation of sovereignty through algorithmic governance, the geopolitical influence of digital platforms, the vulnerability of national institutions to information manipulation, and the growing importance of digital regulatory capacity for national security. This is because algorithmic governance is changing the notion of sovereignty, as it redefines sovereignty as the exclusive authority of the state over its territory, institutions and processes, as noted in the traditional definition of sovereignty. It reveals how the growing use of algorithmic platforms in communication, finance, security and data processing has led to a massive deconcentrations shift of control towards digital infrastructures increasingly controlled by private technology companies, from which the circulation of information in society, digital markets and citizen interaction with political content is increasingly determined.

The study revealed that, in the digital age, the ability to control and manage algorithmic infrastructures, which function across transnational networks, and to shape information flows through machine-learning algorithms, which curate and prioritize information, is becoming a crucial part of sovereignty in influencing public discourse, political engagement, security and data management. This ability to shape the information landscape has serious consequences for national security, in terms of political stability, electoral processes, and public opinion. Digital platforms were identified as a powerful tool through which the geopolitical competition is defined, whereby States and non-State actors resort to strategic communication, data analysis and automatic information campaigns with the aim of impacting foreign domestic politics and governance, leading to information manipulation and digital interference on national institutions and a higher risk of information wars. Digital platforms were observed as a powerful tool, through which the geopolitical competition is shaped, with States and non-State actors resorting to strategic communication, data analysis and automatic information campaigns with the aim of impacting foreign domestic politics and governance, leading

to information manipulation and digital interference on national institutions and higher risk of information wars. The study reveals how the rise of algorithmic systems has opened up novel avenues for influence operations involving targeted messaging, automated bots, and the use of algorithmic news feeds and other forms of data-driven propaganda, to the extent that external actors can use algorithmic recommendation systems to propagate misinformation, polarise the public debate and undermine trust in institutional systems, can exploit these. It demonstrates how algorithmic systems enable new kinds of influence operations: targeted messaging, automated bots and algorithmic news feeds and other forms of data-driven propaganda, which can be exploited by external actors to spread misinformation, polarise the public debate and undermine trust in institutional systems.

The findings also indicate that algorithmic infrastructures are now a core part of security governance infrastructures, governments are now reaching for AI technologies for intelligence analysis, cybersecurity monitoring, predictive policing, and strategic decision-making. The opacity of algorithmic decision-making systems also hinders policymakers from understanding fully how these systems produce security assessments or policy recommendations, thus raising new governance challenges alongside their ability to manage security risks. This poses significant questions about accountability, transparency and ethical governance in national security agencies, as well as the increasing significance of the digital regulatory capacity as part of national security strategy, and the fact that countries with well-developed technological infrastructures, data governance regimes and regulatory institutions are able to better safeguard their digital ecosystems from external interference. On the other hand, states that are dependent on foreign technological platforms, and do not have effective regulatory frameworks, are at risk of strategic vulnerabilities, pointing to digital governance capacity—such as the ability to create cybersecurity institutions, data protection frameworks, and artificial intelligence policy frameworks—as an important aspect of national



security preparedness in the digital age. Consequently, the scope of "national security" is expanding to include control over data infrastructures, algorithmic platforms, and digital governance systems, further enabling states to intervene in critical ways in the future of sovereignty, political stability, and security governance in the twenty-first century.

Discussion of Findings

The results of this research confirm certain arguments found in current literature on technology, governance and sovereignty that algorithmic infrastructures are not only a kind of technology but parts and parcel of the present power dynamics. The findings support the theoretical perspective of technopolitics and algorithmic governance, and they suggest that digital systems are emerging as a structural force that defines national security boundaries, institutional powers and geopolitical rivalries, in line with the research on socio-technical power, Winner (1980) argues that the technologies have political characteristics because they structure social relations and allocate authority. The present results reinforce this point, as they indicate that algorithmic infrastructures now mediate flows and decision-making processes that directly impact state authority, and that technological artefacts operate within networks of actors and institutions, as Latour (2005) argued. The discussion validates the findings that algorithmic sovereignty appears in such networks, in which the control over digital infrastructures becomes a factor in political decisions, and sovereignty becomes no longer exclusively territorial but increasingly infrastructural and data-driven.

The algorithmic curation of content is an important part of the literature on platform power, as in the transformation of national security boundaries discussed in Van, et al. (2018) the digital platforms are seen as influencing the way in which social, economic, and political life is organized, highlighting the platforms' role as a governance mechanism rather than a neutral intermediary. This is confirmation of Gillespie's [2014] claim that algorithms have an important role in the process of determining visibility and relevance in digital

space, as they amplify and suppress information, directly influencing the processes of public perception formation and political agenda-setting, which are closely related to national stability and security. In terms of the literature on surveillance capitalism and data-driven influence, the arguments regarding digital manipulation and information operations reflect Zuboff's (2019) assertion that the "behavioral data extraction" establishes new power asymmetries between technology companies, governments and citizens. The study reinforces the idea that large-scale data analytic create capacities for predictive influence strategies that can shape political behavior, and, in the national security sphere, these capabilities could be used for influence operations, cyber propaganda, or strategic communication campaigns, thus adding to the list of non-kinetic security threats.

Findings with respect to regulatory gaps and institutional vulnerability are consistent with scholarship focusing on governance tensions and issues in algorithmic systems where Pasquale (2015) has posited an opacity of algorithmic "black boxes" which hampers accountability and oversight. The study finds that this opacity makes it more difficult for national security officials to govern, especially in the case of states that depend on outside technology suppliers and that have weak regulatory structures that do not provide transparency into the effects of algorithmic systems on public discourse, risk assessment, or administrative decision-making. This reinforces the growing calls for transparency mechanisms, algorithm audits, and governance changes in digital systems, and it is supportive of the ongoing discussions about digital sovereignty and technological competition. The concept of cyberspace has made it difficult to reconcile with traditional ideas of territorial control, and has led to governance challenges that are not limited to nation-states, as noted by Mueller (2017); a similar theme is echoed by scholars like "algorithmic infrastructures are trans-nation, and unilateral national regulation is challenging" (Mueller 2017). The interdependence is also indicative of wider debates on technological globalization and on the new power dynamics between states and



corporations in the digital age, with the new strategic competition over AIs, data assets, and semiconductor supply chains further corroborating the conclusion that technological infrastructure has become a key element of national security strategies as outlined in recent digital geopolitics literature.

Also, the introduction of AI in public governance systems aligns with the literature on digital transformation in public sector, research on governance by AI shows that automation can enhance the efficiency of public sector governance, but it also poses ethical, institutional, and accountability issues. The results of this study support previous research that indicates an interplay of algorithmic tools in security institutions requires a regulatory component to counter unintended effects, consistent with the growing body of research on governance that focuses on participatory, transparent, and trustworthy institutional regulation as conditions for sustainable digital transformation. Importantly, it builds on previous literature by situating algorithmic governance within the discourse of national security boundary transformation, rather than privacy, corporate power or regulation, this study focuses on the strategic dimension of algorithmic infrastructures. It illustrates how algorithmic systems are increasingly becoming tools that can shape political stability, institutional legitimacy and security governance, thereby bringing together insights from the field of 'techno-politics', platform studies, surveillance theory and digital sovereignty debates in a cohesive national security approach.

The results also show that states with more robust digital governance institutional structures are more likely to be able to control algorithmic risks, consistent with Lyon, (2018) and her analysis of regulatory capacity and technological sovereignty, which argue that institutional preparedness is critical in reducing digital vulnerabilities. The evidence suggests that, in the algorithmic age, the security of the nation can rely on cybersecurity systems, data protection legislation, as well as AI governance systems, alongside military capabilities. The findings thus expand on

theoretical approaches by highlighting the algorithmic as a new strategic domain of power, by corroborating arguments in the literature that technologies are part of political systems, and by pointing to the algorithmic as a central part of the contemporary national security configuration of authority, governance and geopolitical influence, one that is not just a technological phenomenon but a reconfiguration of the boundaries of national security in the digital age.

Conclusion

To sum up, this paper discussed the extent to which digital infiltration and algorithmic systems are reshaping the conventional notions of national security and sovereignty in the digital age. The analysis revealed how algorithmic infrastructures, encompassing data analytics and artificial intelligence, platform-based communication systems, and more, have become important tools of power that affect governance, political stability, and geopolitical rivalry. Algorithmic systems are different from traditional "traditional" security threats, which are geographically bounded; they function across trans-national digital networks and create new "domains of influence" that are also challenging the state and institutional control. The results indicated that algorithmic governance redistributes power and impacts on information flows, public discourse, decision-making processes, and that these changes undermine the exclusive control of the territories and introduce new vulnerabilities related to digital dependency, public information manipulation, and technological asymmetries. In this way, modern-day national security more and more relies on the capacity to control digital infrastructure, data resources and technological skill within the country.

Author's Alternative Country. Alternative Country of the Author.

This research builds on a body of scholarship that has largely been centered on algorithmic governance as an issue of technology and regulation in order to reframe the issue as a national security concern. Previous research has focused on privacy, corporate power, and legal and regulatory structures, however, not enough



research has addressed algorithmic systems as structural drivers of sovereignty transformation. This study proposes the notion of algorithmic sovereignty as a strategic variable affecting state power, political stability, and geopolitical competition. It further develops an overall perspective on sovereignty as the power over digital infrastructures and information flows. Conceptually, it de-centers the notion of regulation and emphasizes the way in which digital infiltration is ubiquitous and creates non-territorial vulnerabilities and new boundaries of current security.

This research is a contribution to the knowledge because:

Proposing algorithmic sovereignty as an analytical tool to understand the effects of the digital infrastructures on the boundaries of national security, connecting algorithmic governance to studies on sovereignty and security. Showing that national security is no longer limited to territorial borders but also involves control over digital infrastructures and questioning the traditional conception of security as a model based on the state, and that technological capacity of governance is a new pillar of strategic autonomy. The security dimension of all-encompassing digital penetration is crucial, especially in societies where the State relies heavily on exogenous digital platforms, and where the digital governance architecture is still under construction.

References

- Allen, G. (2022). *The geopolitics of artificial intelligence and digital sovereignty*. Brookings Institution.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approach* (5th ed.). Sage Publications.
- Deleuze, G. (1992). Postscript on the societies of control. *October*, 59, 3–7.
- Fairclough, N. (2013). *Critical discourse analysis: The critical study of language* (2nd ed.). Routledge.
- Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Vintage Books.
- Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski & K. Foot (Eds.), *Media technologies*. MIT Press.
- Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14-29.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network theory*. Oxford University Press.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. Houghton Mifflin Harcourt.
- Morozov, E. (2013). To save everything, click here: The folly of technological solutionism. *PublicAffairs*.
- Mueller, M. (2017). Will the internet fragment? *Sovereignty, globalization and cyberspace*. Polity Press.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post- Cold War era* (2nd ed.). Lynne Rienner Publishers.
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. [https://doi.org/10.1162/isec_a_00351](https://doi.org/10.1162/isec_a_00351)
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- Ronfeldt, D. (1992). *Cyberocracy is coming*.



RAND Corporation.

Srnicek, N. (2017). Platform capitalism. Polity Press.

Van Dijck, J., Poell, T., & de Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

Winner, L. (1980). Do artifacts have politics?

Daedalus, 109(1), 121-136.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage Publications.

Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.