



Journal of Contemporary Politics

ORIGINAL ARTICLE

Digital Imperialism and Global Inequality: An Analysis of Selected Technological Corporations (Facebook, Cambridge Analytical, Bell Pottinger, Tiktok)

Olowoniya Funke Amanda^{1*}, Braimah Frederick Imuebe¹, Alayerogun Oluwaseunfunmi Emmanuel¹

¹Elizade University, Ilara Mokin, Ondo State, Nigeria

ARTICLE INFO

Article history:

Received 24-04-2026

Accepted 22-07-2026

Published 06-10-2026

* Corresponding author.

Olowoniya Funke Amanda

amanda.olowoniya@elizadeuniversity.edu.ng

<https://doi.org/10.53989/jcp.v5i3.26.43>



ABSTRACT

This study examined digital imperialism and its contribution to global inequality, focusing on the activities of Facebook, Cambridge Analytica, Bell Pottinger, and TikTok in Nigeria. It explored how these corporations influence politics, culture, and the economy through data exploitation, algorithmic control, and platform monopolies. The qualitative approach and the purposive sampling technique were used to conduct interviews with thirty participants, comprising cybersecurity/IT experts and officials of the electoral agencies. Dependency and Post-colonial theory were adopted. The thematic analysis revealed that digital imperialism undermines sovereignty, distorts democratic processes, fosters economic dependency, and promotes cultural homogenization. Weak regulation, low digital literacy, and reliance on foreign-owned infrastructure heighten vulnerability to digital imperialism in the Global South. The study recommends that Sections 41 and 44 of the Nigeria Data Protection Act should be amended to expand the duties of the Nigeria Data Protection Commission, beyond regulatory compliance, to include oversight over data domiciliation and sovereignty-related risks.

Keywords: Data Colonialism, Digital Imperialism, Facebook, Global Inequality, Global South, Tiktok

© 2026 Published by Bangalore University. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

In an era where digital technology has become a global lifeline, transforming how we communicate, access information, and participate in public discourse, its impact on social justice and development can no longer be considered solely positive or neutral. While the promise of technology to empower marginalised voices and foster development is undeniable, a darker, more insidious undercurrent has emerged: the weaponisation of digital tools by powerful technological corporations and complicit political elites¹. This phenomenon, increasingly referred to as digital imperialism, is not only deepening global inequality but also reshaping the dynamics of governance, democracy, and sovereignty in the Global South.

Digital imperialism and global inequality explore how certain Western and global technology firms have become instruments of neocolonial control, exerting significant influence over political processes and social narratives in developing countries. Historically, imperialism involved physical occupation and the extraction of resources. Today, its digital variant leverages data extraction, surveillance, algorithmic manipulation, and narrative control². This is not just an expansion of technological influence but a reconfiguration of power colonising the minds of populations through information warfare, political disinformation, and the monopolisation of online platforms. Global inequality is no longer just about access to food, water, or healthcare; it now includes digital literacy, data sovereignty, algorithmic fairness, and access to unbiased information³. Developing countries, lacking



strong data protection frameworks and digital governance, become fertile ground for technological exploitation and psychological manipulation.

A critical look at the operations and impacts of Facebook, Cambridge Analytica (a member of the SCL Group), Bell Pottinger, and X (TikTok) reveal a disturbing pattern of data exploitation, psychological manipulation, and social engineering⁴. Digital imperialism represents a new form of colonialism, or what Kwame Nkrumah described as neo-colonialism, a system where foreign powers exert control over developing countries through indirect, non-military means. In this digital age, the tools of domination are no longer gunboats and armies, but algorithms, data extraction, and psychological profiling⁵. If imperialism refers to the domination or intrusion into foreign nations to advance the interests and strengthen the power of the intruding entity, then the concept of digital imperialism becomes a logical extension in the modern context.

At its core, digital imperialism exploits the data and digital infrastructure of developing nations for the economic and political interests of powerful technology corporations and their political clients¹. These corporations, often headquartered in the Global North, collect vast amounts of personal and behavioural data from users in the Global South without meaningful consent. This surveillance enables foreign actors not only to profit from personal data but also to influence political outcomes, shape public discourse, and undermine democracies.

There have been scandals surrounding the operations of these multinational digital technological corporations. For instance, Cambridge Analytica's manipulation of elections in Nigeria, Kenya, India, and the Philippines exemplifies how foreign digital consultants can act as modern agents of neo-imperialism, rigging elections, inflaming ethnic tensions, and determining national destinies from abroad⁵⁻⁷. By supporting governments or political elites willing to pay for manipulation, these companies directly undermine the sovereignty of developing nations, echoing Nkrumah's warning that neo-colonialism "is the worst form of imperialism, for those who suffer from it are never sure whether they are free or not"⁸. Thus, digital imperialism operates by colonising minds rather than territories, using technology not to empower, but to control and exploit, turning technology into tools of subjugation rather than liberation.

Cambridge Analytica is a British consulting firm, a member of the SCL Group, particularly known for its involvement in the 2016 US elections and the Brexit campaign. The tipping point in global awareness came with the revelations that Cambridge Analytica, a data analytics firm, had harvested Facebook data from about 87 millions users globally to profile and micro-target voters in

countries like Kenya, the Philippines, and India⁹⁻¹¹. For a payment of £6 million, Cambridge Analytica worked just 90 days ahead of Kenya's controversial 2017 election to engineer psychological campaigns that swayed public opinion in favour of Uhuru Kenyatta¹².

Similarly, defunct UK public relations firm Bell Pottinger had deliberately incited racial hatred in a South African political campaign using multiple Twitter accounts and divisive hashtags to benefit its elite clients; this represents another facet of digital colonialism where ethnic divisions are exploited for profit and power^{13, 14}.

More subtly and no less dangerously, Facebook.org had deployed Free Basics, a stripped-down version of the internet tailored to favour Facebook content as a "humanitarian" solution to internet inaccessibility^{15, 16}. However, critics, including Global Voices and Foreign Policy magazine, have rightly called this initiative a "dictator's dream come true", allowing authoritarian regimes to control online content while tightening surveillance and limiting open access to the broader internet^{17, 18}.

Although efforts to resist such digital imperialism are evolving, for example, India's successful rejection of Free Basics by net neutrality activists has gained traction^{19, 20}. However, much of the developing world remains vulnerable. Adding to these concerns is the role of platforms like TikTok, whose opaque algorithms and foreign ownership raise questions about digital sovereignty, surveillance, and cultural imperialism²¹. These platforms increasingly shape youth consciousness, not just by curating content, but by determining what remains invisible.

The widespread use of troll farms, bot armies, and coordinated disinformation campaigns across at least thirty countries further highlights the instrumental use of technology in undermining democratic discourse²². In many cases, such tools are being used not only by authoritarian states but also by non-state actors, multinational corporations, and even opposition parties, such as Kenya's use of Aristotle to manipulate elections and promote violence²³. These abuses turn technology from a tool of empowerment into one of division and domination.

Despite the vast influence of digital corporations, there is a troubling paucity of academic and policy-oriented literature on the implications of digital imperialism in the Global South. As digital colonisation intensifies, developing countries must urgently establish mechanisms to safeguard digital sovereignty, protect citizens' data, and promote critical digital literacy. In Richard Stallman's radical view, outlawing the collection of personal data



could dismantle surveillance capitalism, but such reforms require political will and grassroots pressure, not mere corporate apologies²⁴.

Also, as Mark Zuckerberg continues his fourteen-year apology tour, expressing regret without systemic change, it becomes clear that genuine reform will not emerge from the very actors benefiting from the current system²⁵. Rather, as Paulo Freire and Bell Hooks have emphasised, liberation must come through critical consciousness, education, and collective resistance. Thus, while drawing from the immense benefits of digitalisation, its double-impact effect must not be overlooked.

In recent years, the rapid expansion of digital technology across the Global South has raised urgent concerns about the unequal distribution of power, access, and control over information. While technology has been widely celebrated as a tool for development, empowerment, and connectivity, an emerging pattern reveals that dominant global tech corporations such as Facebook, TikTok, Cambridge Analytica, and Bell Pottinger have exploited their influence in ways that reinforce rather than reduce global inequality. These firms' involvement in electoral processes manipulation, ethnic tension exacerbation, citizens psychological profiling through social media (Facebook's Free Basics), among other practices not only undermine democratic governance but also entrench a form of digital imperialism, where the sovereignty of developing nations is compromised by foreign control of digital infrastructures and data ecosystems^{2, 26, 27}.

Although studies^{28, 29} have highlighted the potential of technology to enhance citizen participation, economic inclusion, and development outcomes, there has been limited research specifically addressing how these same technologies can be co-opted to serve imperialistic or anti-democratic ends^{3, 30}.

While scholars and journalists have exposed isolated cases such as the Cambridge Analytica scandal in Kenya and India or Bell Pottinger disinformation campaigns in South Africa, comprehensive academic investigations into the broader consequences of digital imperialism for global inequality remain sparse^{5, 31}. Existing literature also tends to focus either on data privacy or disinformation, without sufficiently linking these issues to systemic power imbalances and historical patterns of exploitation inherent in the global system.

This new form of imperialism, accompanied by globalisation, has become worrisome, particularly with state and non-state actors' involvement and the inadequacy of literature in the subject area. This study examined how technological advancements, such as the internet and mobile devices, contributed to the rise of digital

imperialism and exacerbated global inequality, and also how the operations and influence of digital corporations, specifically Facebook, Cambridge Analytica, Bell Pottinger, and TikTok, perpetuated digital imperialism and deepened global inequality.

This study further interrogates how data manipulation, algorithmic bias, information gatekeeping, and narrative engineering are being deployed in developing countries and to what effect. In doing so, the study will contribute to a more nuanced understanding of the intersection between technology, neocolonialism, and underdevelopment, while offering actionable insights on how digital spaces can be decolonised to promote equity, autonomy, and digital justice in the Global South.

REVIEW OF LITERATURE

Conceptual Clarification

Digital Imperialism, Data Colonialism, Digital Sovereignty and Surveillance Capitalism:

The concepts of digital imperialism, data colonialism, surveillance capitalism, and digital sovereignty are often used interchangeably. While digital imperialism denotes data extraction and monetisation from the Global South through digital infrastructure dependence, it's often used as data colonialism to depict the power structure and control due to a superior capacity and ownership position, replicating the territorial scramble and conquest of colonies in Africa, Asia and Latin America in the 15th and 19th centuries.

Therefore, data colonialism and digital imperialism act as a rearview mirror that explains the chronological dynamism of imperialism from the colonial period to the 21st century, while data colonialism highlights a continuation of the power, control, economic and political influence inherent in colonialism; digital imperialism wears a new garb in the quest to retain economic power and market expansion in the contemporary global system. So, both concepts shed light on the imbalance that characterises the global system, exposing and affirming that he who pays the piper dictates the tune, as evidenced in the activities of powerful non-state actors (multinational tech corporations).

Digital sovereignty, on the other hand, is the capacity of a nation to maintain significant control over its data infrastructure, software, and digital decision-making in conformity with the nation's laws, policies and strategic interests to curtail geopolitical risk. Conversely, surveillance capitalism is an economic model where tech corporations commodify personal data by extensive tracking, analysing and predicting users' behaviour to influence their future decisions and generate revenue from it¹.



While these concepts are multifaceted, they all agree on the significance of decision-making power and reduced passive dependency. This does not imply the elimination of foreign tech operations but the flexibility to choose and control your nation's digital operations.

Conceptual Analysis

Concept of Digital Imperialism:

Digital imperialism refers to the domination of the digital sphere, including data, platforms, and infrastructure, by powerful corporations or states from the Global North, resulting in asymmetrical control over information, communication, and technological resources in the Global South². Digital imperialism exposes the extension of imperial domination in the digital domain. It is a modern form of control where powerful global actors, particularly multinational tech corporations and governments of the Global North, exploit digital technologies to exert influence over less powerful nations. Unlike traditional colonialism that relied on physical occupation, digital imperialism operates through data extraction, surveillance, algorithmic governance, and platform control.

One of the key mechanisms by which digital imperialism exerts control is the overwhelming dominance of Western technology corporations such as Meta (formerly Facebook), Google, and TikTok across the Global South. These platforms serve not only as communication tools but also as gatekeepers of data and information³². Their pervasive presence allows them to collect vast amounts of personal data, track behavioural patterns, and monitor communication networks, often without the informed consent of users in developing countries^{1, 2}. This data extraction forms the basis for a new kind of surveillance capitalism, wherein users become raw material for predictive analytics and profit generation.

Furthermore, these platforms play an influential role in shaping political discourse. Through the use of algorithmic curation and targeted advertising, they can promote or suppress specific narratives, contributing to the manipulation of public opinion and even affecting electoral outcomes. This was notably observed in the Cambridge Analytica scandal, where data-driven microtargeting was used to sway voters in both the United States and various developing nations³³. Such practices reveal the extent to which digital platforms can act as covert political actors, often without transparency or accountability.

Understanding Digital and Global Inequality in the 21st Century

Inequality is a multidimensional concept, deeply embedded in global structures, while political scientists explore its effects on democracy and governance,

postcolonial scholars link global inequality to historical and systemic domination that sustains global disparities³⁴. Economists such as Piketty and Milanovic link global inequality to disparities in income and wealth, showing how globalisation benefits some regions more than others. Development theorists, such as Sen, focus on unequal access to capabilities like education and healthcare⁷⁵.

In the 21st century, the emergence and widespread adoption of digital technologies have significantly altered the landscape of global inequality. This manifests not only in economic terms but also in access, literacy, representation, and governance, each along a broader pattern of global disparity. These new dimensions are deeply embedded within technological infrastructures, shaping who participates in the digital world and who remains marginalised.

A primary dimension of digital inequality lies in access to technology and infrastructure. Internet connectivity, digital devices, and stable electricity have become foundational to participating in social, educational, and economic life. Yet, large portions of the global population, particularly in rural regions and among low-income communities, lack consistent or affordable access to these resources. This "digital divide" restricts entire populations from engaging with essential services, educational platforms, and labour markets³⁵. As digital participation becomes a prerequisite for modern inclusion, the absence of infrastructure entrenches inequality.

Closely related to access is the issue of control over data and digital platforms, which is dominated by a small number of powerful corporations, primarily based in the Global North. These companies accumulate and profit from vast quantities of user data, often without meaningful oversight or transparent consent. Zuboff (2019)¹ describes this phenomenon as "surveillance capitalism," where personal data becomes the raw material for commercial gain. For users in the Global South, this creates an asymmetrical relationship in which digital resources are consumed but rarely controlled, reinforcing global power imbalances in the digital realm.

Even where access exists, digital literacy and education present another layer of inequality. The ability to critically navigate, evaluate, and utilise digital tools varies widely. Those with higher digital skills can leverage online resources for education, employment, and innovation. Others, however, face challenges understanding basic digital functions and are more susceptible to misinformation or economic exploitation. Warschauer (2004) highlights that without investment in digital education, technology risks reproducing, rather than remedying, social inequalities.



Also, representation in digital content and narratives plays a crucial role in shaping global inequality. Digital platforms often reflect the values, interests, and worldviews of their creators, which are predominantly shaped by Western cultural logics. As a result, many communities find themselves either invisibilised or stereotyped in digital media and algorithms. Noble (2018) argues that algorithmic bias can reinforce harmful racial and cultural stereotypes, limit diverse voices and perpetuate epistemic injustice in digital environments.

Therefore, the issue of influence over global digital governance mechanisms underscores the structural nature of global inequality in the digital era, as standards are typically negotiated and enforced by powerful multinational corporations, leaving developing countries with minimal stake in these decisions². As digital governance becomes a key battleground for rights, equity, and sovereignty, the exclusion of marginalised voices further cements a digitally unequal world order.

Digital Imperialism, Technological Corporations and Global Inequality: The Nexus

The nexus between digital imperialism, technological corporations, and global inequality lies in how control over digital infrastructures, platforms, and data by powerful multinational corporations and advanced nations reinforces historic patterns of dominance. This concentration of digital power in a few global tech giants from the Global North often exacerbates rather than reduces global inequalities, making it essential to address both digital access and the unequal distribution of digital power to promote fair and inclusive global development^{2, 20, 36}.

Unlike traditional industrial firms, technological corporations often scale rapidly through network effects and platform-based business models, allowing them to dominate entire sectors without necessarily owning physical infrastructure. These corporations are characterised by their heavy reliance on data-driven processes, intellectual property, and algorithmic governance elements that enable them to centralise control and extract economic value across borders³⁷.

Scholars^{2, 38} across disciplines have critically examined the role of technological multinational corporations (MNCs), highlighting how they shape global systems of power, inequality, and development. Political economists argue that these corporations wield structural power by influencing global policy through lobbying and regulation evasion, particularly in developing countries^{39, 40, 41}.

Surveillance Capitalism and Digital Imperialism

Surveillance capitalism illustrates how power, knowledge, and profit are unequally distributed in today's digital economy. It exposes not only how personal data is treated as a commercial resource but also reveals the mechanisms through which corporations exert control over individuals and societies, often without their awareness. The defining feature is the large-scale extraction of personal data without users' consent. These Corporations routinely harvest data from search histories, social media interactions, mobile app usage, and increasingly from Internet of Things (IoT) devices embedded in homes, cars, and public spaces³⁵. Users often agree to complex terms and conditions without fully understanding the scope or purpose of data collection. This opaque data harvesting process transforms ordinary human experience into "behavioural surplus" raw material for corporate profit¹. In this way, everyday digital activity becomes a site of extraction akin to mining or logging, with individuals largely unaware of what they are surrendering.

The nexus between surveillance capitalism and digital imperialism lies in the global expansion of capitalist market logic into the digital realm; in this case, the "resource" is personal and behavioural data, and the control is exercised through digital platforms, algorithms, and infrastructure¹. Together, surveillance capitalism and digital imperialism constitute a new form of global inequality, one in which profit is generated through the commodification of human experience, and power is maintained through the technological and epistemic domination of the Global South².

Zuboff (2019)¹ argues that corporations such as Google and Facebook commodify human behaviour by extracting and selling user data to predict and influence actions, transforming autonomy into profit. Such practices reflect data colonialism, where the Global South serves as a data resource zone while the Global North retains control and reaps economic benefits, echoing historical colonial patterns and undermining digital sovereignty, as the Global South nations are denied the ability to regulate and shape their digital ecosystems.

Empirical Review

Using an instrumental variable approach and Afrobarometer seven-year cross-sectional data across 35 African countries, Joël, Yasmine, and Mathilde (2024)⁴² observed that the internet is often utilised as an enabler of propaganda because it serves as a conduit for political misinformation, influencing users' opinions on the value of democracy, voting habits, and protest and weakening trust in political institutions. This is in line with the dependency theoretical framework position that the digital divide is not merely a matter of unequal access to internet connectivity, but a systemic outcome of power imbalances embedded in



technological ownership, infrastructure, regulation, and economic returns⁴³. Thus, media channels and policymakers need to encourage critical thinking among nationals to tackle misinformation. However, the study overlooked the global implications of the actions of these foreign tech corporations.

Zuboff (2019)¹, using extensive case studies, corporate document analysis, and theoretical critique, investigates how major tech companies such as Facebook and TikTok extract and commodify users' behavioural data through sophisticated predictive algorithms, and how user behaviour is transformed into profit-making predictive products. This buttresses the post-colonial and dependency theorist assertion that neocolonialism is the highest stage of imperialism, manifesting in infrastructural and technological dependencies, global inequality, relegation of indigenous culture, and an indirect furtherance of colonial knowledge⁴⁴. The study illustrates how surveillance capitalism consolidates economic and informational power in the hands of a few dominant corporations, thereby exacerbating global inequality. However, while offering a thorough critique of privacy erosion and corporate influence, Zuboff (2019)¹ ignores the evolving asymmetrical dependence within the Global South, aligning with the complex interdependency theoretical framework that unequal power dynamics and coercion can occur within the same region (Global South).

Cadwalladr and Graham-Harrison (2018)⁹, in an investigative study on the Facebook–Cambridge Analytica data scandal, reveal how personal data from millions of users was exploited to influence elections in countries including the U.S. and Nigeria. Their research relies on leaked documents, whistleblower interviews, and investigative journalism to expose how psychographic profiling was used to micro-target voters and manipulate electoral outcomes. This highlights the dependency theory position that the global economic system intrinsically favours the Global North. However, while illustrating the political weaponisation of data, Cadwalladr and Graham-Harrison (2018) overlook the broader economic and democratic consequences for the affected nations in the long run⁹.

Hassan and Segun (2020)⁴⁵ in collaboration with Tactical Tech and the Centre for Democracy and Development (CDD) using semi structured interviews and desk reviews of news articles assesses the use of data in Nigeria elections using the case study of the Cambridge Analytica involvement in the 2015 elections where the defunct tech corporation utilised its digital arsenal to purportedly spread disinformation and published delicate information about the health and fiscal information of the opposition candidate Muhammadu Buhari. Despite the Nigerian

government's investigations and promise to prosecute, nothing has been done on the matter, inadvertently sending a wrong message to other foreign firms. However, Hassan and Segun (2020) overlooked internal dynamics within the nation that fostered such activities⁴⁵.

Chakravartty and Da Silva (2012)⁴⁶, in an empirical media content analysis and interviews, analysed methods employed by media technological corporations such as Bell Pottinger to manipulate public perception and spread misinformation in developing countries. While highlighting the symbolic and discursive mechanisms of influence, the study revealed tactics like narrative control and reputational laundering used to marginalise nations in the Global South. However, the study did not fully address the measurable economic impacts of these media interventions.

Ugor and Afolayan (2020)⁴⁷, using qualitative interviews and content analysis, argued that TikTok and similar entertainment platforms influence youth culture across Africa. The study revealed that these platforms both enable cultural expression and impose Global North-centric aesthetic standards, contributing to cultural homogenisation. This is in line with the post-colonial framework that imperialist power structures continue to influence outcomes in the Global South. However, the study did not adequately examine how platform monetisation reinforces economic dependency on foreign corporations.

THEORETICAL FRAMEWORK - POSTCOLONIAL AND DEPENDENCY THEORY

Post-colonial Theory

Post-colonial theory offers a structural lens via which digital imperialism can be viewed as an extension of colonial domination in modern, digital forms. Drawing from Kwame Nkrumah's concept of neo-colonialism and theorists such as Frantz Fanon and Gayatri Spivak, this theory interrogates how colonial control is sustained after the formal end of colonialism through institutions, language and culture⁸. The theory explicates digital imperialism as a system of indirect control where the post-colonial nation's economy and political systems are influenced by foreign powers to further external interests. In the present day, this control is progressively implemented through data extraction, algorithmic bias, and platform monopolies, which this study terms digital neo-colonialism^{1, 2}.

Post-colonial theory likewise critiques the cultural destruction and epistemic control inherent in global tech ecosystems. Digital platforms often highlight Western narratives and epistemologies, while sidelining indigenous cultures and local knowledge systems. Hence, post-colonial



theory frames digital imperialism not just as an economic or technological manifestation, but as a cultural and ideological development that reproduces colonial hierarchies in cyberspace. While post-colonial theory strongly addresses the cultural, political, and ideological continuities of colonialism, it does not completely account for the technological complexity and corporate dynamics of the contemporary digital landscape.

Dependency Theory

Dependency scholars such as Raúl Prebisch, Andre Gunder Frank, and Samir Amin frame underdevelopment as a structural outcome of the historical and ongoing integration of peripheral economies into a global capitalist system controlled by the core, i.e., the Global North. In the digital age, this framework highlights how former colonies and developing nations are structurally positioned to depend on foreign, mostly Western technological infrastructures and digital platforms. Rather than investing in autonomous digital systems, developing countries are locked into asymmetrical relationships where they import hardware, rely on external platforms (such as Facebook, Google, X or TikTok), and entrust data governance to foreign corporations^{1, 2}.

In this light, digital imperialism can be seen as a continuation of the historical core-periphery relationship, updated for the information age. The digital divide is not merely a matter of unequal access to internet connectivity; it is a systemic outcome of power imbalances embedded in technological ownership, infrastructure, regulation, and economic returns⁴³. These relationships are not neutral, as the absence of robust local tech ecosystems and weak regulatory frameworks creates conditions in which the Global South contributes data, content, and profit but gains little ownership, sovereignty, or long-term development leverage.

Moreover, this dependency is compounded by the absence of capital investment in local technological innovation and the outsourcing of governance functions such as identity verification, biometric registration, and public communications to private foreign entities²⁰. This deepens structural inequalities, as profits are extracted from user engagement, and data flows in the Global South but accrue primarily to firms headquartered in the Global North. As a result, digital dependency mirrors earlier forms of economic dependency, making it difficult for countries in the Global South to achieve technological self-reliance or equitable participation in the global digital economy.

MATERIALS AND METHODS

Research Design

This study adopted a qualitative research design to examine the influence of digital imperialism on global inequality. It uses the case studies of selected multinational technological corporations such as Facebook, Cambridge Analytica, Bell Pottinger, and TikTok.

Population of the Study

The study population comprises 30 participants, categorised into three groups.

- i. Information Technology (IT) and Cybersecurity Experts experienced working with multinational tech corporations remotely and on-site (15).
- ii. Information Technology Experts from electoral agencies within Africa (12).
- iii. Cybersecurity experts in tertiary institutions (3).

Sample Size and Sampling Technique

The purposive sampling technique was employed to determine the sample size for this study and is tailored to specific audiences with in-depth experiences relevant to the study objectives⁴⁸. Participants were selected based on their professional expertise, and those with a minimum of 10 years of work experience were included. This was to validate that they had participated in at least two presidential elections.

Category	Years of Experience	Sample Size	Industry
Information Technology Experts with Multinational corporation experience	Between 10-15 years	15	Social Media
IT Experts with Electoral experience	10-20 years	12	Electoral Agency
Cybersecurity Professors	Senior Lecturer and above	3	Universities in Nigeria

Method of Data Collection/ Data Analysis

The primary data were collected through interviews, recorded and transcribed. The secondary data were sourced from relevant scholarly, peer-reviewed articles and journals related to the topic, and both were thematically analysed using NVivo software.

Ethical Considerations

This study ensured that the data collected remained credible and were utilised solely for the research. It assented to the request of informants for anonymity of identity and organisation.



Reflexivity and Limitations

This study acknowledges that the concept of digital imperialism is evolving and is context-specific within the Global South, as evidenced in China's growing influence in the digital industry. A major limitation is the reliance on primary data only from those who have worked within Africa, which may not fully capture the experiences of other regions in the Global South. Nevertheless, the synthesis of interdisciplinary and peer-reviewed literature permits a complete understanding of the subject matter.

Presentation/Analysis of Interview Data

Table 1: Examine how technological advancements such as the internet and mobile devices have contributed to the rise of digital imperialism and exacerbated inequality in Nigeria

Name	Description
Major Theme 1: Impact of Technological Advancements on digital imperialism and inequalities	
	of Rapid technological progress in Nigeria has outpaced the country's capacity to secure and control its digital assets, leading to growing data vulnerabilities and sovereignty concerns.
Reliance on foreign infrastructure	Nigeria lacks sufficient local data centres, increasing reliance on foreign data servers. Many mobile apps and election platforms are not domiciled in Nigeria.
Weak data control capacity	Nigeria lacks technologies to ensure data sovereignty. Human and institutional capacity for digital security is infantile.
Institutional progress and gaps	Nigeria has made some progress with legal frameworks but lacks enforcement. Regulatory institutions remain under-resourced and politically limited.
Vulnerability of national digital assets	Technological advancement has introduced more vulnerabilities. Data can be accessed through phishing, hacking, and unpatched software bugs.
Inadequate digital incident response	Hacks go years without proper response. Lack of early detection or remedial action in government platforms.

Major Theme 1: Impact of Technological Advancements on Digital Imperialism and Inequality

This theme highlights how Nigeria's growing dependence on foreign internet-enabled and mobile technologies has exposed national digital assets to greater risks. While advancements have improved services and connectivity, they have outpaced the development of local infrastructure

and governance mechanisms. Data sovereignty, the ability of a state to govern and secure its data, remains weak due to limited local data centres, outdated regulations, and technological inadequacy. Institutions struggle to respond to cyber incidents due to a lack of tools, training, and coordination; hence, as more services move online, Nigeria becomes more vulnerable without proportionate investments in digital security^{49, 50}. Below are the sub-themes under this major theme.

Reliance On Foreign Infrastructure

Nigeria's digital infrastructure is heavily reliant on foreign servers, platforms, and cloud services. Despite a few local efforts, such as MainOne, most data is still stored abroad, reducing national control and increasing exposure to external surveillance and data misuse. A respondent has this to say

A significant portion of our data continues to be hosted and processed overseas by foreign tech companies. This reliance reduces national control over sensitive data and exposes the country to external surveillance, misuse, or exploitation.

The respondent emphasised that Nigeria's infrastructure deficit results in the storage of data outside national borders. This situation limits national sovereignty and introduces surveillance risks, making the country dependent on foreign-controlled systems. This corroborates the findings of DPI Africa (2026)⁷⁴ that Africa functions at only about 20% of its obligatory data-centre capacity, and that Nigeria must invest and treat data centres as vital public digital infrastructure, else its digital economy ambitions would only remain a mirage.

Weak Data Control Capacity

The country lacks the technological capability, human resources, and institutional strength to control, collect, and secure data in line with international standards. Even with increased digital adoption, the absence of strong local tech systems undermines sovereignty. A respondent had this to say

Nigeria lacks the technological infrastructure necessary to manage data sovereignty, collect, and secure data in line with international standards.

Here, the participant points to a systemic incapacity, not just infrastructure, but the absence of expertise and standards. This response shows how inadequate technological capacity undermines sovereignty, reinforcing foreign control over Nigeria's digital assets. This is in line with the data sovereignty and national security concerns raised by the Nigeria Data Protection Commission (NDPC); despite the nation's data centre market being



valued at \$1.9 billion by 2031, over 90% of Nigeria's data is hosted abroad⁵¹.

Institutional Progress and Gaps

Although some frameworks have been initiated, such as the Nigeria Data Protection Regulation (NDPR), they suffer from poor implementation, inadequate funding, and limited legal authority. Progress exists, but the gap between policy design and enforcement remains wide. This buttresses Adeoye's (2026)⁵² findings that although the Nigerian laws establish fundamental data protection principles, enforcement remains weak due to inadequate penalties for non-compliance, overlapping jurisdictions and discrepancies in judicial interpretation.

Vulnerability of National Digital Assets

Improved technological developments have exposed confidential assets to threats such as phishing, hacking, and unauthorised access. The digital migration of sensitive information without adequate protection has led to increased risks. Respondent opines that;

Some hacks and vulnerabilities on so-called national digital assets will persist for years without fixes being developed.

This reveals institutional inertia or inadequate capability. Unaddressed vulnerabilities leave Nigeria's digital systems open to exploitation, revealing how technological advancement has increased exposure without proportional safeguards⁵³.

Inadequate Digital Incident Response

Nigeria's cybersecurity landscape is significantly hampered by a dearth of specialised expertise and a sluggish institutional response mechanism. Despite growing digital threats, many vulnerabilities across government platforms and critical national infrastructures remain unaddressed for prolonged periods. This delay is not just a technical issue but reveals deeper systemic weaknesses, including inadequate funding, low prioritisation of cybersecurity, and poor coordination among relevant agencies. An interview respondent puts it this way. agencies. An interview respondent puts it this way.

As a specialist, I understand how to identify common threats, respond, and assist with user awareness.

This overdependence on general IT personnel or moderately skilled individuals means that most cybersecurity responses are reactive rather than preventive⁵⁴. It reflects a culture of firefighting, addressing challenges after they happen instead of implementing robust, proactive strategies such as continuous network monitoring, threat intelligence, penetration testing, and rapid incident containment.

Moreover, the lack of professional specialisation weakens institutional capacity to build resilience against sophisticated attacks such as advanced persistent threats (APTs), ransomware, and social engineering campaigns. Without highly trained cybersecurity teams embedded in key institutions, Nigeria remains vulnerable to threats that exploit not just technological gaps, but also human and organisational deficiencies⁵⁵.

Table 2: Analyse the operations and influence of digital corporations, specifically Facebook, Cambridge Analytica, Bell Pottinger, and TikTok in perpetuating digital imperialism and deepening global inequality in Nigeria

Major Theme 2: Risks and Influence of Foreign Digital Corporations	
Foreign digital companies dominate Nigeria's digital ecosystem, exploiting data, evading accountability, and amplifying misinformation with little local oversight.	
Foreign data control and exploitation	Facebook, TikTok, and others control Nigerian user data. Nigeria suffers from control over data usage, location, and protection.
Lack of transparency and accountability	Privacy policies of corporations are vague and designed for other jurisdictions. Regulatory frameworks in Nigeria can't effectively hold them accountable.
Psychological manipulation and propaganda	Algorithms amplify or suppress narratives. Foreign platforms are used for political propaganda and fake news.
Security risk for professionals	Social engineering and manipulation by multinational corporations make cybersecurity work harder.
Misinformation during elections	Foreign platforms create divisions and reduce trust in democracy. Disinformation spreads rapidly without government oversight.

Major Theme 2: Risks and Influence of Foreign Digital Corporations

This theme explores the risks that multinational technological corporations (e.g., Facebook, TikTok, and Cambridge Analytica) pose to Nigeria's digital and national security, prompting the Nigerian Counter Terrorism Centre (NCTC) to enter into collaboration with social media corporations⁵⁶. These foreign entities have access to massive volumes of Nigerian user data, often without consent or oversight. Their algorithms and platform policies can manipulate public opinion, interfere in political processes, and bypass national regulation. Nigerian institutions lack the technical and legal mechanisms to monitor or hold these companies accountable, thus creating a digital power imbalance. These corporations can influence national debates, elections, and policies without being subject to local laws or public



scrutiny. Below are the sub-themes under this major theme⁵⁷.

Foreign Data Control and Exploitation

Multinational platforms like Facebook and TikTok collect vast amounts of data from Nigerian users but operate under the jurisdiction of foreign legal systems. These corporations often bypass Nigerian oversight, posing a threat to user privacy and state sovereignty. This can be seen in the account of a respondent:

Nigeria does not have control over how its citizens' data is being stored, processed, and used, which in itself is a security risk.

This statement highlights the asymmetry between foreign platforms' exploitation and Nigeria's regulatory inertia. The absence of domestic control over data life cycles undermines national cybersecurity^{58, 59}.

Lack of Transparency and Accountability

These corporations provide vague or opaque privacy policies tailored to global rather than local standards. The absence of enforceable mechanisms in Nigeria allows them to avoid scrutiny or legal consequences for data breaches or misuse. One interview respondent puts it this way.

These companies are often not fully transparent about how they collect, store, or use data from Nigerian users. Their privacy policies are usually vague.

Here, the interviewee exposes the legal opacity of foreign platforms. The generalised policies fail to align with Nigeria's regulatory needs, creating blind spots in data governance. This resonates with Awuese (2026)⁶⁰ position that data has become the new currency, so government must know their right to privacy and request better protection from corporations for their citizens, because if you are not paying for the product, you are the product.

Psychological Manipulation and Propaganda

In the age of digital communication, the influence of foreign technology corporations extends far beyond data collection or commercial activity; it penetrates the very core of political discourse and public opinion. Through algorithmic curation, these platforms personalise the content that users see, reinforcing existing biases, shaping beliefs, and in some cases, manipulating democratic outcomes. Another respondent puts it this way.

They can easily manipulate this data to propagate false political information, such as election results and smear campaigns.

This quote encapsulates a troubling dynamic: foreign platforms, through their access to granular user data and control over content delivery algorithms, wield disproportionate power to influence political narratives^{61, 62}. These platforms can determine which voices are amplified and which are silenced, not based on truth or democratic value, but on engagement metrics and monetisation potential.

Security Risk for Professionals

The growing influence of foreign digital platforms extends beyond the collection and misuse of data; it includes subtle yet potent forms of psychological operations that undermine the effectiveness of local cybersecurity professionals. These operations, often embedded in content curation algorithms and platform design, contribute to the spread of misinformation, political propaganda, and manipulative narratives. Such tactics complicate the work of cybersecurity professionals who are tasked with defending national digital infrastructure. This is what an interviewee had to say.

This type of influence can be categorised as a social engineering attack, which is very hard to defend against due to the human factor.

This response underscores a critical challenge: social engineering attacks do not primarily exploit technical vulnerabilities but rather psychological and habitual weaknesses in individuals. These types of attacks include phishing, misinformation, impersonation, and manipulation through digital media, all of which are designed to deceive users into compromising sensitive systems or spreading false information. This resonates with the findings of Apene *et al.* (2025)⁶³ that social engineering remains one of the most prevalent and costly types of cybercrime, largely due to its exploitation of man-made error and trust.

For cybersecurity professionals in Nigeria, defending against such attacks presents a unique and complex task. Unlike technical breaches that can often be addressed with firewalls, encryption, or system patches, social engineering requires high levels of public awareness, continuous training, and coordinated institutional response resources that are often limited in developing contexts. This is in line with the recommendation of Awuese (2026)⁶⁰ that the government must promote awareness campaigns on the efficient use of social media and the internet.

Misinformation During Elections

Electoral periods are critical junctures in any democracy, and the integrity of information during such times is essential for ensuring free, fair, and credible elections. In Nigeria, the rise of foreign-owned digital platforms such as



Facebook and TikTok has introduced a new and potent threat to democratic stability: the unregulated and rapid spread of false or misleading content.

Such false or misleading content can quickly spread, undermining trust in democratic processes.

This statement reflects a recurring challenge: foreign platforms operate largely beyond the oversight of Nigerian institutions, and their internal moderation systems are either ineffective or inapplicable in Nigeria's unique political, social, and linguistic contexts. As a result, false claims, doctored content, inflammatory rhetoric, and election-related disinformation ranging from fake polling dates to falsified results or manipulated narratives proliferate with little to no regulation.

The underlying design logic of these platforms is a critical factor in this risk. Algorithms are optimised to prioritise engagement over accuracy, meaning content that triggers emotional responses, such as fear, anger, or outrage, is often favoured and more widely distributed than fact-based or nuanced political content. Although social media has democratised political engagement, it has also led to some impediments, as the handling of these algorithms often intensifies political fragmentation, exposing users to content that reinforces their prejudice, furthering a more divided political environment⁶⁴.

Summary of Data Analysis

The data analysis reveals that despite the immense benefits of globalisation, technological advancement, institutional weaknesses, foreign corporate dominance, and global policy asymmetries collectively reinforce digital imperialism in Nigeria. Much like the economic consequences of second-hand textile dumping that displace local industries, digital imperialism imposes a structural imbalance that undermines Nigeria's sovereignty, suppresses local innovation, and widens global inequality.

One of the major findings is Nigeria's heavy dependence on foreign digital infrastructure, including data centres, cloud services, and social platforms. As critical national data is stored abroad and managed by multinational corporations such as Facebook, Google, and TikTok, Nigeria loses control over sensitive information, increasing its vulnerability to foreign surveillance, manipulation, and exploitation⁶⁵. The rapid adoption of the internet and mobile technologies has not been matched by local capacity building, leaving the nation exposed to cyber threats without sufficient regulatory or technical safeguards.

Weak institutional frameworks further intensify infrastructural and technological dependency. Nigeria's

data protection and cybersecurity laws remain outdated, poorly enforced, and overly reliant on foreign legal models such as the EU's GDPR. Regulatory bodies lack the authority, resources, and coordination to confront the fast-evolving digital landscape^{66, 67}. These institutional gaps mirror the policy failures that further digital exploitation.

Ultimately, digital imperialism thrives, like a modern extension of colonial dependency, due to a digital ecosystem governed by external rules, foreign infrastructure, and unequal access to profits. The implications for political autonomy and economic development are significant because foreign platforms wield the power to shape public opinion, control narratives, and influence national elections, often serving the geopolitical or commercial interests of external powers⁶⁸.

The study underscores the urgent need for Nigeria to assert digital sovereignty by investing in local infrastructure, revising outdated regulatory frameworks, building cybersecurity capacity, and resisting one-sided global digital arrangements^{69, 70}. Without such efforts, digital imperialism will continue to reproduce and intensify global inequality in the information age.

FINDINGS/CONCLUSION

The findings of this study reveal that technological advancements, particularly the proliferation of the internet and mobile devices, have served as powerful enablers of digital imperialism, reshaping socio-political, economic, and cultural dynamics in the Global South. This aligns with Zuboff's (2019)¹ position that such technological tools, while offering connectivity and convenience, have become instruments for large-scale surveillance capitalism. Also, both the respondents and secondary sources indicate that these technologies are not merely neutral infrastructures but are embedded with asymmetrical power relations that favour global technological corporations headquartered in the Global North, highlighting the dependency theoretical framework position of integration into an exploitative global capitalist system. This buttresses Couldry and Mejias' (2019)² assertion that data extraction and algorithmic governance extend historical imperialist practices into the digital domain, creating a new form of dependency that entrenches global inequality.

Furthermore, the study affirms that selected technological corporations- Facebook, Cambridge Analytica, Bell Pottinger, and TikTok play active roles in perpetuating global inequality through deliberate practices of data manipulation, targeted disinformation, and narrative control. The operational patterns identified resonate with the documented activities of Cambridge Analytica in



Kenya and India, where psychographic profiling and microtargeting influenced electoral outcomes⁹. These findings corroborate Wylie's (2019)⁵ claim that such corporations function as covert political actors capable of undermining democratic processes in developing nations.

Similarly, the role of Bell Pottinger in South Africa, as revealed in this study, underscores Fraser's (2017)¹⁴ position that information warfare and ethnic manipulation have become lucrative tools in digital imperialism, often serving elite interests at the expense of national cohesion. In the Nigerian context, TikTok's content curation patterns not only shape youth culture but also influence political consciousness, often in ways that align with foreign commercial and geopolitical interests. This aligns with Wan Ismail, Aini Alivi and Dharejo's (2025)⁷¹ position that TikTok portentously impacts the voting behaviour of youths and influences political choices, affirming the post-colonial theory assertion that social media perpetuates cultural hegemony.

In addition, the study reveals that the implications of digital imperialism extend deeply into the socio-economic fabric of the Global South. A major finding is the erosion of digital sovereignty, where developing nations lack the infrastructural capacity and legislative authority to control their own data flows. This is consistent with the position of Pohle and Thiel (2020)³⁶ that digital dependency restricts the autonomy of states, making them vulnerable to external control over critical information systems. The reliance on foreign-owned platforms, as documented in the Nigerian case, mirrors Ndemo and Weiss's (2017)⁷² argument that dependency on external digital infrastructure stifles indigenous innovation and entrenches the peripheral status of developing economies. This supports the findings of Hassan and Segun (2020)⁴⁵ that the inadequacy of political consulting firms in Nigeria's political campaign industry makes foreign firms an alternative.

Another critical dimension emerging from the findings is the weaponisation of digital tools for political destabilisation. Disinformation campaigns, troll farms, and bot networks are documented as operational across several countries, including Nigeria. This aligns with Bradshaw and Howard's (2017)⁷³ finding that coordinated computational propaganda has become a global phenomenon. The Nigerian experience reflects a broader pattern where fragile democracies are particularly susceptible to these tactics, which exploit existing ethnic, religious, and political cleavages to polarise societies.

In conclusion, digitalisation has revolutionised all sectors of the 21st-century global system; to draw from these benefits, nations must position themselves optimally by

being producers and not just consumers. Nonetheless, digital imperialism is neither an abstract theoretical construct nor an inevitable by-product of technological progress. Rather, it is a deliberate, structured, and evolving form of domination that operates across economic, political, cultural, and epistemic dimensions. By examining the Nigerian case within the broader Global South, the study concludes that the operations of Facebook, Cambridge Analytica, Bell Pottinger, and TikTok collectively reproduce and deepen global inequalities. The convergence of technological dependency, data exploitation, political manipulation, and cultural homogenisation demands urgent policy, legal, and civil society interventions aimed at safeguarding digital sovereignty, promoting equitable technological development, and decolonising digital spaces.

Recommendations

The Nigerian government must prioritise investment in digital infrastructure, supported by public-private partnerships, and foreign direct investment, as this would guarantee a key stakeholder position in policies and decision-making.

Section 5 of the 2023 Nigeria Data Protection Act should be amended to recognise data as an important national asset and its protection for the nation's digital sovereignty.

Furthermore, Section 41 and 44 of the Nigeria Data Protection Act should be amended to expand the duties of the Nigeria Data Protection Commission, beyond regulatory compliance, to include oversight over data domiciliation

Nigeria can draw lessons from the international collaborative models of nations like Estonia, China, Singapore, South Korea and India, while adapting its approach to its unique economic, legal, and cultural realities to address implementation challenges

Grants to support domestic innovation and public awareness campaigns on the double-edged nature of digitalisation should be promoted.

REFERENCES

1. Zuboff S. (2019). *The Age of Surveillance Capitalism: The Fight for A Human Future at The New Frontier of Power*. Public Affairs.
2. Couldry N, Mejias UA. (2019). *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*. Stanford University Press.
3. Unwin T. Reclaiming Information and Communication Technologies for Development. *Oxford Scholarship Online*. 2017; . Available from: <https://doi.org/10.1093/oso/9780198795292.001.0001>
4. Roberts T. (2018). *Digital Development, What's in A Name? Opening The Black Box of ICT4D*. In M. Graham & L. Hjorth (Eds.), *Digital Economies at Global Margins* (pp. 69–91). MIT Press.
5. Wylie C. (2019). *Mindfck: Cambridge Analytica and the Plot to Break America*. Random House.



6. Ekdale B, Tully M. How the Nigerian and Kenyan media handled Cambridge Analytica. . Available from: <https://doi.org/10.64628/aaj.evkdsfwf66>
7. BBC. (2018a, March 25). *Cambridge Analytica linked firm 'boasted of poll interference'*. . Available from: <https://www.bbc.com/news/uk-43528219>
8. Nkrumah K. (1965). *Neo-colonialism: The Last Stage of Imperialism*. Thomas Nelson & Sons.
9. Cadwalladr C, Graham-Harrison E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. . Available from: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
10. BBC. (2018b, April 4). *Facebook scandal 'hit 87 million users'*. . Available from: <https://www.bbc.com/news/technology-43649018>
11. BBC. (2018c, March 20). *Cambridge Analytica's Kenya election role must be investigated*.
12. Greenfield P. (2018, March 20). *Cambridge Analytica: Links to Kenya's election raise new questions*. The Guardian. . Available from: <https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-links-to-kenyas-election-raise-new-questions>
13. Kiroyan N. (2018, May 22). *Learning from the Bell Pottinger Case*. *PR Indonesia Magazine*, 38th Edition, pp. 55.
14. Fraser A. (2017, September 5). *We go inside the Guptabot fake news network*. *Daily Maverick/TechCentral*. . Available from: <https://www.dailymaverick.co.za/article/2017-09-05-we-go-inside-the-guptabot-fake-news-network/>
15. Gorwa R. The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*. 2019; 8 (2) . Available from: <https://doi.org/10.14763/2019.2.1407>
16. Srinivasan J. (2017). Where Is the Public in Critical Perspectives on Digital Technologies? *Information Technology for Development*, 23(1), 163–185.
17. West DM. (2016, January 12). *Internet Shutdowns Cost Countries \$2.4 Billion Last Year*. Brookings Institution.
18. Global Voices. (2017, February 15). *Facebook's Free Basics: A "dictator's dream" for India's internet?* Global Voices.
19. McMillan R. (2016, February 8). *India bans Facebook's Free Basics service*. The Wall Street Journal.
20. Gurumurthy A, Chami N. (2017). *Digital India: Whose India? IT for Change*.
21. Tufekci Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.
22. Oxford Internet Institute. (2019). *Industrialized Disinformation: 70 Countries Manipulated by Governments, Politicians, Parties*. Oxford University Press.
23. Howard PN, Bradshaw S. (2018). *The Global Organization of Social Media Disinformation Campaigns*. Oxford Internet Institute.
24. Stallman R. (2015). The Right to Read and Freedom in The Digital Society. *Communications of the ACM*, 62(6), 38–40.
25. Vaidhyathan S. (2018). *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford University Press.
26. Nyabola N. *Digital Democracy, Analogue Politics: How The Internet Era Is Transforming Politics in Kenya*. 2018; . Available from: <https://doi.org/10.5040/9781350219656>
27. McNamee R. (2019). *Zucked: Waking up to the Facebook Catastrophe*. Penguin Press.
28. Kayode WO, Nelson O. (2019). Role of Information and Communications Technology (ICT) in Governance in Southwest Nigeria. *KoG*, 3(2), 1–10.
29. Tiago P, Micah LS. Civic Tech in the Global South: Assessing Technology for the Public Good. 2017; . Available from: <https://doi.org/10.1596/27947>
30. Heeks R. (2017). *Information and Communication Technology for Development (ICT4D)*. Routledge.
31. Moore M. (2018). *Bell Pottinger, the South African Scandal, and the Collapse of a PR Giant*. Centre for the Study of Media, Communication and Power, King's College London.
32. Germano F, Sobbrío F. Opinion dynamics via search engines (and other algorithmic gatekeepers). *Journal of Public Economics*. 2020; 187 :104188 . Available from: <https://doi.org/10.1016/j.jpubeco.2020.104188>
33. Isaak J, Hanna MJ. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*. 2018; 51 (8) :56-59 . Available from: <https://doi.org/10.1109/mc.2018.3191268>
34. Bhambra GK. *Decolonising Social Theory, Public Sociology and Digital Platforms*. *Doing Sociology*. (2024, July 31); . Available from: <https://doingsociology.org/2024/07/31/decolonising-social-theory-public-sociology-and-digital-platforms-gurminder-k-bhambra/>
35. Van Dijck J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*. 2014; 12 (2) :197-208 . Available from: <https://doi.org/10.24908/ss.v12i2.4776>
36. Pohle J, Thiel T. Digital sovereignty. *Internet Policy Review*. 2020; 9 (4) . Available from: <https://doi.org/10.14763/2020.4.1532>
37. Kenney M, Zysman J. (2016). The Rise of the Platform Economy: How Platforms Transform Industries and Create New Opportunities. *Issues in Science and Technology*, 32(3), 61–69.
38. Fuchs C. (2017). *Social Media: A Critical Introduction (2nd ed.)*. SAGE Publications.
39. Delalić S, Merdanović A, Kasumović Z. Multinational Corporations (MNCs) and Global Governance in the Age of Globalization: Challenges and Opportunities – Reshaping Power Dynamics. *Društvene i humanističke studije (Online)*. 2025; 10 (2(28)) :773-802 . Available from: <https://doi.org/10.51558/2490-3647.2025.10.2.773>
40. Polk A, Schmutzler A, Müller A. Lobbying and the power of multinational firms. *European Journal of Political Economy*. 2014; 36 :209-227 . Available from: <https://doi.org/10.1016/j.ejpoleco.2014.07.010>
41. Strange S. *The Retreat of the State: The Diffusion of Power in The World Economy*. Cambridge University Press. 1996; . Available from: <https://doi.org/10.1017/cbo9780511559143>
42. Joël C, Yasmine E, Mathilde M. Misinformation technology: Internet use and political misperceptions in Africa. *Journal of Comparative Economics*. 2024; 52 (2) :400-433 . Available from: <https://doi.org/10.1016/j.jce.2024.01.002>
43. Foster JB, McChesney RW. (2014). *The Endless Crisis: How Monopoly-Finance Capital Produces Stagnation and Upheaval from the USA to China*. Monthly Review Press.
44. Kapoor I. Capitalism, culture, agency: Dependency versus postcolonial theory. *Third World Quarterly*. 2002; 23 (4) :647-664 . Available from: <https://doi.org/10.1080/0143659022000005319>
45. Hassan I, Segun T. (2020). *Personal Data and the Influence Industry in Nigerian Elections: Data-Driven Campaigning by Formal and Informal Actors*. Tactical Tech and the Centre for Democracy and Development.
46. Chakravartty P, Da Silva T. (2012). Postcolonial agency in the digital age: Bell Pottinger and the politics of media manipulation. *African Journalism Studies*, 33(3), 45–62.
47. Ugor P, Afolayan A. (2020). Youth, Digital Cultures, and Cultural Imperialism in Africa: A TikTok Case Study. *African Studies Review*, 63(2), 134–153.
48. Tajik O, Golzar J, Noor S. (2024). Purposive Sampling. *International Journal of Education and Languages Studies*, 2(2).
49. Fasogbon M. (2026, February 28). *Experts Warn Nigeria's Digital Ambitions at Risk Without Infrastructure Investment*. ThisDay.
50. Guardian Nigeria. (2026, April 16). *Nigeria's digital growth and the rising stakes of cybersecurity*.
51. Nnamani A. (2026, May 03). *90% of Nigeria's data hosted abroad, NDPC flags sovereignty threat*. The Sun.
52. Adeoye B. *The Legal Framework for the Protection of Users' Data on Social Media in Nigeria*. . Available from: <https://doi.org/10.2139/ssrn.6115408>



53. Balogun F. (2026, June 2). *Cyberattacks expose the fragility of Nigeria's Digital Economy as businesses face rising risks*. Business Day.
54. Adeyemi A. (2025, July 23). *Nigeria's cybersecurity framework is mostly reactive*. The Guardian.
55. Lewis L, Alan W. (2023). *Cybersecurity Challenges in Nigeria's Government Agencies and Ministries*. ResearchGate.
56. Sahara Reporters. (2025, December 23). *Nigeria Working with Facebook, TikTok, X, Others To Delete Terrorists' Accounts, Curb Propaganda – Counter-Terrorism Chief*.
57. Business Day. (2018, April 1). *Presidency investigates Cambridge Analytica on Nigeria's data hacking*.
58. Onyeagoro J. (2025, December 17). *Galaxy Backbone Champions Data Sovereignty to Secure Nigeria's Digital Future*. Tech Africa News.
59. Ajiji YM. (2017). *Cyber Security Issues in Nigeria and Challenges*.
60. Awuese LI. (2026). *The Cost of Free Data: How Data Subjects Unknowingly Trade Privacy for Convenience*.
61. O'Neil C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.
62. Okonkwo OA. Power dynamics of information control, censorship, and digital transparency shaping human rights discourse in the information society. *GSC Advanced Research and Reviews*. 2021; 9 (3) :184-202 . Available from: <https://doi.org/10.30574/gscarr.2021.9.3.0283>
63. Apene OZ, *et al.* Social Engineering Attacks: Global Trends, Nigerian Case Studies, and Mitigation Strategies. *European Journal of Applied Science, Engineering and Technology*. 2025; 3 (5) :241-249 . Available from: [https://doi.org/10.59324/ejaset.2025.3\(5\).20](https://doi.org/10.59324/ejaset.2025.3(5).20)
64. Agama O, Onum O. Examining the Influence of Social Media Algorithms on Political Polarization in Democracies. *Cultural Communication and Socialization Journal*. 2025; 6 (1) :01-08 . Available from: <https://doi.org/10.26480/ccsj.01.2025.17.24>
65. Ibeh R. (2026, June 14). *80% of .ng domain is hosted abroad, exposing Nigeria's digital dependence*. Business Day.
66. Babajide C, Martin S. (2022). *Data Privacy Laws in Nigeria: Compliance and Enforcement Issues*. ResearchGate.
67. Edah R. (2025). *Navigating the Intersection of Cybersecurity and Data Protection Laws in Nigeria*.
68. Bretas VP, Tippmann E. Geopolitical tensions: risks and challenges for internationally scaling businesses. *Multinational Business Review*. 2025; 33 (4) :585-603 . Available from: <https://doi.org/10.1108/mbr-07-2025-0244>
69. Patrick-Okwoli L. (2026, July 16). *Nigeria risks digital exclusion without reliable infrastructure, FG tells Stakeholders*. Business Day.
70. Falade PV, Osho O. (2025). *Nigeria's Digital Sovereignty: Analysis of Cybersecurity Legislation, Policies, and Strategies*.
71. Wan Ismail W, Aini Alivi M, Dharejo N. Tiktok's Influence On Young Voters: A Review Of Social Media's Role In Political Decisions. *International Journal of Environmental Sciences*. 2025; :817-828 . Available from: <https://doi.org/10.64252/y5j0z997>
72. Ndemo B, Weiss T. *Digital Kenya: An Entrepreneurial Revolution in the Making*. Palgrave Macmillan. 2017; . Available from: <https://doi.org/10.1057/978-1-137-57878-5>
73. Bradshaw S, Howard PN. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute.
74. DPI Africa. (2026, January 22). *Nigeria's Digital Public Infrastructure Hampered by Data Centre Shortage*. DPI Africa Info Hub.
75. Milanovic B. *Global inequality: A new approach for the age of globalization*, Cambridge, Massachusetts: Harvard University Press, 2016. *Ekonomski horizonti*. 2016; 18 (2) :181-182 . Available from: <https://doi.org/10.5937/ekonhor1602181t>

